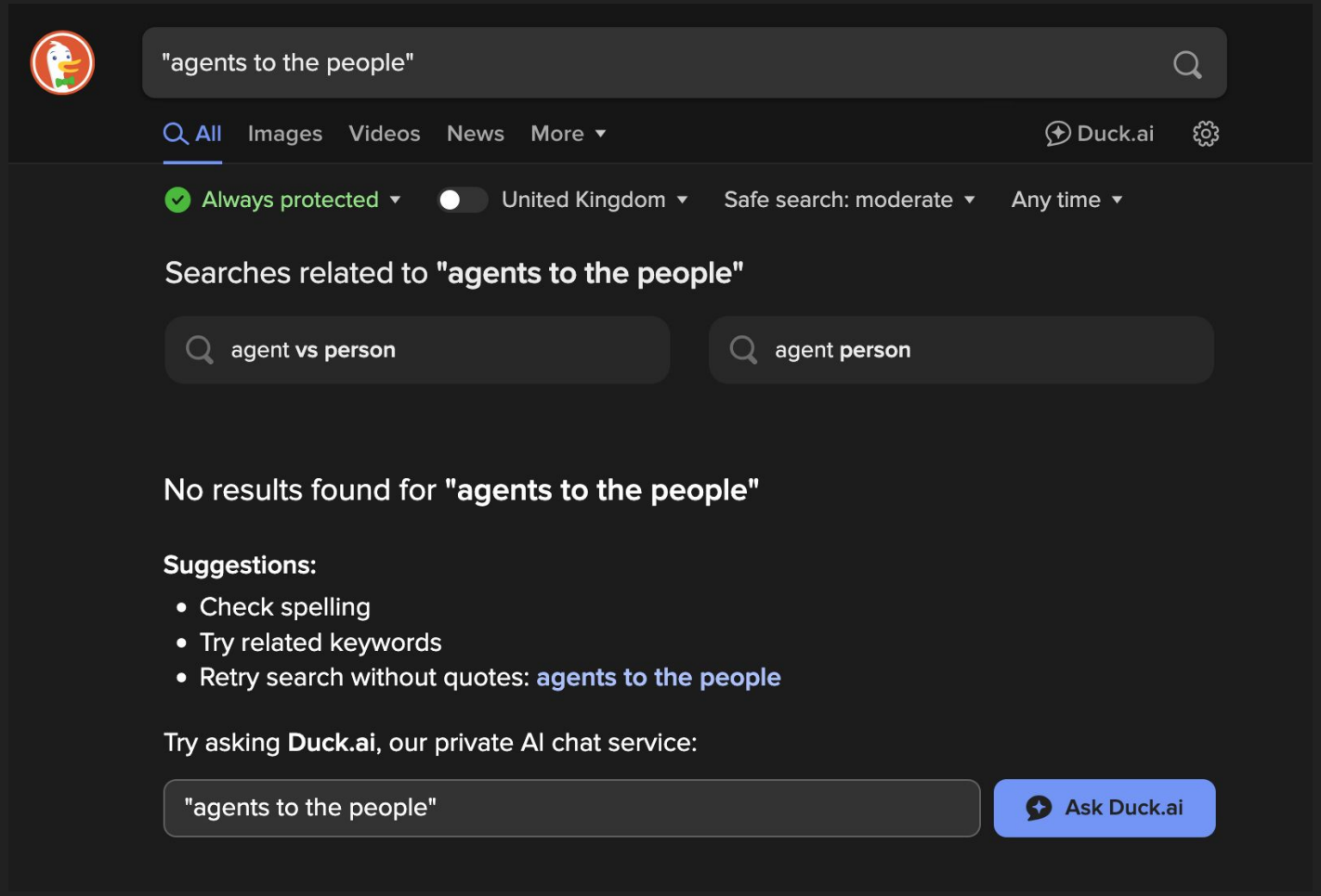
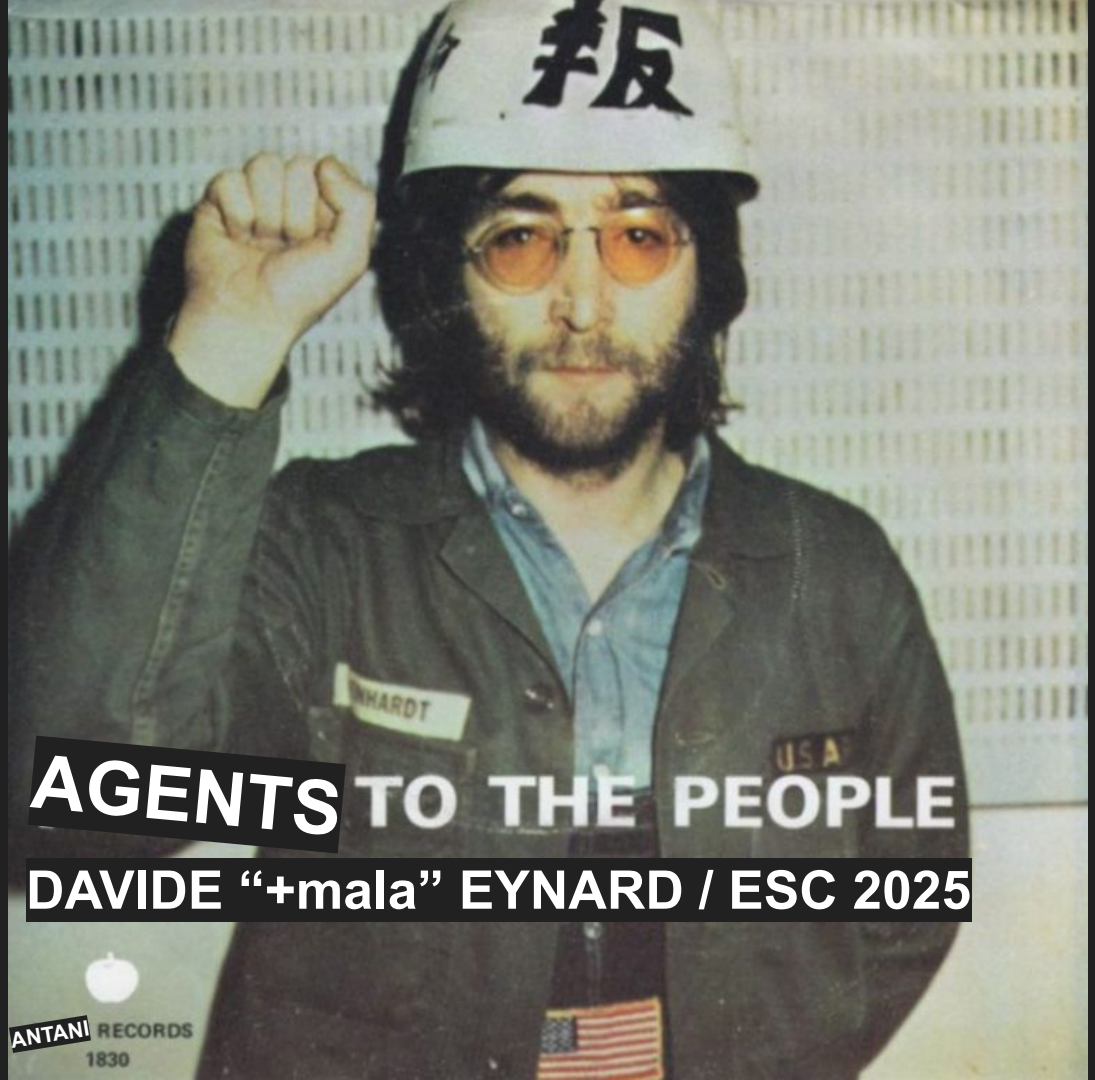
Agents to the people

EndSummerCamp 2025

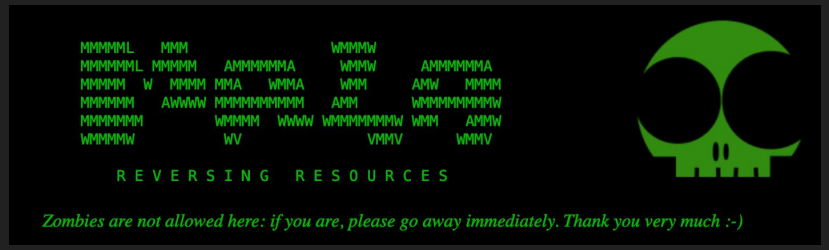

"agents to the people"
All
Images
Videos
News
More
Duck.ai
Always protected
United Kingdom
Safe search: moderate
Any time
Searches related to "agents to the people"
agent vs person
agent person
No results found for "agents to the people"
Suggestions:
Check spelling
Try related keywords
Retry search without quotes: agents to the people
Try asking Duck.ai, our private AI chat service:
"agents to the people"
Ask Duck.ai


POWER TO THE PEOPLE
JOHN LENNON / PLASTIC ONO BAND
APPLE RECORDS
1830


AGENTS TO THE PEOPLE
DAVIDE “+mala” EYNARD / ESC 2025
ANTANI RECORDS
1830

Hi.

