CSCE689: Programming LLMs

HW3 Report (Personal AI Assistant)

Contents

CSCE689: Programming LLMs 1

HW3 Report (Personal AI Assistant) 1

Goal 2

Solution 2

- Summary and code walkthrough 2
- Code Walkthrough 2
- Supported tools 2

Privacy Handling 3

Clarification Handling 3

Setup Instructions 3

Appendix: Chat Screenshots 5

Internet Search proof 5

Sending Emails 8

Read PDFs 10

Schedule Meetings 12

Asking Questions 13

Compound Actions 13

Omar Khater

Goal

Write a personal AI assistant that can

- Write and send emails on your behalf (1pt)
- Read multiple PDF files and answer questions (1pt)
- Schedule meetings for you (2pt)
- Search the Internet (2pt)
- Ask you questions, e.g., for your private information or when uncertain (2pt)

Key requirement (2pt):

- Do not leak your private information (use a local LLM instead) Feel free to use any public LLM APIs for non-private data.

Solution

In this submission, I created a personal AI assistant based on a locally deployed LLM, namely the Meta Llama 3.2 3B. The assistant is a basic Flask app with simple UI that mimics ChatGPT style.

Summary and code walkthrough

The ai_assistant.py and app.py files create a Flask-based personal assistant application that leverages language models and various APIs to perform complex tasks such as reading PDFs, conducting internet searches, sending emails, and scheduling meetings. The assistant interacts with users through a web interface and processes requests with an underlying language model.

Code Walkthrough

- **ai_assistant.py** defines the assistant's core functionality, including supported tools, task handling, and language model interactions. It uses an instance of the AIAssistant class to manage different modules, each designed to handle a specific task.
- **app.py** sets up the Flask application, handling requests through defined endpoints:
  - status: Returns the assistant's status as a JSON response.
  - chat: Processes user messages and returns model responses.
  - index: Renders the main HTML interface.

Supported tools

The assistant supports four main tools, each with its own function and parameters. These tools can be invoked based on the user's input, allowing the assistant to offer versatile, task-specific responses.

OmarKhater

PDF Analyzer

The function read_pdfs extracts text and generates embeddings. The user query is parsed to give information about the analyzed content. Please note that basic embeddings analyzing is coded as a proof of concept.

Internet Research

The app can executes internet search using Tavily API. The function internet_search encapsulates the logic needed to do the search.

Email Drafting and Sending

The function send_email is trying to look up the recipient by name in a contacts file or using a direct email address.

Schedule Meetings

The function schedule_meeting schedule meeting through Zoho Calendar, creating events and adding participant.

Privacy Handling

To ensure privacy, only local LLM is used which is Ollama. The Python API library is used to interact with models all while ensuring that no sensitive data is sent over the internet.

Clarification Handling

The chat API from python Ollama is used to ensure that the assistant can keep conversation style with the user.

Setup Instructions

Note: The application & setup instruction has been tested with *Python 3.10 and PowerShell on Windows 11*.

- [Optional] Create & Activate Python Virtual Environment by running the following in the terminal.

```
python -m venv test_env
.\test_env\Scripts\activate
```

- Install requirements.txt

```
1.pip-compile requirements.in && pip-sync requirements.txt
```

- Run the Flask application by using the following command

```
python app.py
```

- Create the custom assistant from the model file

```
ollama create mymodel -f ./Modelfile1.
```

- Open the local server on any browser

```
http://127.0.0.1:5000/
```

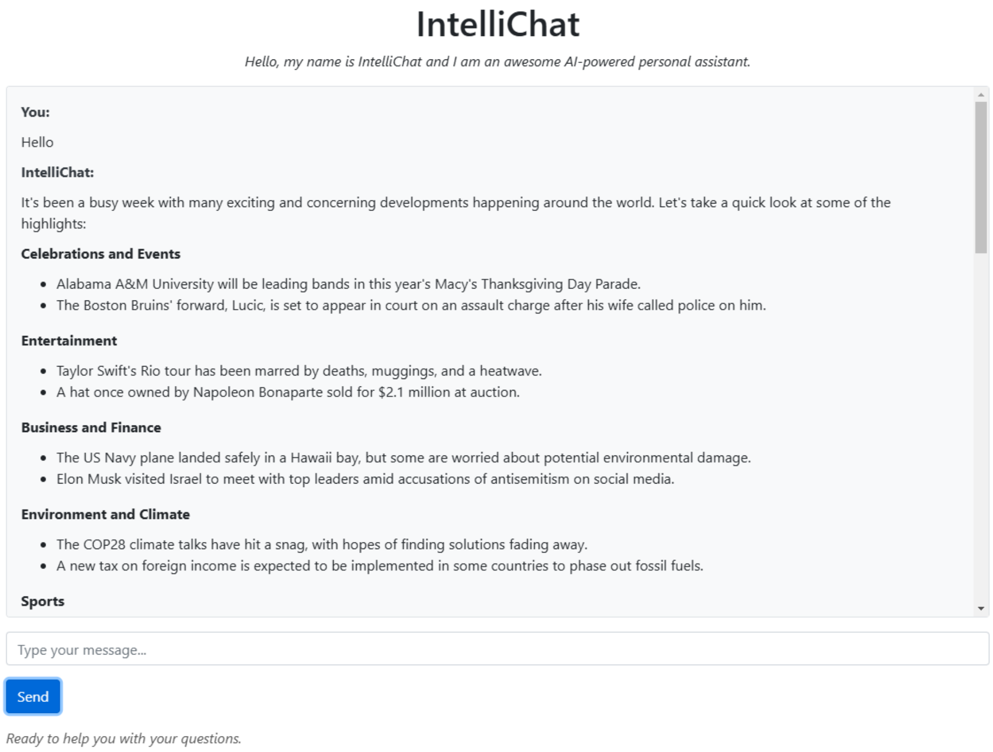
Omar Khater

- Have fun with IntelliChat!

Omar Khater

Appendix: Chat Screenshots

Internet Search proof



Hello, my name is IntelliChat and I am an awesome AI-powered personal assistant.

You:

Hello

IntelliChat:

It's been a busy week with many exciting and concerning developments happening around the world. Let's take a quick look at some of the highlights:

Celebrations and Events

- Alabama A&M University will be leading bands in this year's Macy's Thanksgiving Day Parade.
- The Boston Bruins' forward, Lucic, is set to appear in court on an assault charge after his wife called police on him.

Entertainment

- Taylor Swift's Rio tour has been marred by deaths, muggings, and a heatwave.
- A hat once owned by Napoleon Bonaparte sold for $2.1 million at auction.

Business and Finance

- The US Navy plane landed safely in a Hawaii bay, but some are worried about potential environmental damage.
- Elon Musk visited Israel to meet with top leaders amid accusations of antisemitism on social media.