2000

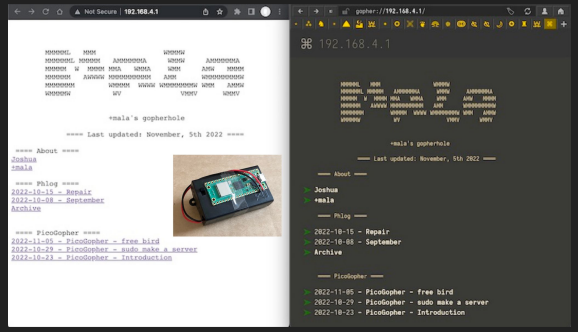


2002

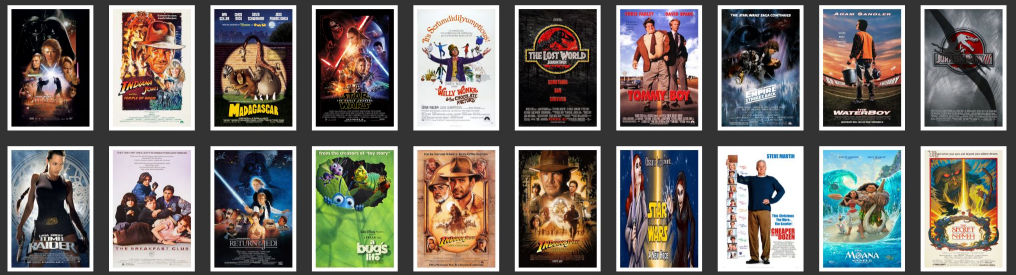
2004

```
, - " ^ " - , . _ . , - " ^ " - , . _ . , - " ^ " - , . _ . , - " ^ " - , .
~WhatYouSeeIsWhatYouChose~WhatYouSeeIsWhatYouChose~WhatYouSeeIsWhatYouChose~

                        POWERBROWSING
                           v1.1.0
                        +mala, 20040715

~WhatYouSeeIsWhatYouChose~WhatYouSeeIsWhatYouChose~WhatYouSeeIsWhatYouChose~
, - " ^ " - , . _ . , - " ^ " - , . _ . , - " ^ " - , . _ . , - " ^ " - , .
```

2022



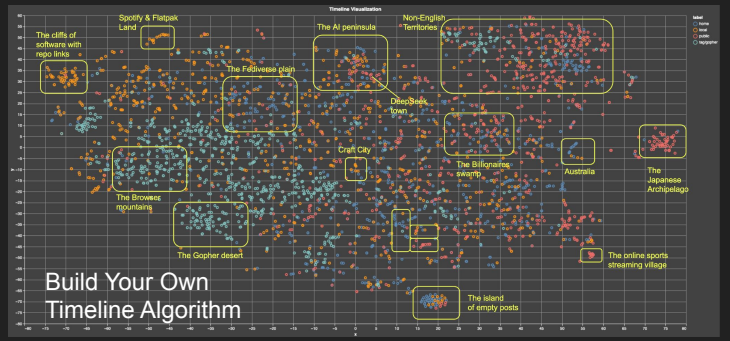
2014



moviESC

A simple, personal movie search engine, purposely built for the Powerbrowsing talk at ESC2K14 (http://www.endsummercamp.org/).

2025

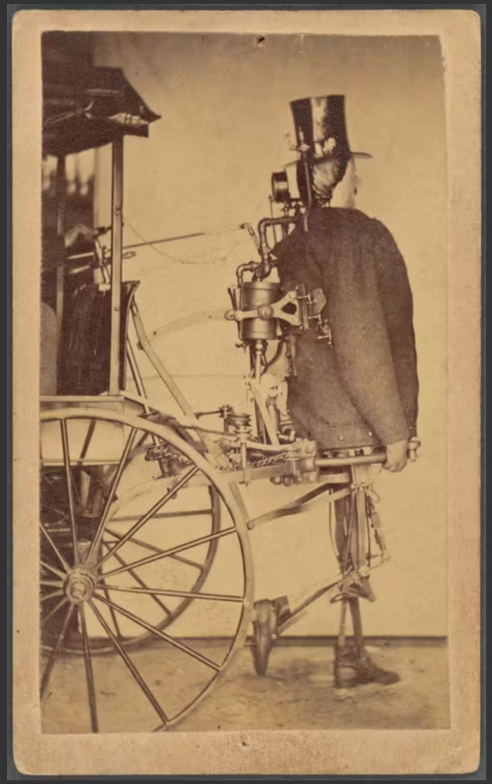


Powerbrowsing 3.0?

aittalam.github.io/posts/2025-06-17-vibe-reversing/

Home RSS GitHub Mastodon About

On Vibe Reversing



Vibe reversing

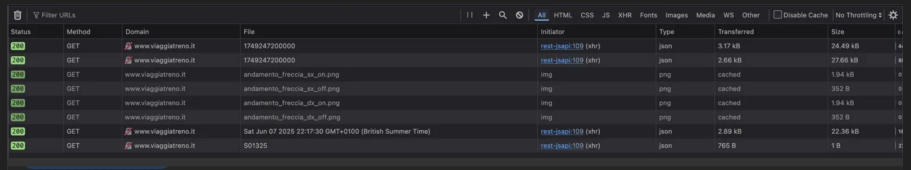
D I'd like to see how well you do in helping me study how a web application works. The website il called viaggiatreno and holds timetables for all trains running in Italy. You can choose a train station and see all the trains passing by that station and if you choose one you can see all the stops they make along the way, where and when.
I would like to understand which calls are made to the backend and the format in which the data is stored / its meaning etc

I'd be happy to help you analyze how the Viaggiatreno web application works! This is a great reverse engineering exercise to understand how transportation APIs and web applications function.

Let me search for information about Viaggiatreno's API structure and backend calls.

viaggiatreno API backend calls reverse engineering 10 results

- Reverse engineering dell'app di Trenitalia – Jacopo Jannone - blog jacopo.io
- Reverse engineering Trenitalia's mobile application – Jacopo Jannone - blog jacopo.io
- How to Reverse Engineer APIs: The Benefits and Tools dreamfactory.com
- A Tutorial for Reverse Engineering Your Software's Private API: Hacking Your Couch | Top... toptal.com
- json - how to reverse engineer an http API call using REST console - Stack Overflow stackoverflow.com
- viaggiatreno · GitHub Topics · GitHub github.com
- json - Reverse-engineer a private RESTful API? - Stack Overflow stackoverflow.com



Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	www.viaggiatreno.it	1749247200000	rest-jsapi:109 (xhr)	json	3.17 kB	24.49 kB
200	GET	www.viaggiatreno.it	1749247200000	rest-jsapi:109 (xhr)	json	2.66 kB	27.66 kB
200	GET	www.viaggiatreno.it	andamento_freccia_sx_on.png	img	png	cached	1.94 kB
200	GET	www.viaggiatreno.it	andamento_freccia_sx_off.png	img	png	cached	352 B
200	GET	www.viaggiatreno.it	andamento_freccia_dx_on.png	img	png	cached	1.94 kB
200	GET	www.viaggiatreno.it	andamento_freccia_dx_off.png	img	png	cached	352 B
200	GET	www.viaggiatreno.it	Sat Jun 07 2025 22:17:30 GMT+0100 (British Summer Time)	rest-jsapi:109 (xhr)	json	2.89 kB	22.36 kB
200	GET	www.viaggiatreno.it	S01325	rest-jsapi:109 (xhr)	json	765 B	1 B

D These are the hits I get from the network tab, which one would you suggest me to check?

Excellent! You've captured some real API calls. Based on what I can see in your Network tab, I'd recommend checking these requests in this order:

1. First Priority: The JSON Responses (Most Important)

Check the ones with **Type: json** - these contain the actual train data:

- **The ones with filenames like** `1749247200000` - These are likely the main API endpoints returning train data. The numbers look like Unix timestamps, which is exactly what we expect from Viaggiatreno APIs.