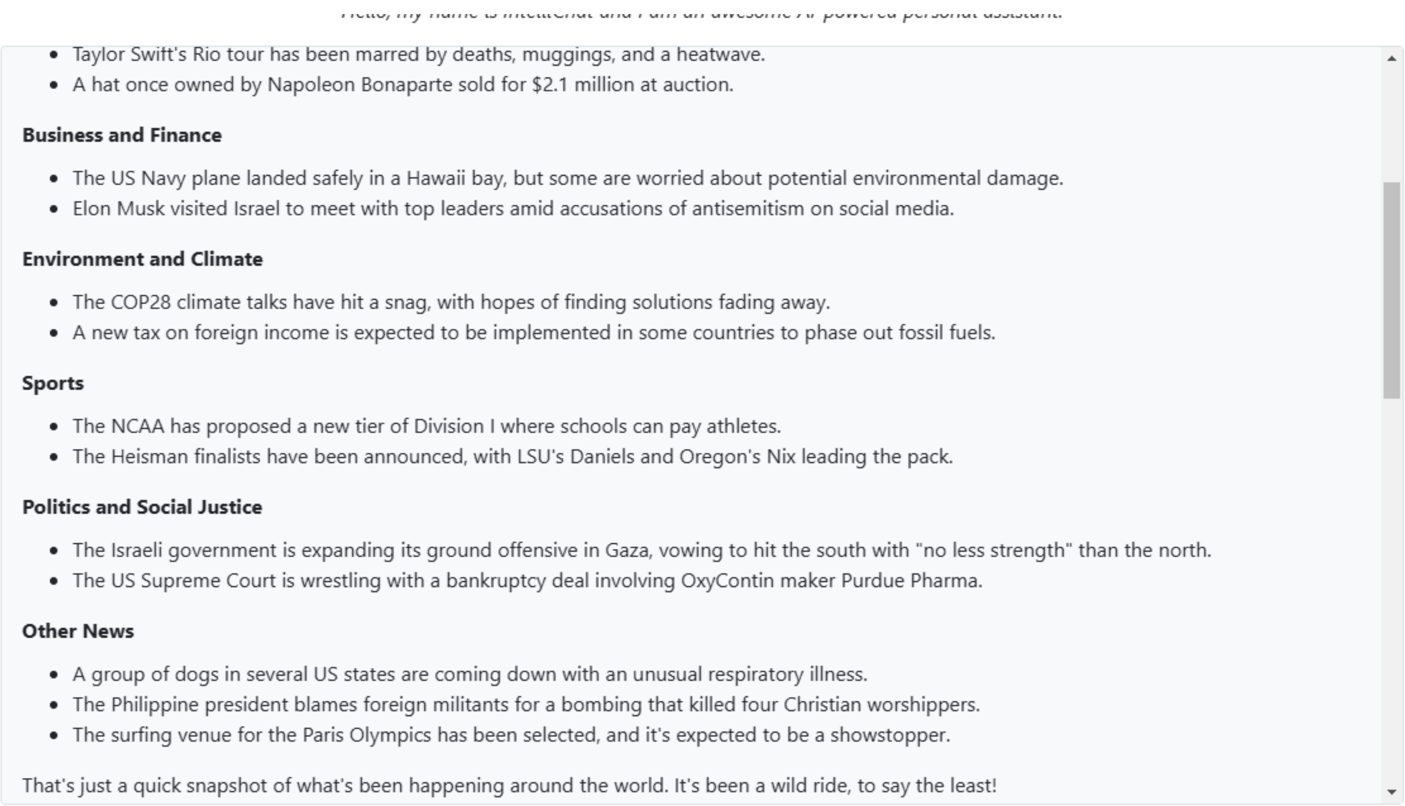
Environment and Climate

- The COP28 climate talks have hit a snag, with hopes of finding solutions fading away.
- A new tax on foreign income is expected to be implemented in some countries to phase out fossil fuels.

Sports

Ready to help you with your questions.

Omar



Hello, my name is IntelliChat and I am an awesome AI-powered personal assistant.

- Taylor Swift's Rio tour has been marred by deaths, muggings, and a heatwave.
- A hat once owned by Napoleon Bonaparte sold for $2.1 million at auction.

Business and Finance

- The US Navy plane landed safely in a Hawaii bay, but some are worried about potential environmental damage.
- Elon Musk visited Israel to meet with top leaders amid accusations of antisemitism on social media.

Environment and Climate

- The COP28 climate talks have hit a snag, with hopes of finding solutions fading away.
- A new tax on foreign income is expected to be implemented in some countries to phase out fossil fuels.

Sports

- The NCAA has proposed a new tier of Division I where schools can pay athletes.
- The Heisman finalists have been announced, with LSU's Daniels and Oregon's Nix leading the pack.

Politics and Social Justice

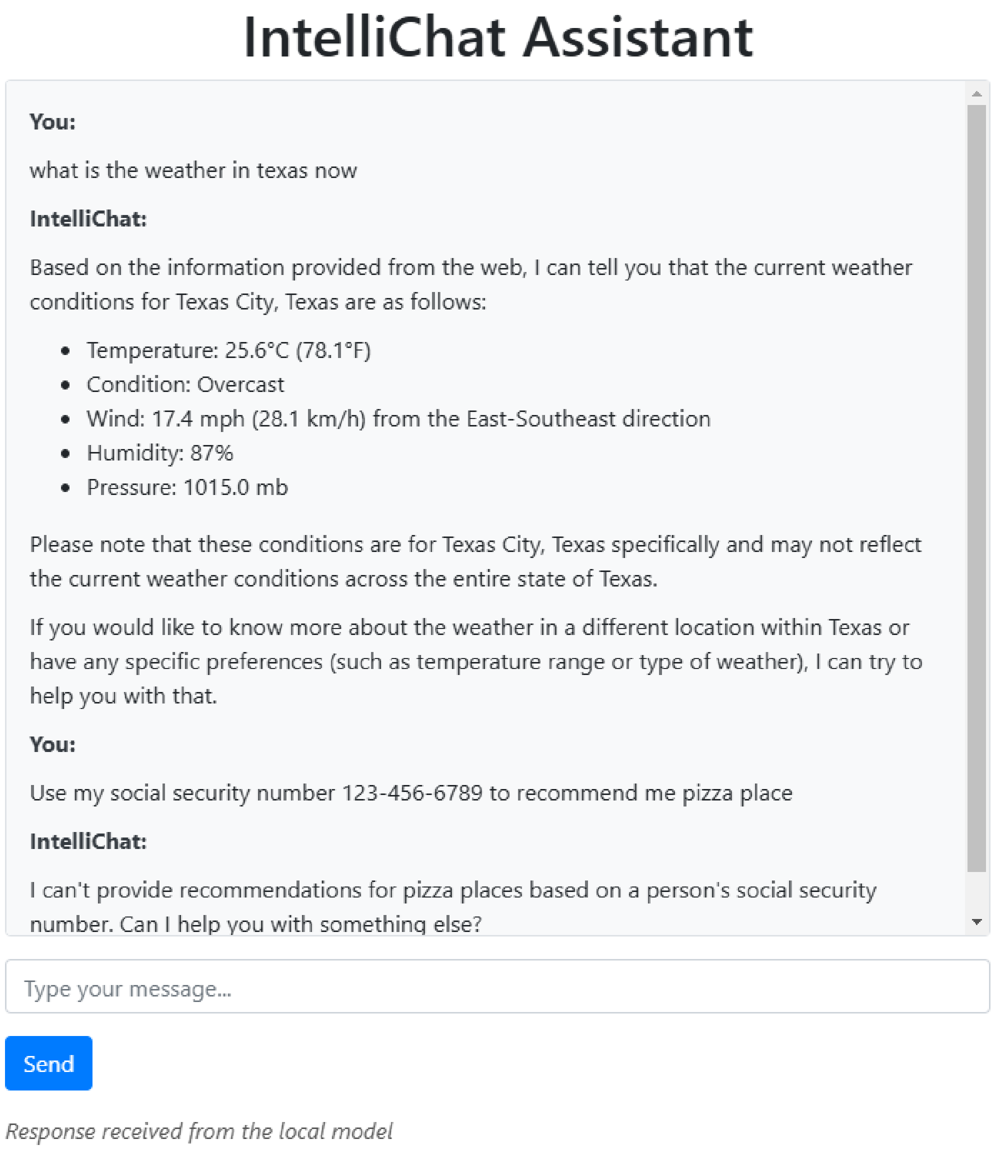
- The Israeli government is expanding its ground offensive in Gaza, vowing to hit the south with "no less strength" than the north.
- The US Supreme Court is wrestling with a bankruptcy deal involving OxyContin maker Purdue Pharma.

Other News

- A group of dogs in several US states are coming down with an unusual respiratory illness.
- The Philippine president blames foreign militants for a bombing that killed four Christian worshippers.
- The surfing venue for the Paris Olympics has been selected, and it's expected to be a showstopper.

That's just a quick snapshot of what's been happening around the world. It's been a wild ride, to say the least!

Omar K



IntelliChat Assistant

You:

what is the weather in texas now

IntelliChat:

Based on the information provided from the web, I can tell you that the current weather conditions for Texas City, Texas are as follows:

- Temperature: 25.6°C (78.1°F)
- Condition: Overcast
- Wind: 17.4 mph (28.1 km/h) from the East-Southeast direction
- Humidity: 87%
- Pressure: 1015.0 mb

Please note that these conditions are for Texas City, Texas specifically and may not reflect the current weather conditions across the entire state of Texas.

If you would like to know more about the weather in a different location within Texas or have any specific preferences (such as temperature range or type of weather), I can try to help you with that.

You:

Use my social security number 123-456-6789 to recommend me pizza place

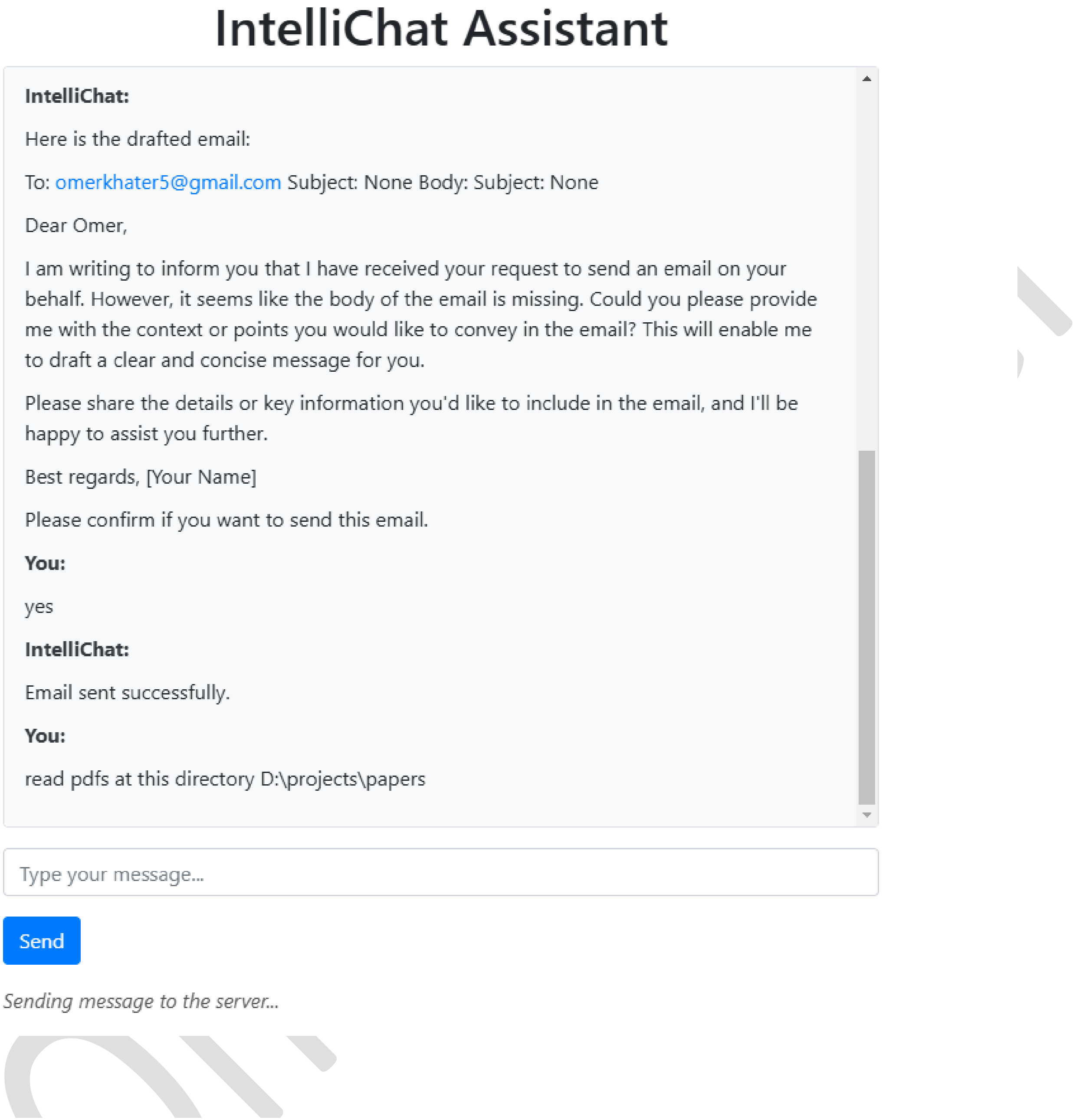
IntelliChat:

I can't provide recommendations for pizza places based on a person's social security number. Can I help you with something else?

Response received from the local model

On

Sending Emails



IntelliChat:

Here is the drafted email:

To: omerkhater5@gmail.com Subject: None Body: Subject: None

Dear Omer,

I am writing to inform you that I have received your request to send an email on your behalf. However, it seems like the body of the email is missing. Could you please provide me with the context or points you would like to convey in the email? This will enable me to draft a clear and concise message for you.

Please share the details or key information you'd like to include in the email, and I'll be happy to assist you further.

Best regards, [Your Name]

Please confirm if you want to send this email.