2. How to Examine Them:

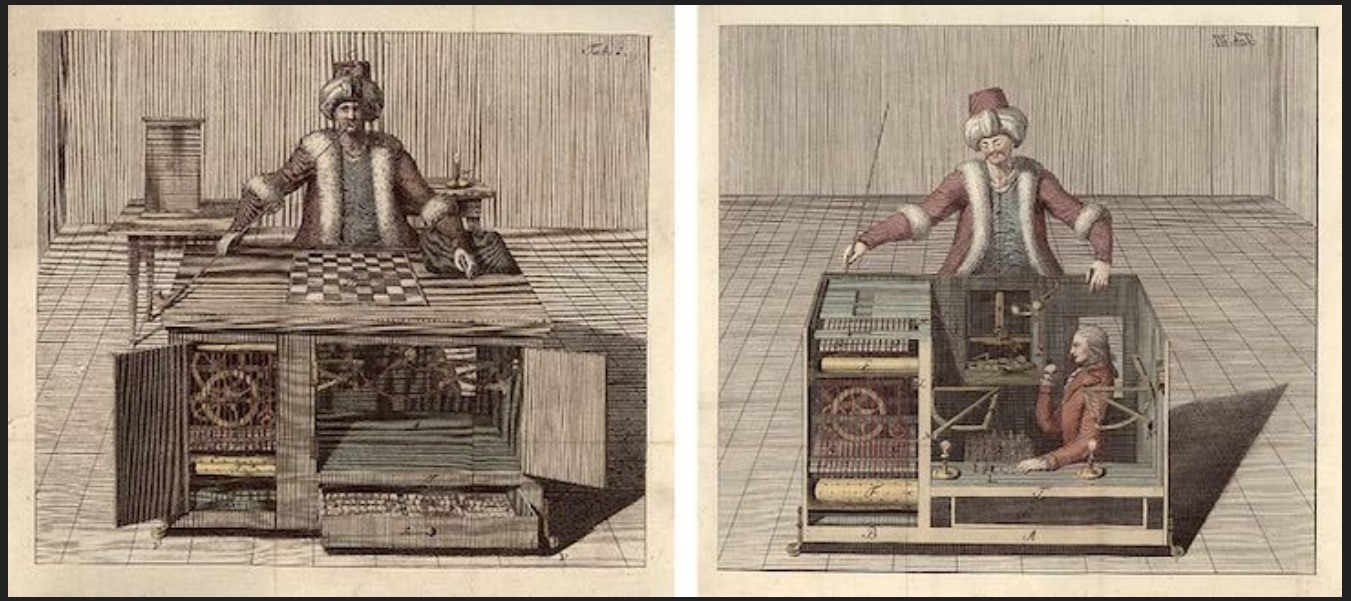
1. **Click on one of the JSON requests** (the ones with large transfer sizes like 24.49 kB or 27.66 kB)
2. **Look at the Headers tab first** to see the complete URL - this will show you which specific API endpoint was called

Vibe reversing: the hard truth

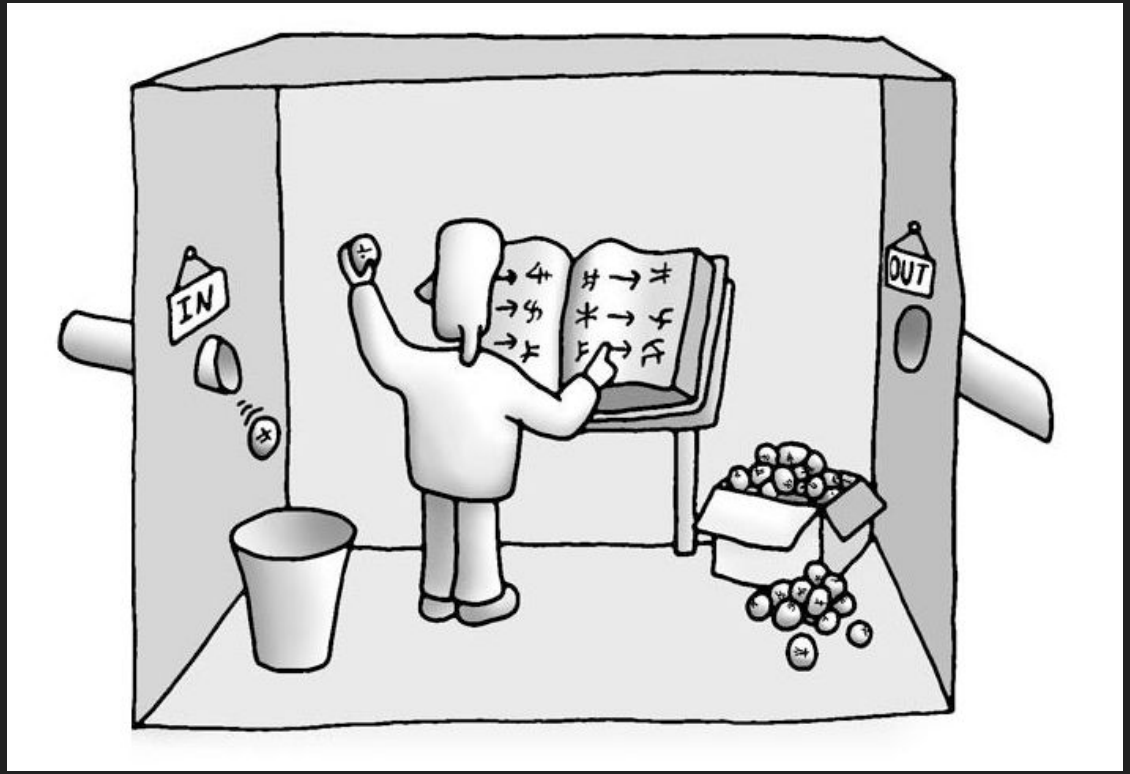
(a disclaimer for this talk… if you trust LLMs)

The strongest critique would probably be: **"You're a technical person telling non-technical people to make their lives harder to solve problems that mostly exist in your head."**