You:

yes

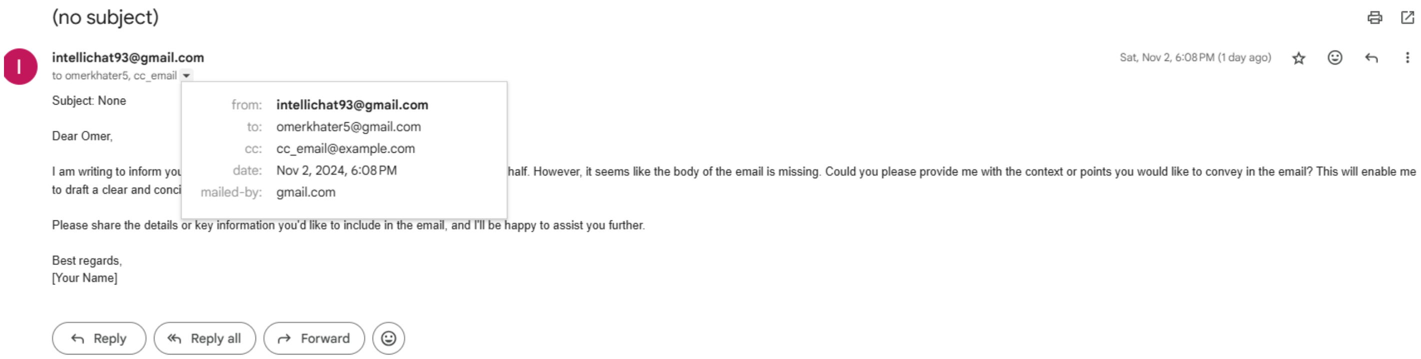
IntelliChat:

Email sent successfully.

You:

read pdfs at this directory D:\projects\papers

Sending message to the server...



intellichat93@gmail.com
to omerkhater5, cc_email

Sat, Nov 2, 6:08 PM (1 day ago)

from: **intellichat93@gmail.com**
to: omerkhater5@gmail.com
cc: cc_email@example.com
date: Nov 2, 2024, 6:08 PM
mailed-by: gmail.com

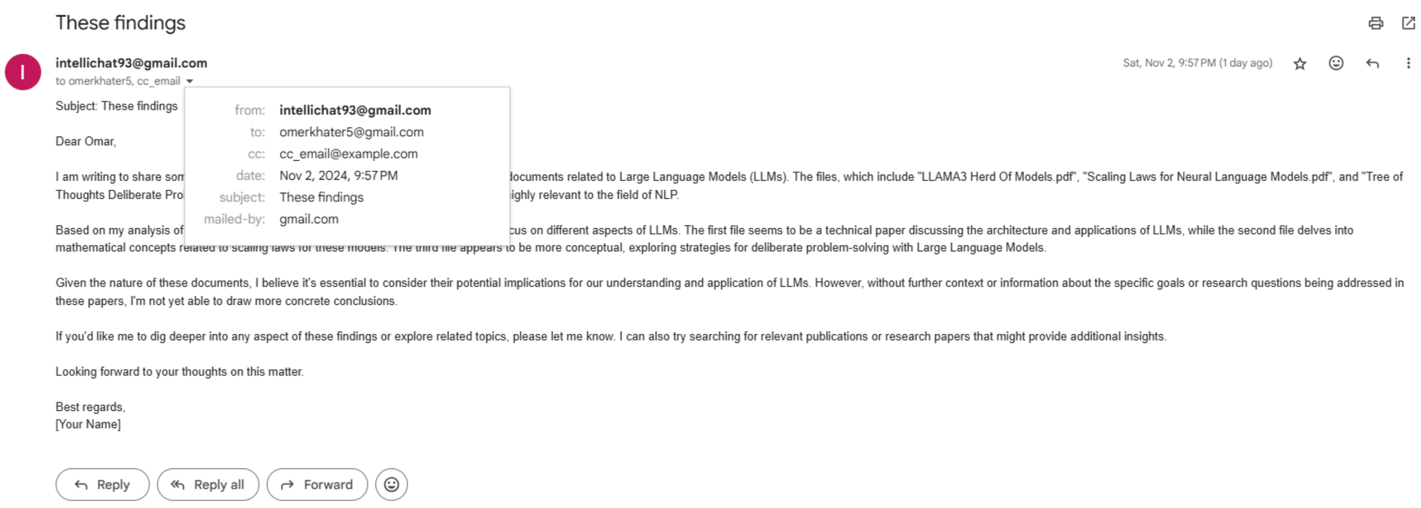
Subject: None

Dear Omer,

I am writing to inform you
half. However, it seems like the body of the email is missing. Could you please provide me with the context or points you would like to convey in the email? This will enable me
to draft a clear and conci

Please share the details or key information you'd like to include in the email, and I'll be happy to assist you further.

Best regards,
[Your Name]



These findings

intellichat93@gmail.com
to omerkhater5, cc_email

Sat, Nov 2, 9:57 PM (1 day ago)

from: **intellichat93@gmail.com**
to: omerkhater5@gmail.com
cc: cc_email@example.com
date: Nov 2, 2024, 9:57 PM
subject: These findings
mailed-by: gmail.com

Subject: These findings

Dear Omar,

I am writing to share som locuments related to Large Language Models (LLMs). The files, which include "LLAMA3 Herd Of Models.pdf", "Scaling Laws for Neural Language Models.pdf", and "Tree of Thoughts Deliberate Pro ighly relevant to the field of NLP.

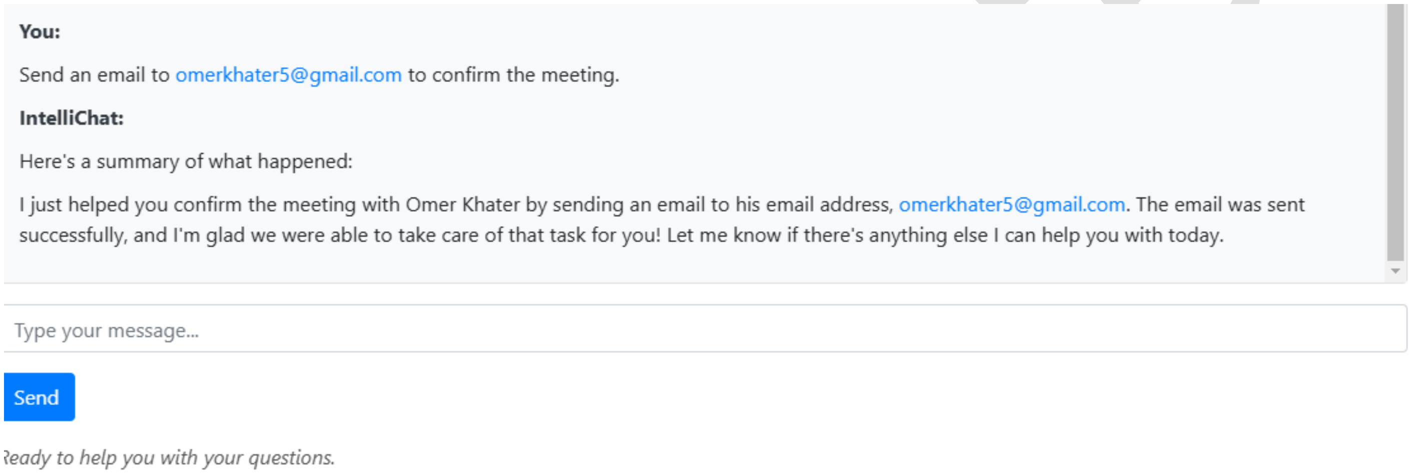
Based on my analysis of cus on different aspects of LLMs. The first file seems to be a technical paper discussing the architecture and applications of LLMs, while the second file delves into mathematical concepts to be more conceptual, exploring strategies for deliberate problem-solving with Large Language Models.