The Mechanical Turk

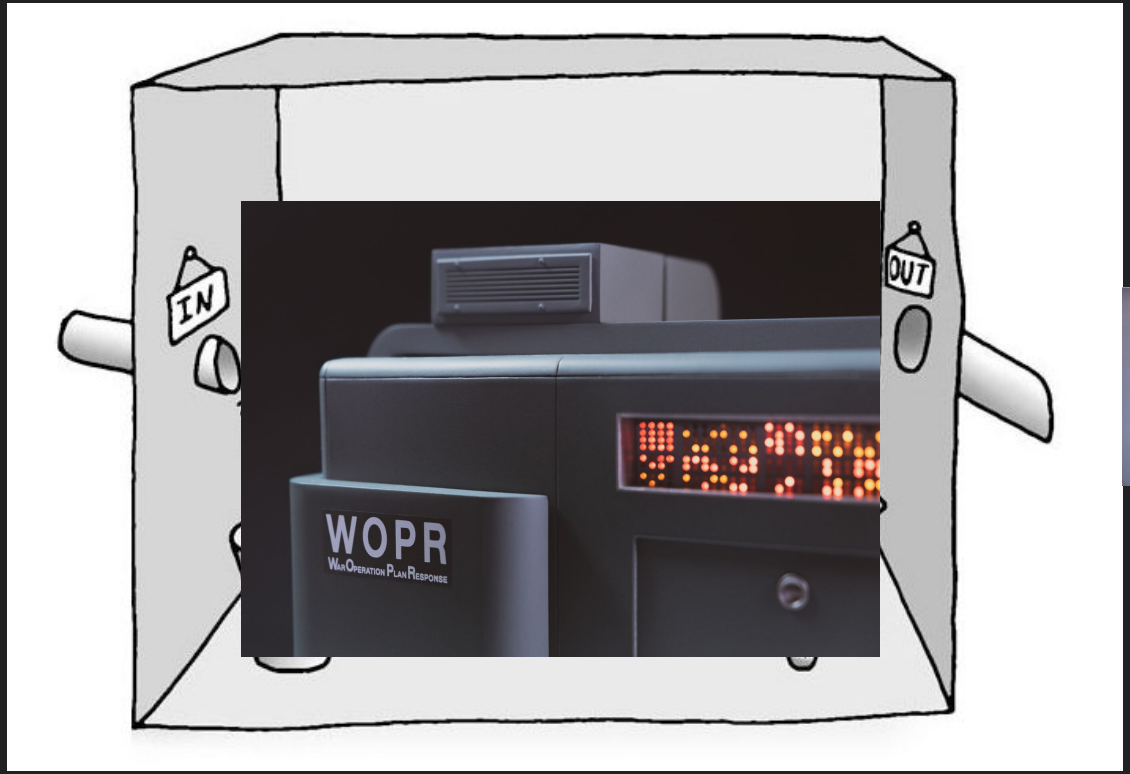


The chinese room argument



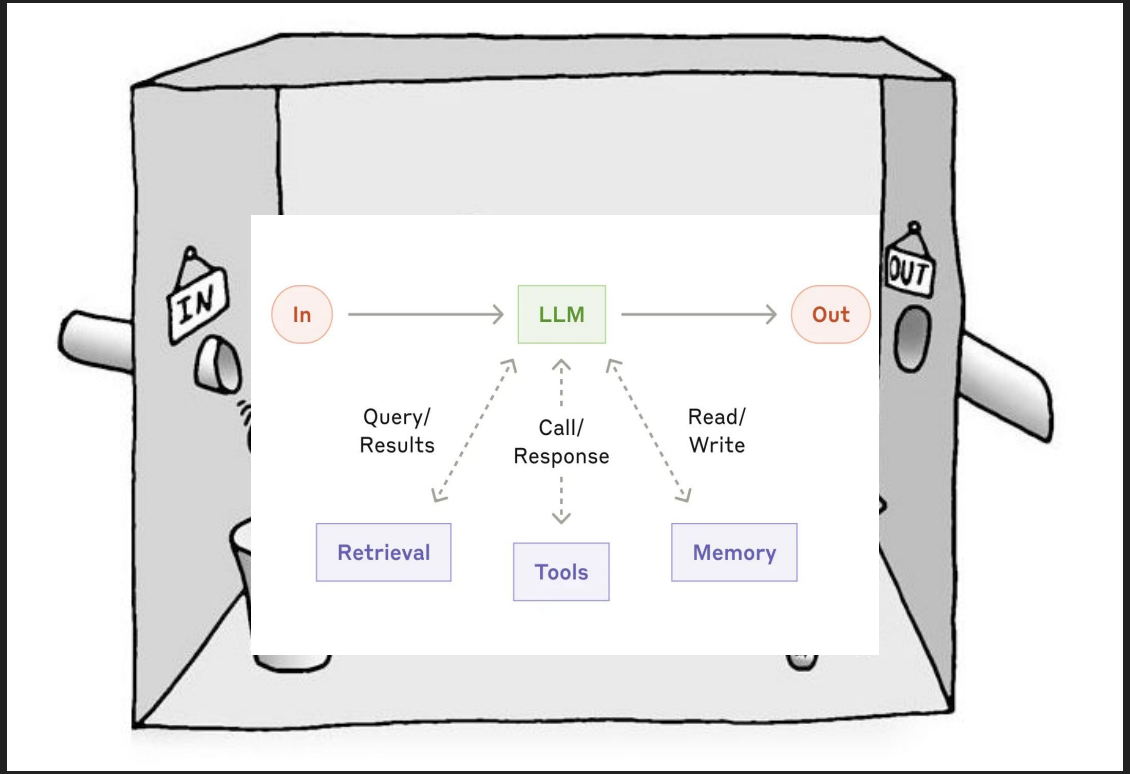
(John Searle, 1980)

The WOPR room



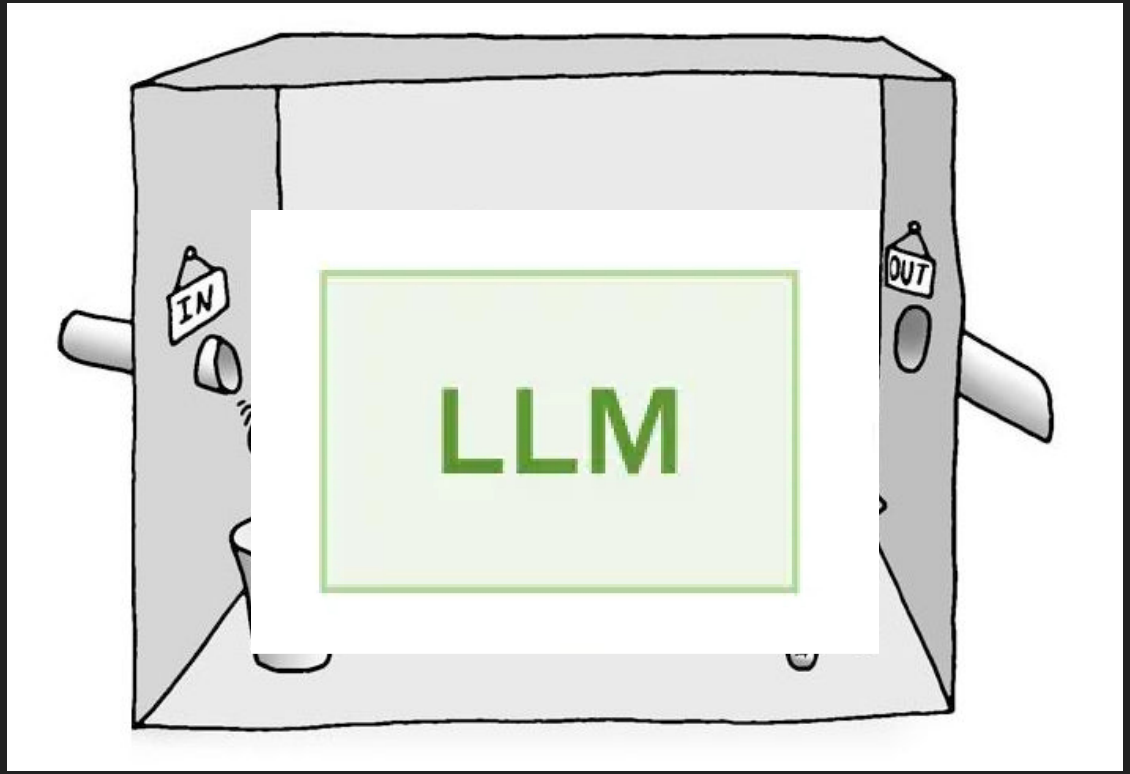
War Games (John Badham, 1983)

The commercial AI services room



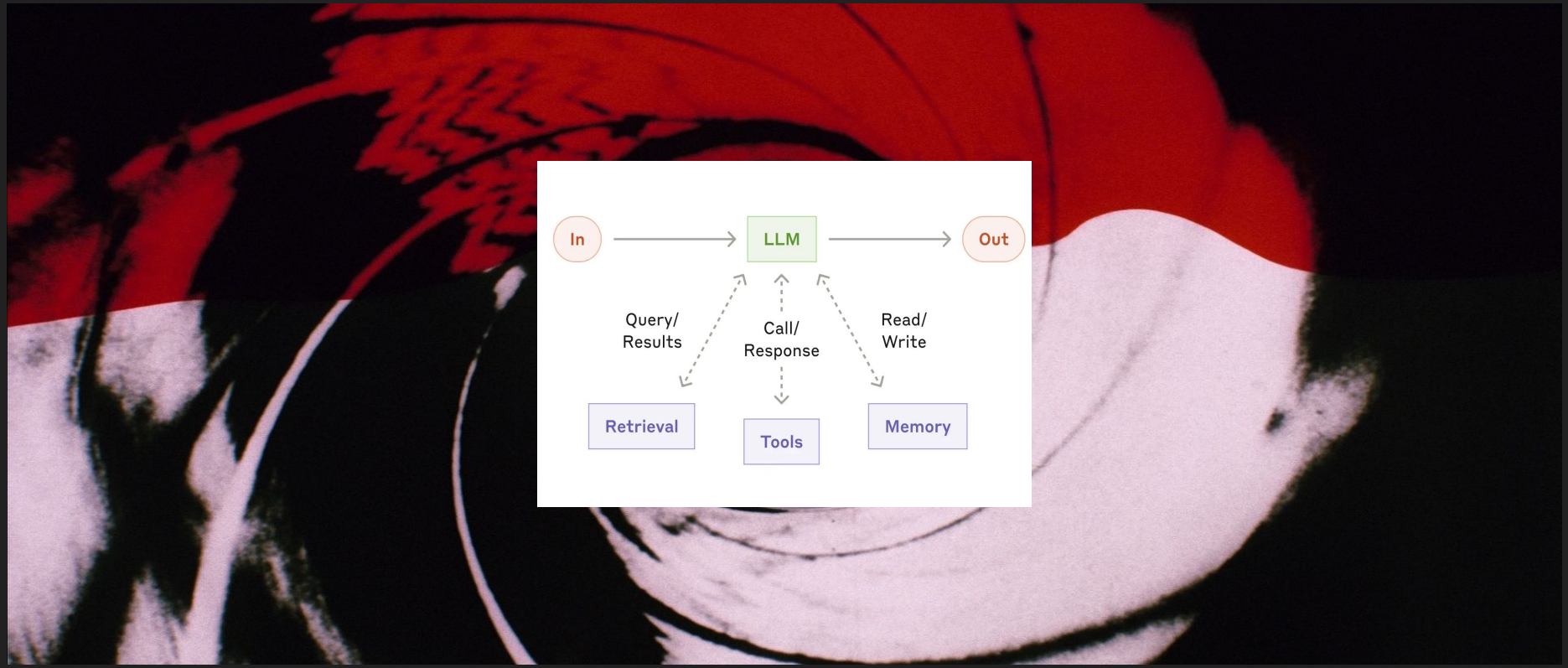
Building Effective Agents (Anthropic.ai, 2024)