Given the nature of these documents, I believe it's essential to consider their potential implications for our understanding and application of LLMs. However, without further context or information about the specific goals or research questions being addressed in these papers, I'm not yet able to draw more concrete conclusions.

If you'd like me to dig deeper into any aspect of these findings or explore related topics, please let me know. I can also try searching for relevant publications or research papers that might provide additional insights.

Looking forward to your thoughts on this matter.

Best regards,
[Your Name]



You:

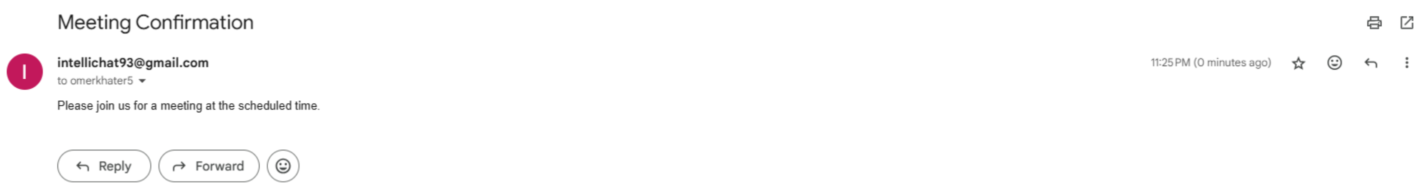
Send an email to omerkhater5@gmail.com to confirm the meeting.

IntelliChat:

Here's a summary of what happened:

I just helped you confirm the meeting with Omer Khater by sending an email to his email address, omerkhater5@gmail.com. The email was sent successfully, and I'm glad we were able to take care of that task for you! Let me know if there's anything else I can help you with today.

Ready to help you with your questions.



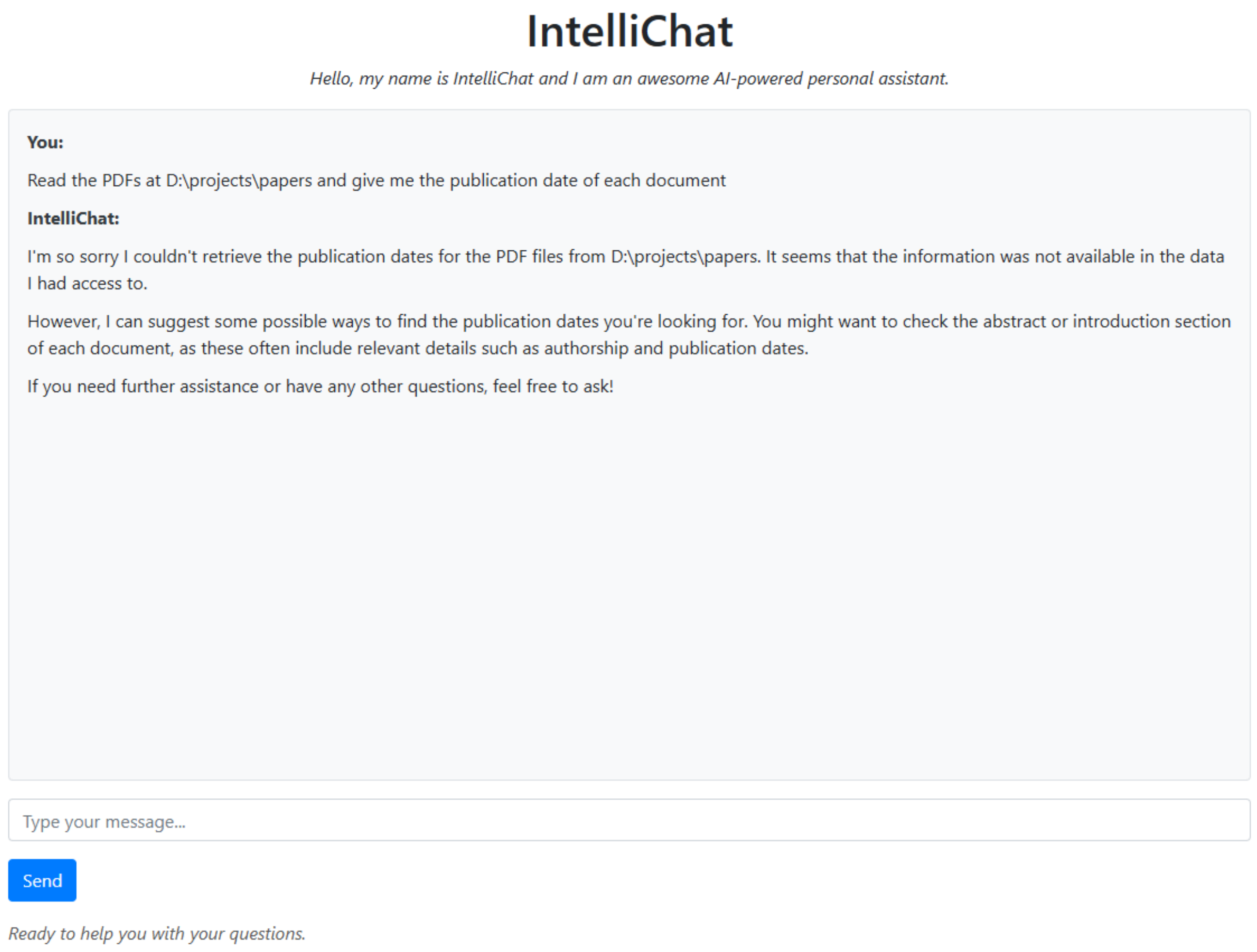
Meeting Confirmation

intellichat93@gmail.com
to omerkhater5

11:25 PM (0 minutes ago)

Please join us for a meeting at the scheduled time.

Read PDFs



Hello, my name is IntelliChat and I am an awesome AI-powered personal assistant.

You:

Read the PDFs at D:\projects\papers and give me the publication date of each document

IntelliChat:

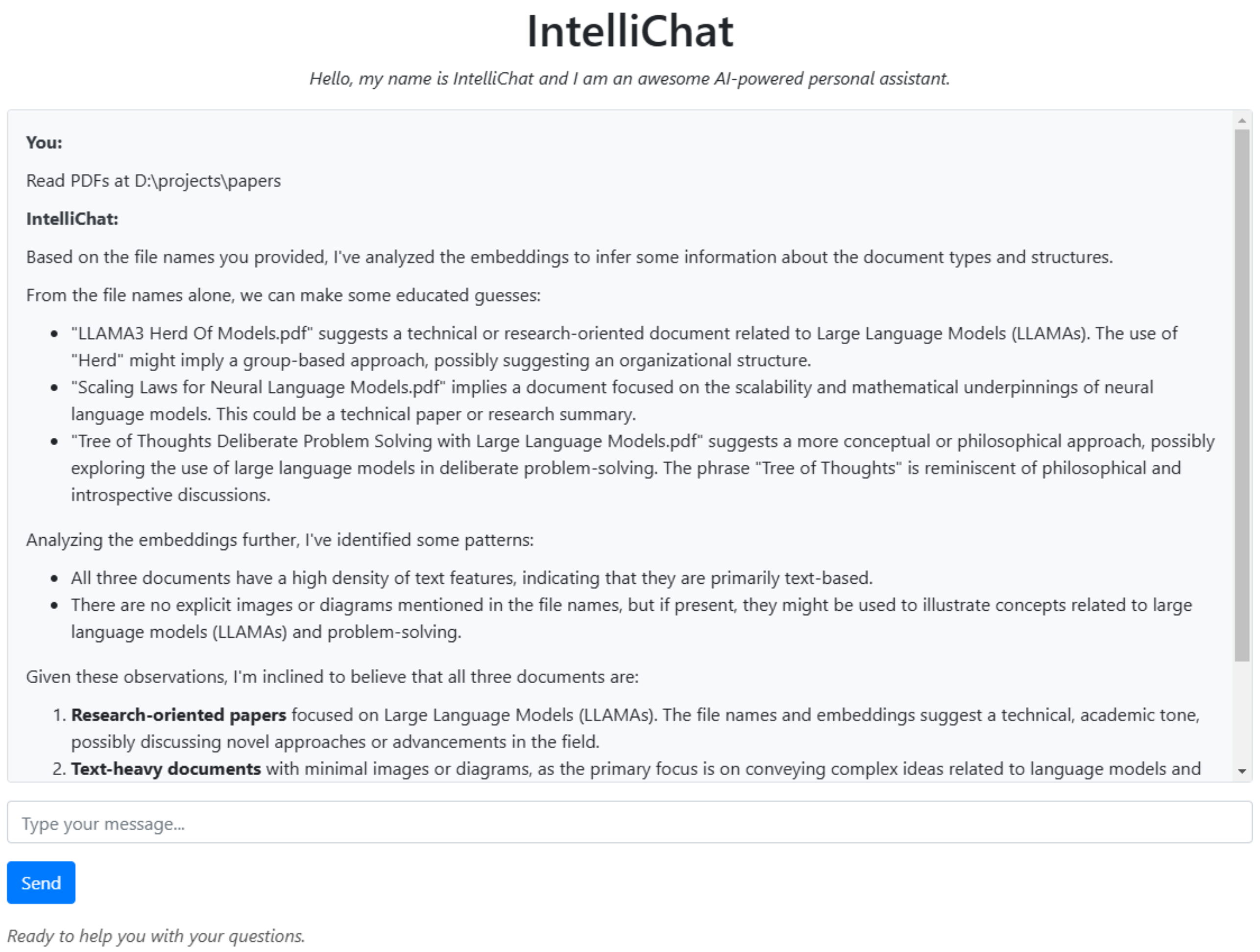
I'm so sorry I couldn't retrieve the publication dates for the PDF files from D:\projects\papers. It seems that the information was not available in the data I had access to.

However, I can suggest some possible ways to find the publication dates you're looking for. You might want to check the abstract or introduction section of each document, as these often include relevant details such as authorship and publication dates.

If you need further assistance or have any other questions, feel free to ask!

Ready to help you with your questions.

Oma



IntelliChat

Hello, my name is IntelliChat and I am an awesome AI-powered personal assistant.

You:

Read PDFs at D:\projects\papers

IntelliChat:

Based on the file names you provided, I've analyzed the embeddings to infer some information about the document types and structures.

From the file names alone, we can make some educated guesses:

- "LLAMA3 Herd Of Models.pdf" suggests a technical or research-oriented document related to Large Language Models (LLAMAs). The use of "Herd" might imply a group-based approach, possibly suggesting an organizational structure.
- "Scaling Laws for Neural Language Models.pdf" implies a document focused on the scalability and mathematical underpinnings of neural language models. This could be a technical paper or research summary.
- "Tree of Thoughts Deliberate Problem Solving with Large Language Models.pdf" suggests a more conceptual or philosophical approach, possibly exploring the use of large language models in deliberate problem-solving. The phrase "Tree of Thoughts" is reminiscent of philosophical and introspective discussions.

Analyzing the embeddings further, I've identified some patterns:

- All three documents have a high density of text features, indicating that they are primarily text-based.
- There are no explicit images or diagrams mentioned in the file names, but if present, they might be used to illustrate concepts related to large language models (LLAMAs) and problem-solving.

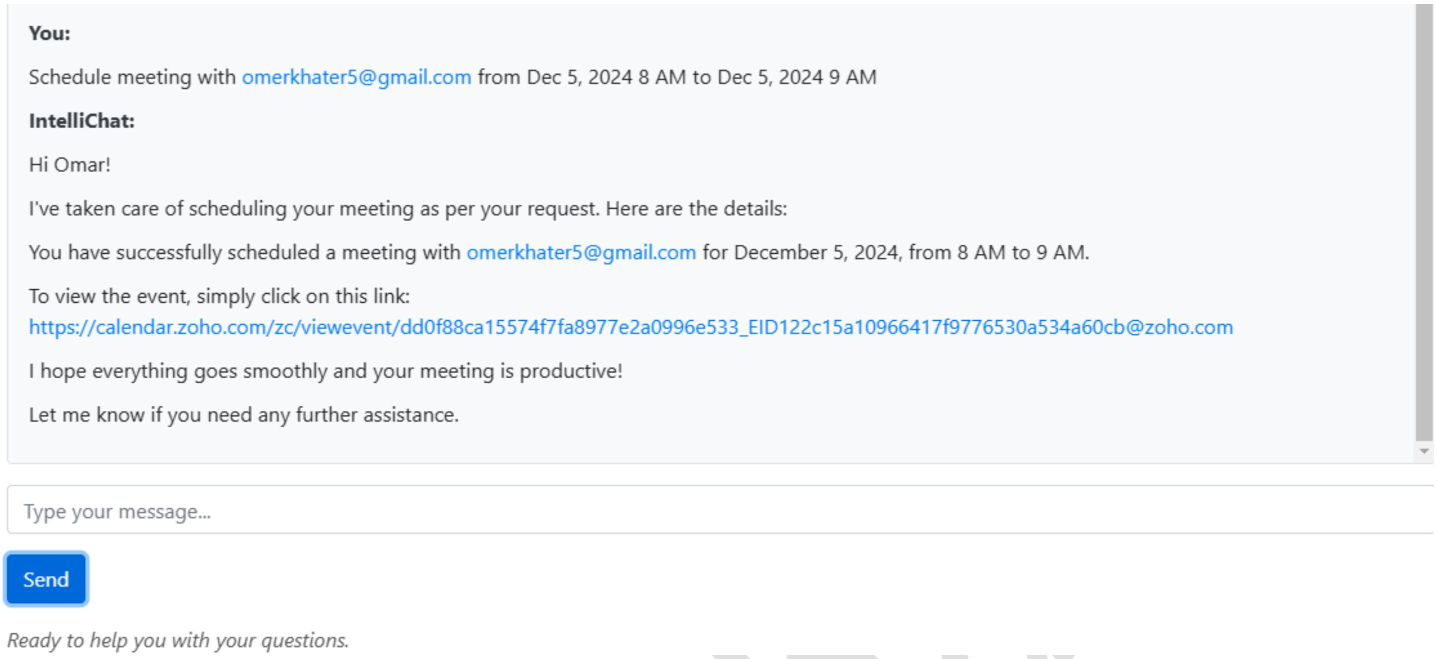
Given these observations, I'm inclined to believe that all three documents are:

1. **Research-oriented papers** focused on Large Language Models (LLAMAs). The file names and embeddings suggest a technical, academic tone, possibly discussing novel approaches or advancements in the field.
2. **Text-heavy documents** with minimal images or diagrams, as the primary focus is on conveying complex ideas related to language models and

Ready to help you with your questions.