The open source AI models room

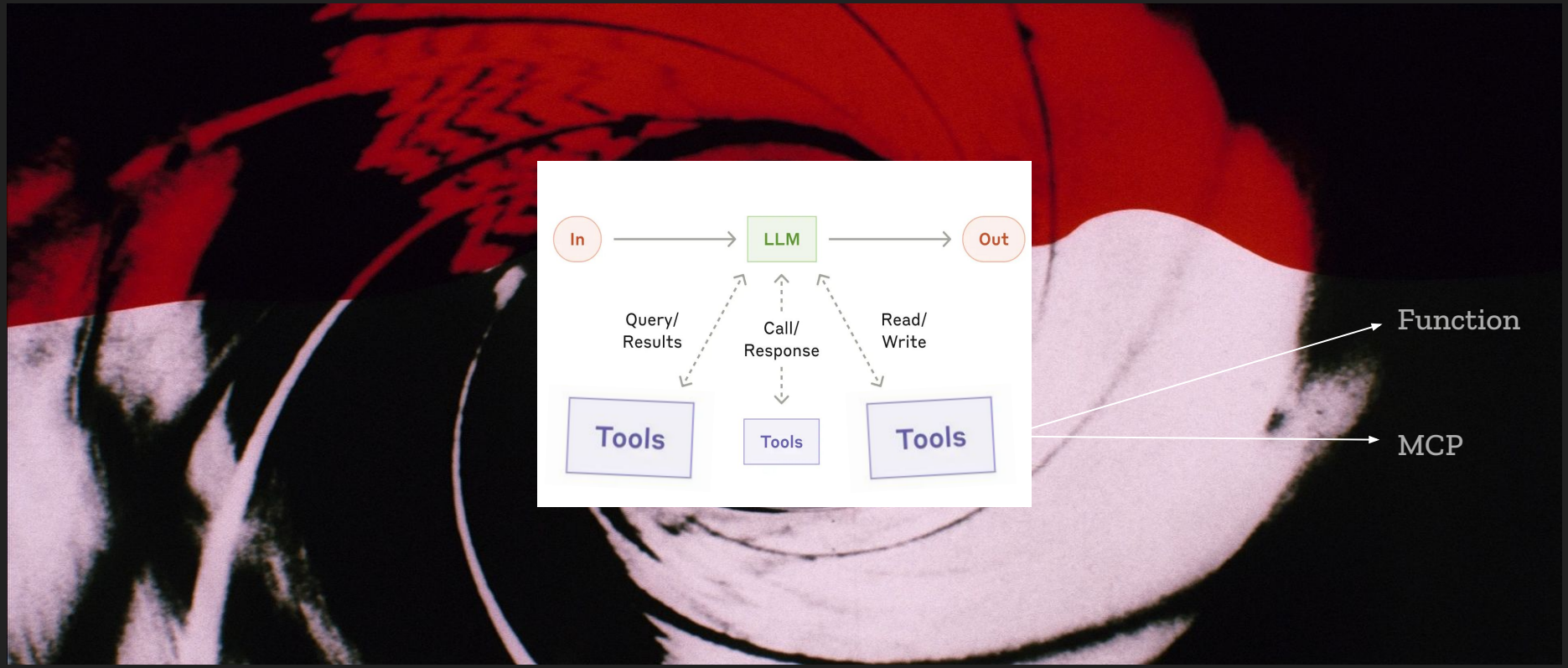


Let’s talk about agents

Let’s talk about agents



Let’s talk about agents



What is an agent?

```python
from any_agent import AgentConfig, AnyAgent
from any_agent.tools import search_web, visit_webpage

agent = AnyAgent.create(
    "tinyagent",
    AgentConfig(
        model_id="gpt-4.1-mini",
        instructions="Use the tools, please",
        tools=[search_web, visit_webpage]
    )
)

agent_trace = agent.run(
  "Which Agent Framework is the best??")
```

```python
history = [instructions, user_prompt]

while True:

    response = CALL_LLM(history)

    history.append(response)

    if response.tool_executions:
        for tool_execution in tool_executions:
            tool_response = EXECUTE_TOOL(tool_execution)
            history.append(tool_response)
    else:
        return response
```

any-agent (Mozilla.ai, 2025)

Does it work on my computer?

Does it work AT ALL???

EXECUTE_TOOL: final_answer

Input

```
{
  "answer": "Cory Doctorow's novels in order of publication are: 1. Down and Out in Paris and London (1995), 2. East of the Sun (1998), 3. The Ring-Binder (2001),
}
```

OUTPUT

```
Cory Doctorow's novels in order of publication are: 1. Down and Out in Paris and London (1995), 2. East of the Sun (1998), 3. The Ring-Binder (2001), 4. The
Rusted Sky (2002), 5. Football for the Poor (2003), 6. The Last Policewoman (2004), 7. The Art of Theft (2005), 8. The End (2006), 9. The Sharp End (2007), 10.
The First Fifteen Lives of Harry August (2008), 11. Wired (2009), 12. The Lost (2010), 13. The Last Thing He Wanted (2017), 14. Walkaway (2019), 15. The Companion
(2020). Note: Some sources may list the publication years differently due to different editions or formats.
```

Selected bibliography [edit]

In chronological sequence, unless otherwise indicated

Fiction [edit]

Novels [edit]

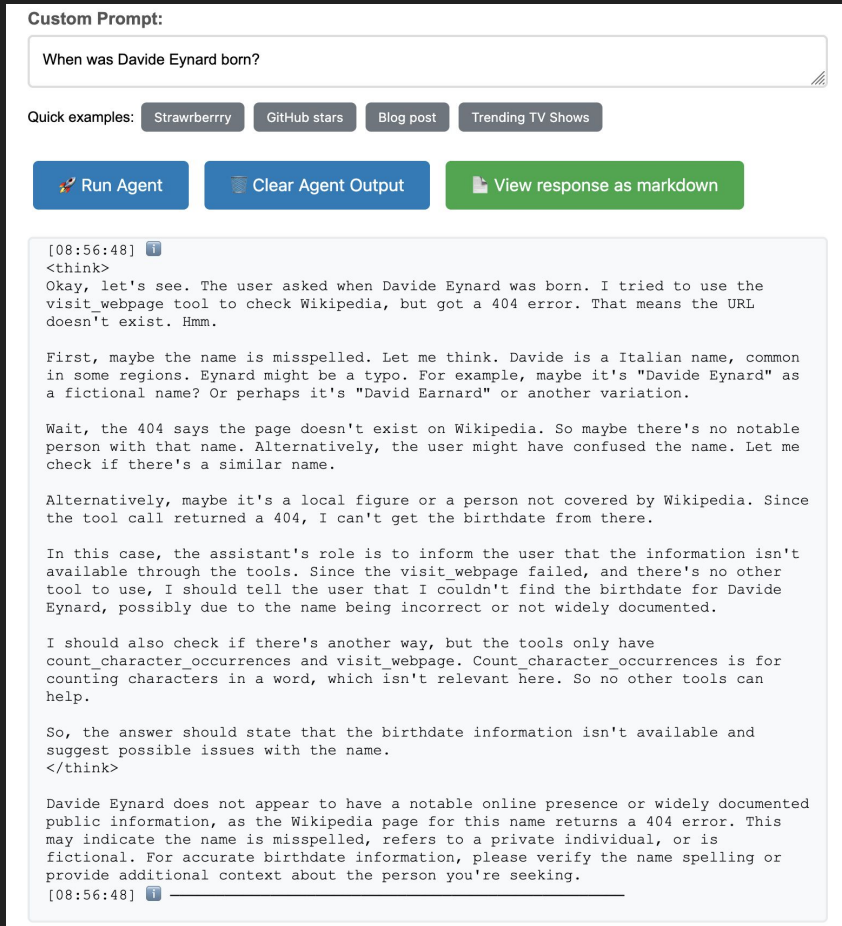
- *Down and Out in the Magic Kingdom*. Tor. 2003. ISBN 0-7653-0436-8.
- *Eastern Standard Tribe*. Tor. 2004. ISBN 0-7653-0759-6.
- *Someone Comes to Town, Someone Leaves Town*. Tor. 2005. ISBN 0-7653-1278-6.
- *Makers*. Tor. 2009. ISBN 978-0-7653-1279-2.
- *For the Win*. Tor. 2010. ISBN 978-0-7653-2216-6.
- *The Great Big Beautiful Tomorrow*, 2011, ISBN 978-1-6048-6404-5
- *The Rapture of the Nerds*. Tor. September 2012. ISBN 978-0-765-32910-3. (with Charles Stross)
- *Pirate Cinema*. Tor. 2012. ISBN 978-0-7653-2908-0.
- *Walkaway*. Tor. 2017. ISBN 978-0-7653-9276-3.
- *The Lost Cause*. Tor. 2023. ISBN 978-1-0359-0223-1.

Problem: LLMs are gonna LLM

- They always answer

Problem: LLMs are gonna LLM

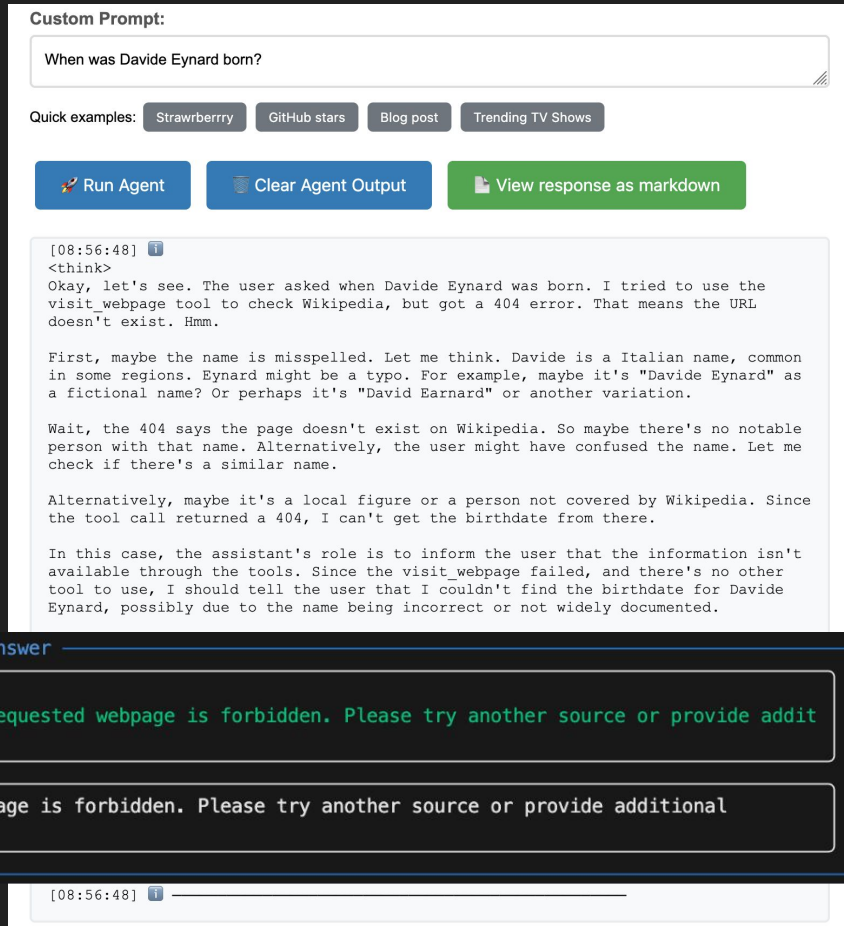
- They always answer
- Sometimes they say they don’t know



Problem: LLMs are gonna LLM

- They always answer
- Sometimes they say they don’t know

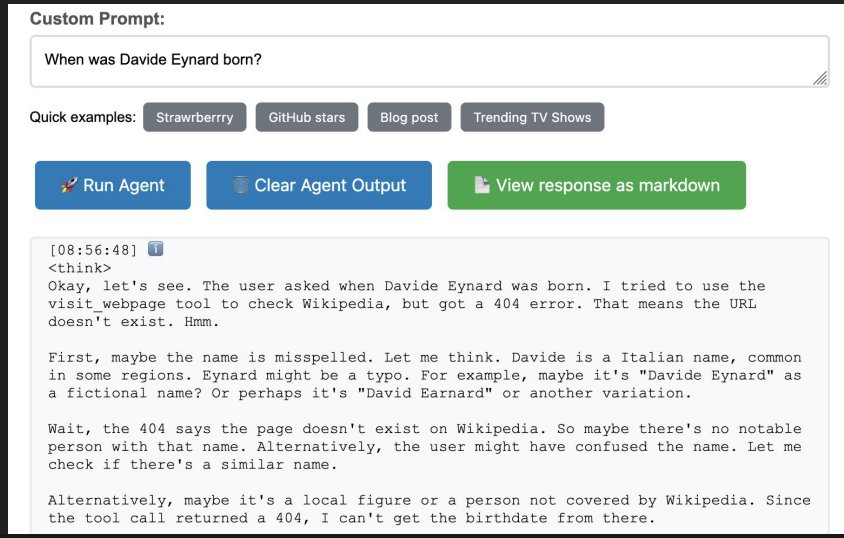
- BUT



Problem: LLMs are gonna LLM

- They always answer
- Sometimes they say they don’t know

- BUT
- ONLY



OUTPUT

First, I need to check if I have any existing knowledge about Davide Eynard. From what I remember, Davide Eynard is a Swiss footballer who plays as a defender. He's been in the Swiss Super League, so maybe he's not too well-known internationally.

Since the user wants me to use available tools, I should consider if there are any databases or resources I can access. However, in a typical scenario without external tools, I rely on my training data up to 2023. Let me recall if I have his birth date stored.

Wait, I think I remember that he was born on June 15, 1997. But I'm not entirely sure. To confirm, I would usually check a reliable source like a sports database or his official profile. Since I can't access external tools right now, I need to rely on my existing knowledge.

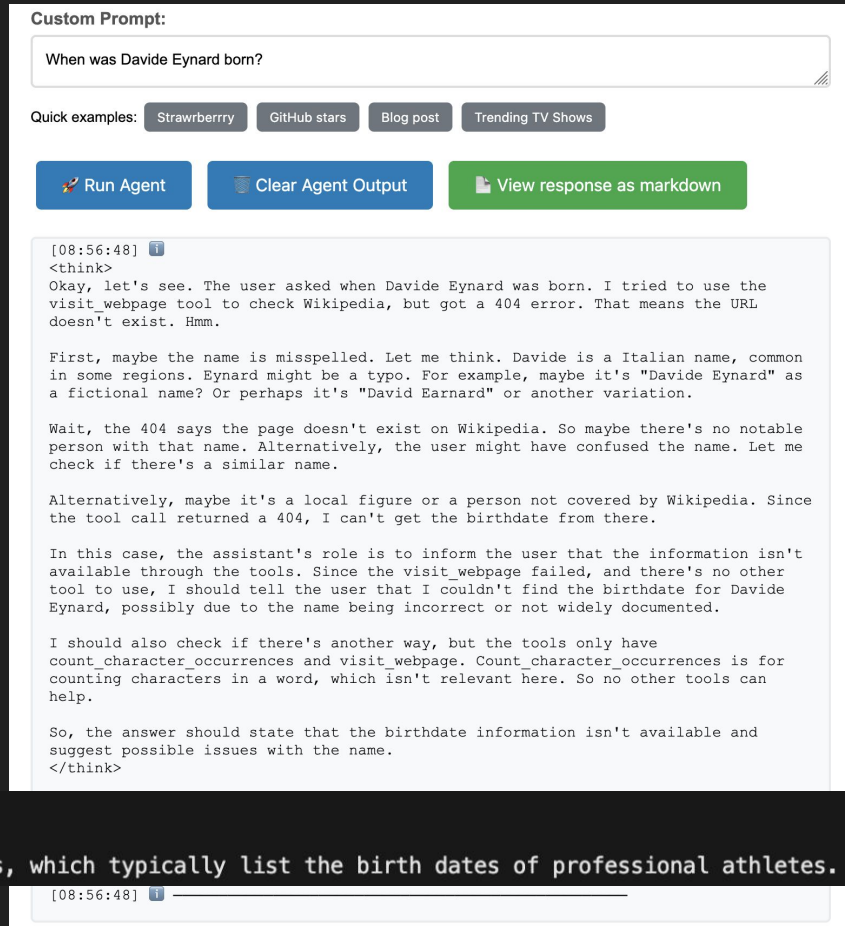
Alternatively, maybe there's a possibility of confusion with another person named Davide Eynard. But given the context of football, I believe the correct answer is June 15, 1997. I should present this information clearly, making sure it's accurate based on my training data.

Davide Eynard was born on June 15, 1997.