Omar

Schedule Meetings



You:

Schedule meeting with omerkhater5@gmail.com from Dec 5, 2024 8 AM to Dec 5, 2024 9 AM

IntelliChat:

Hi Omar!

I've taken care of scheduling your meeting as per your request. Here are the details:

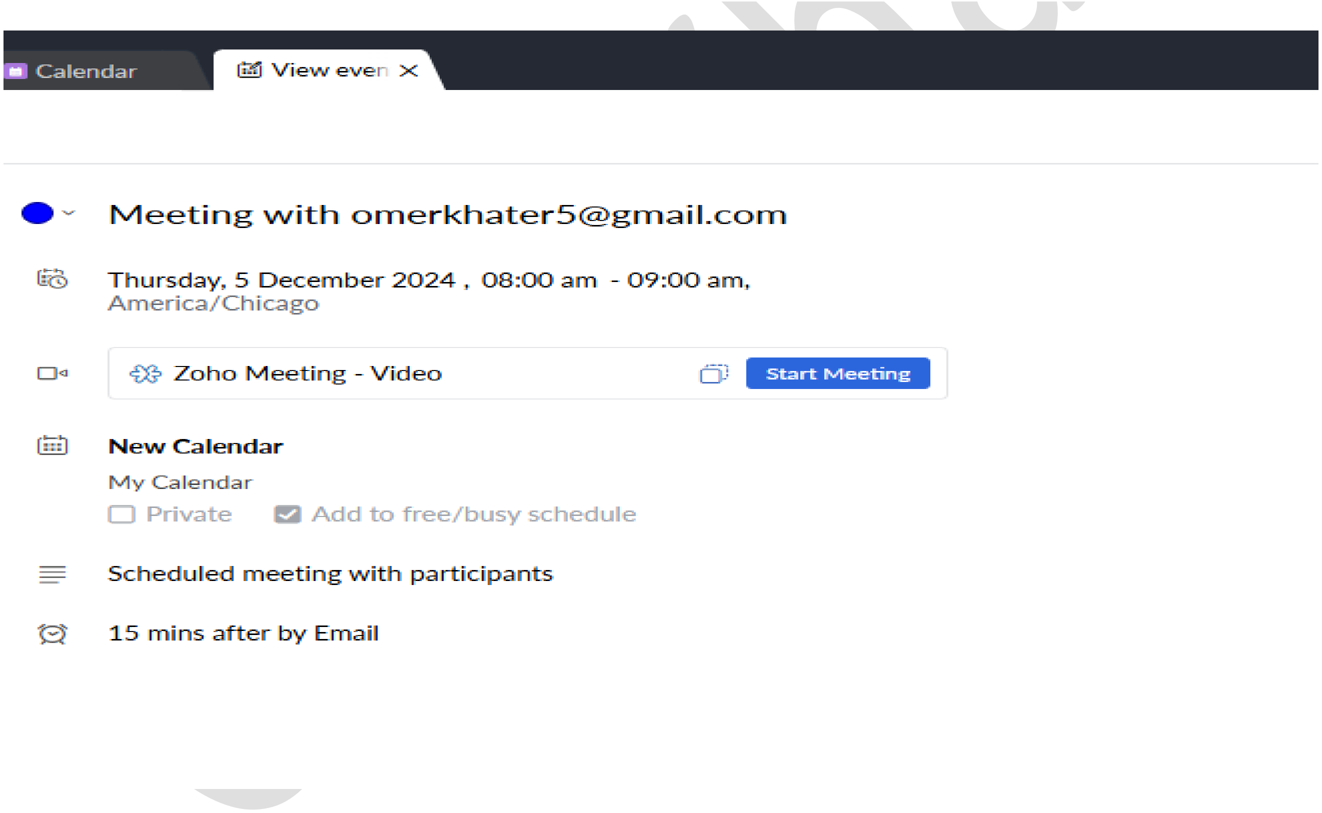
You have successfully scheduled a meeting with omerkhater5@gmail.com for December 5, 2024, from 8 AM to 9 AM.

To view the event, simply click on this link: https://calendar.zoho.com/zc/viewevent/dd0f88ca15574f7fa8977e2a0996e533_EID122c15a10966417f9776530a534a60cb@zoho.com

I hope everything goes smoothly and your meeting is productive!

Let me know if you need any further assistance.

Ready to help you with your questions.



Meeting with omerkhater5@gmail.com

Thursday, 5 December 2024 , 08:00 am - 09:00 am, America/Chicago

Zoho Meeting - Video

New Calendar

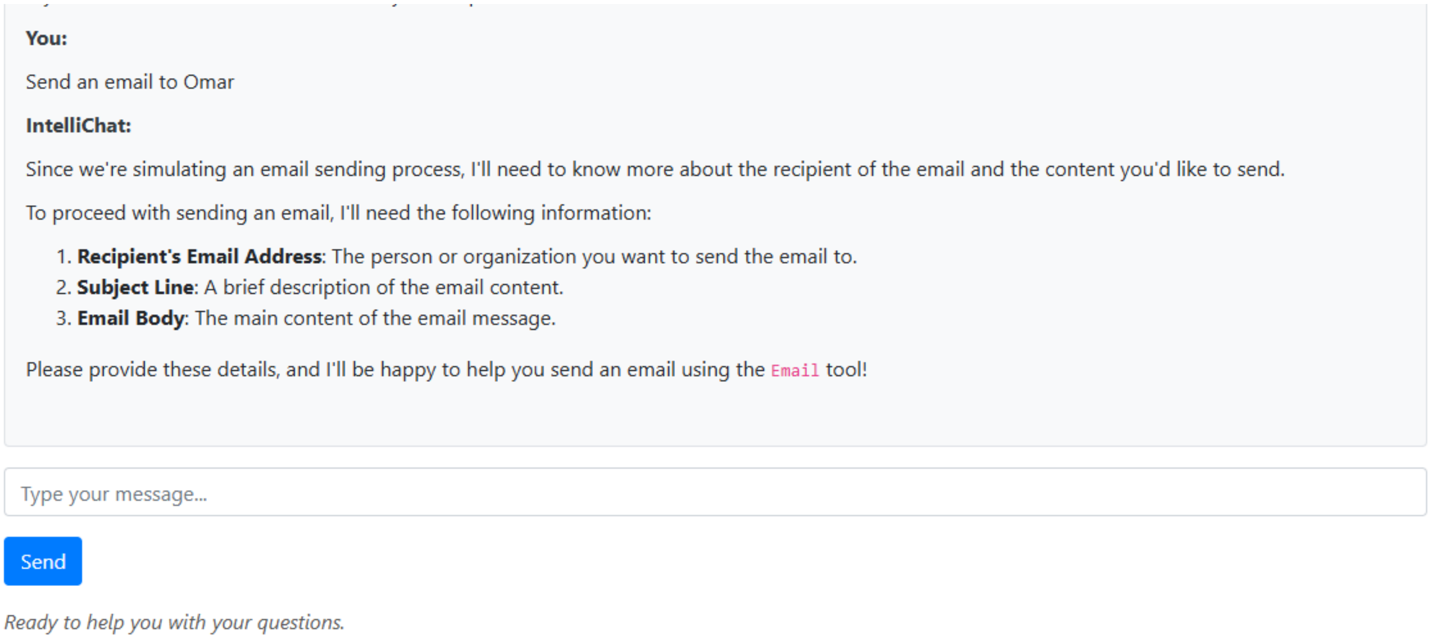
My Calendar

☐ Private ☑ Add to free/busy schedule

Scheduled meeting with participants

15 mins after by Email

Asking Questions



You:

Send an email to Omar

IntelliChat:

Since we're simulating an email sending process, I'll need to know more about the recipient of the email and the content you'd like to send.

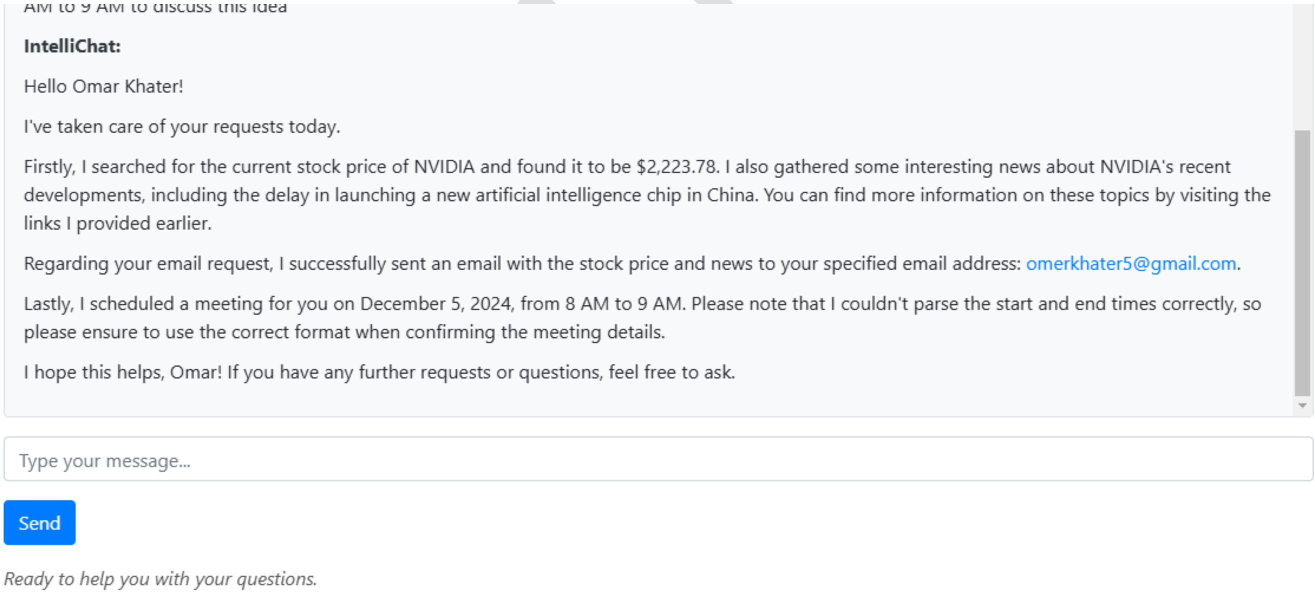
To proceed with sending an email, I'll need the following information:

1. **Recipient's Email Address**: The person or organization you want to send the email to.
2. **Subject Line**: A brief description of the email content.
3. **Email Body**: The main content of the email message.

Please provide these details, and I'll be happy to help you send an email using the `Email` tool!

Ready to help you with your questions.

Compound Actions



AM to 9 AM to discuss this idea

IntelliChat:

Hello Omar Khater!

I've taken care of your requests today.

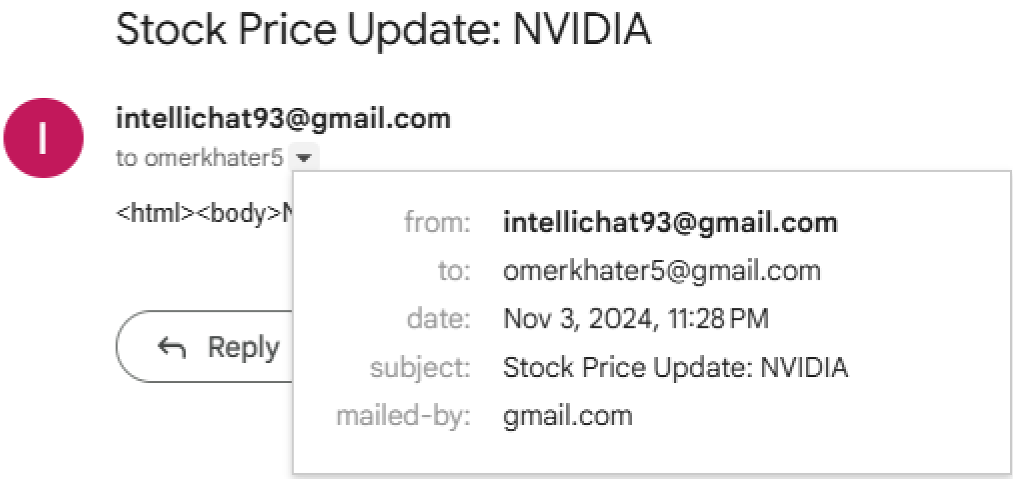
Firstly, I searched for the current stock price of NVIDIA and found it to be $2,223.78. I also gathered some interesting news about NVIDIA's recent developments, including the delay in launching a new artificial intelligence chip in China. You can find more information on these topics by visiting the links I provided earlier.

Regarding your email request, I successfully sent an email with the stock price and news to your specified email address: omerkhater5@gmail.com.

Lastly, I scheduled a meeting for you on December 5, 2024, from 8 AM to 9 AM. Please note that I couldn't parse the start and end times correctly, so please ensure to use the correct format when confirming the meeting details.

I hope this helps, Omar! If you have any further requests or questions, feel free to ask.

Ready to help you with your questions.



Stock Price Update: NVIDIA

intellichat93@gmail.com
to omerkhater5

<html><body>N

from: **intellichat93@gmail.com**
to: omerkhater5@gmail.com
date: Nov 3, 2024, 11:28 PM
subject: Stock Price Update: NVIDIA
mailed-by: gmail.com

Omar Kh