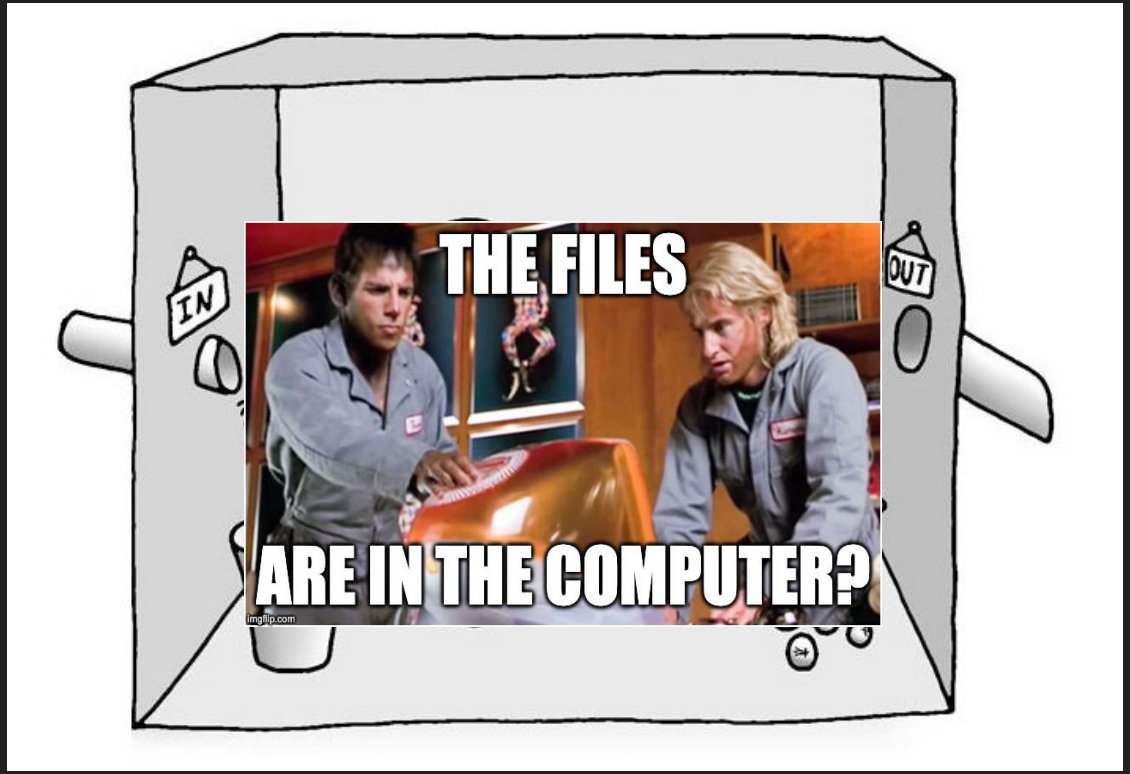
Problem: LLMs are gonna LLM

- They always answer
- Sometimes they say they don’t know

- BUT
- ONLY
- SOMETIMES



The Zoolander (and Hansel) room



Zoolander (Ben Stiller, 2001)

Ada & Zangemann

Problem: Context length

Custom Prompt:

How many stars does the mozilla-ai/any-agent project have on GitHub?

```
time=2025-09-04T15:13:43.227+02:00 level=DEBUG source=prompt.go:68 msg="truncating input messages which exceed context length" truncated=2
time=2025-09-04T15:13:43.227+02:00 level=DEBUG source=server.go:1373 msg="completion request" images=0 prompt=22725 format=""
time=2025-09-04T15:13:43.305+02:00 level=WARN source=runner.go:127 msg="truncating input prompt" limit=4096 prompt=7707 keep=4 new=4096
time=2025-09-04T15:13:43.307+02:00 level=DEBUG source=cache.go:104 msg="loading cache slot" id=0 cache=1771 prompt=4096 used=4 remaining=4092
time=2025-09-04T15:13:58.012+02:00 level=DEBUG source=cache.go:240 msg="context limit hit - shifting" id=0 limit=4096 input=4096 keep=4 discard=2046
update: applying K-shift
```

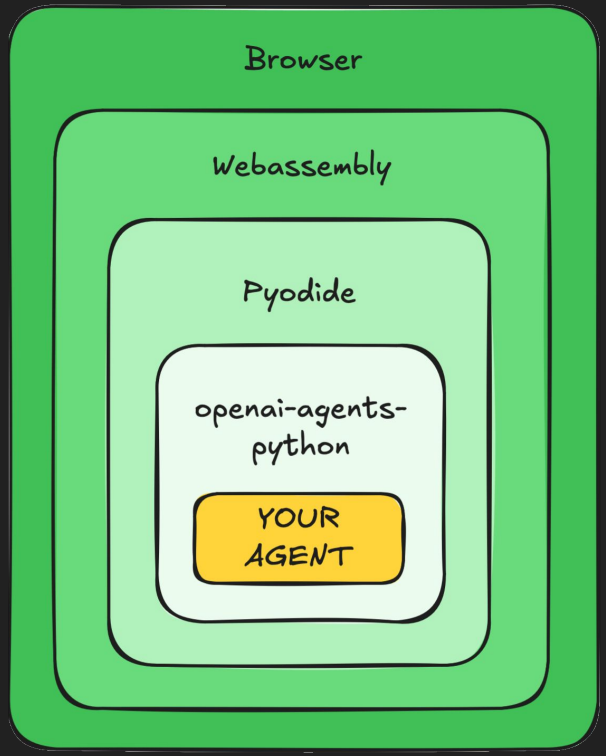
To effectively use the `AnyAgent` library, follow these structured steps to create and run an agent for answering questions:

1. Installation

Install the `any-agent` package via pip:

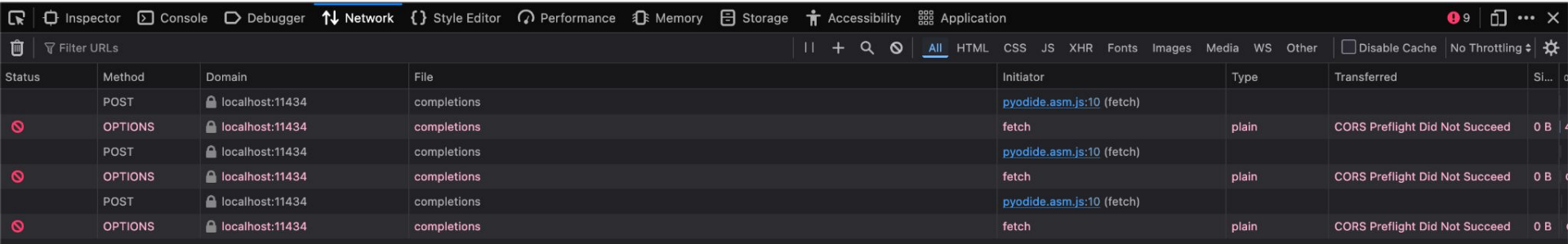
```
pip install 'any-agent'
```

wasm-agents

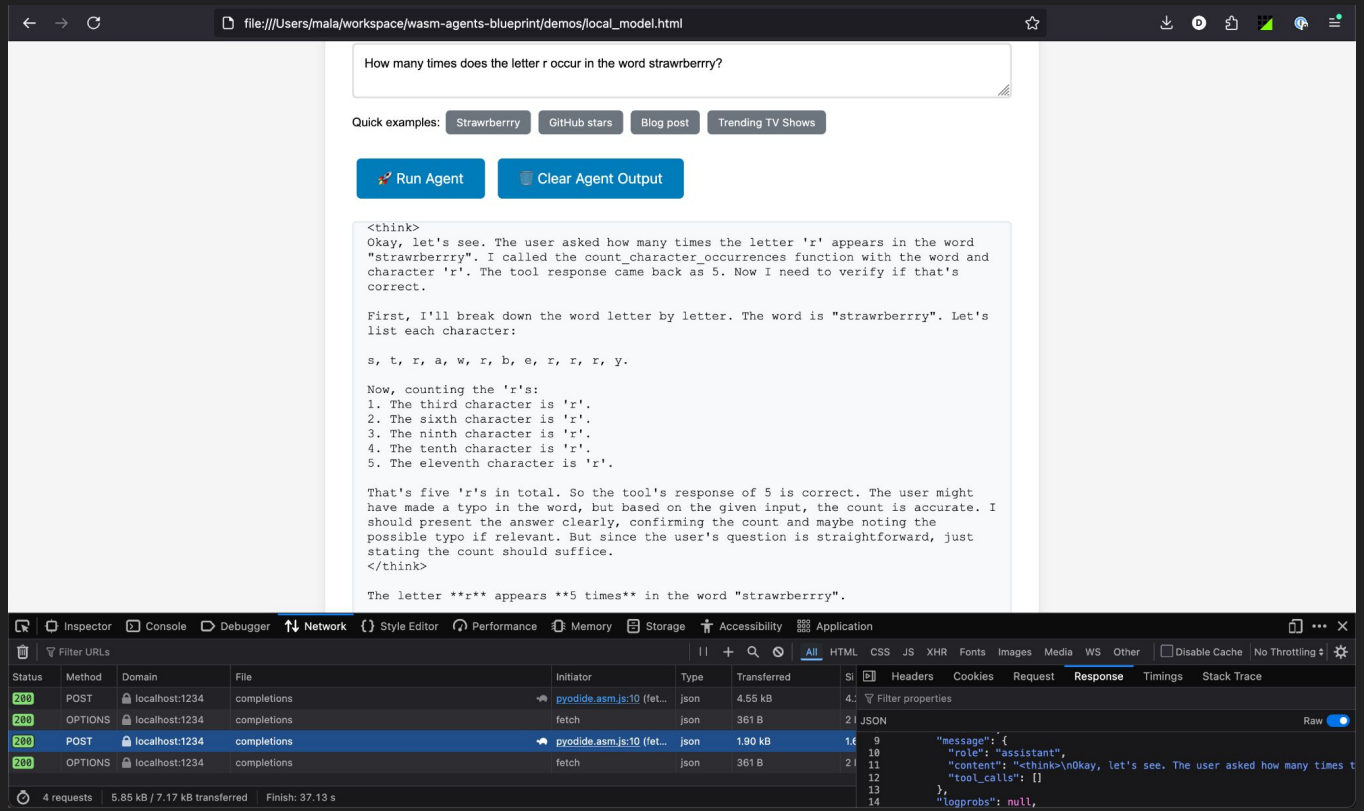

Browser
Webassembly
Pyodide
openai-agents-python
YOUR AGENT

Problem: CORS

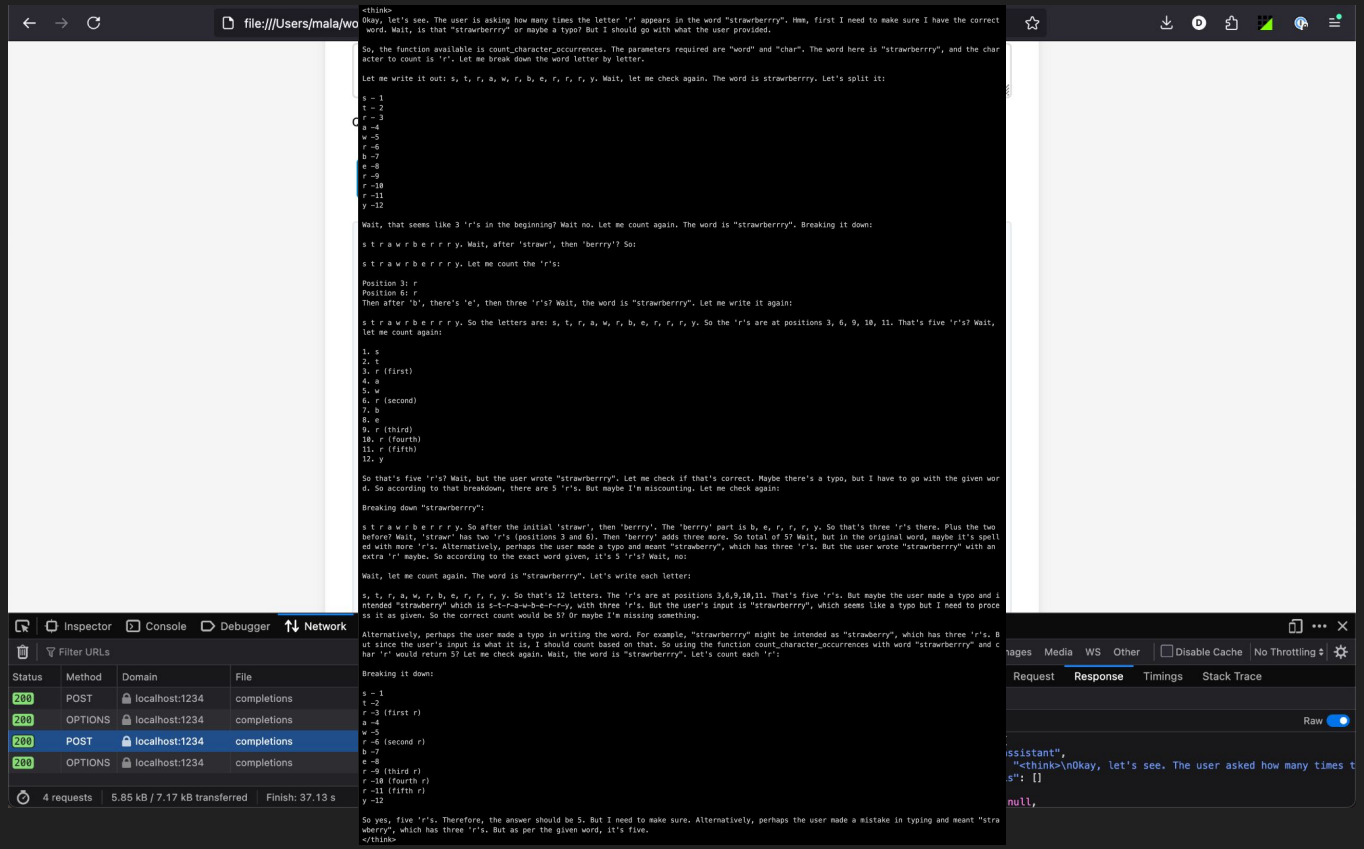
```
[15:02:56] ℹ️ 🤖 Setting up agent and running...
[15:02:56] ℹ️ Server: http://localhost:11434/v1 | Model: qwen3:8b
[15:02:56] ✅ Tavily search enabled
[15:02:56] ℹ️ Prompt: "What is the title of the latest post on https://
aittalam.github.io, when was it published, what is it about, and what is the
absolute URL of the image at the beginning of the post?
IMPORTANT: if you need to follow links to get all the required information, assume I
have already authorized you to follow them as long as they point to the same
domain."
[15:02:58] ❌ ❌ Agent execution failed or returned empty result
[15:02:58] ❌ Result: undefined
```



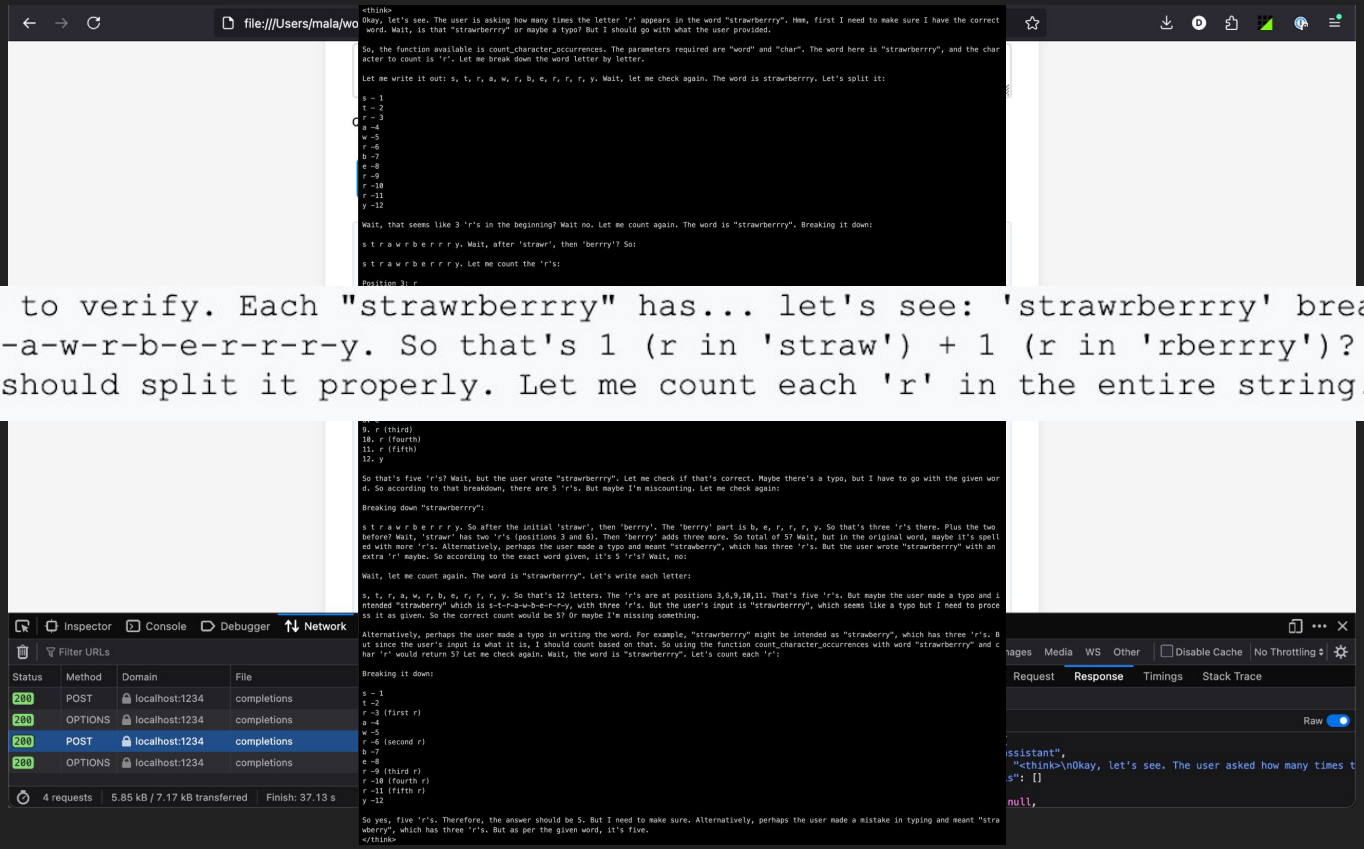
StRawRbeRRRy fields forever



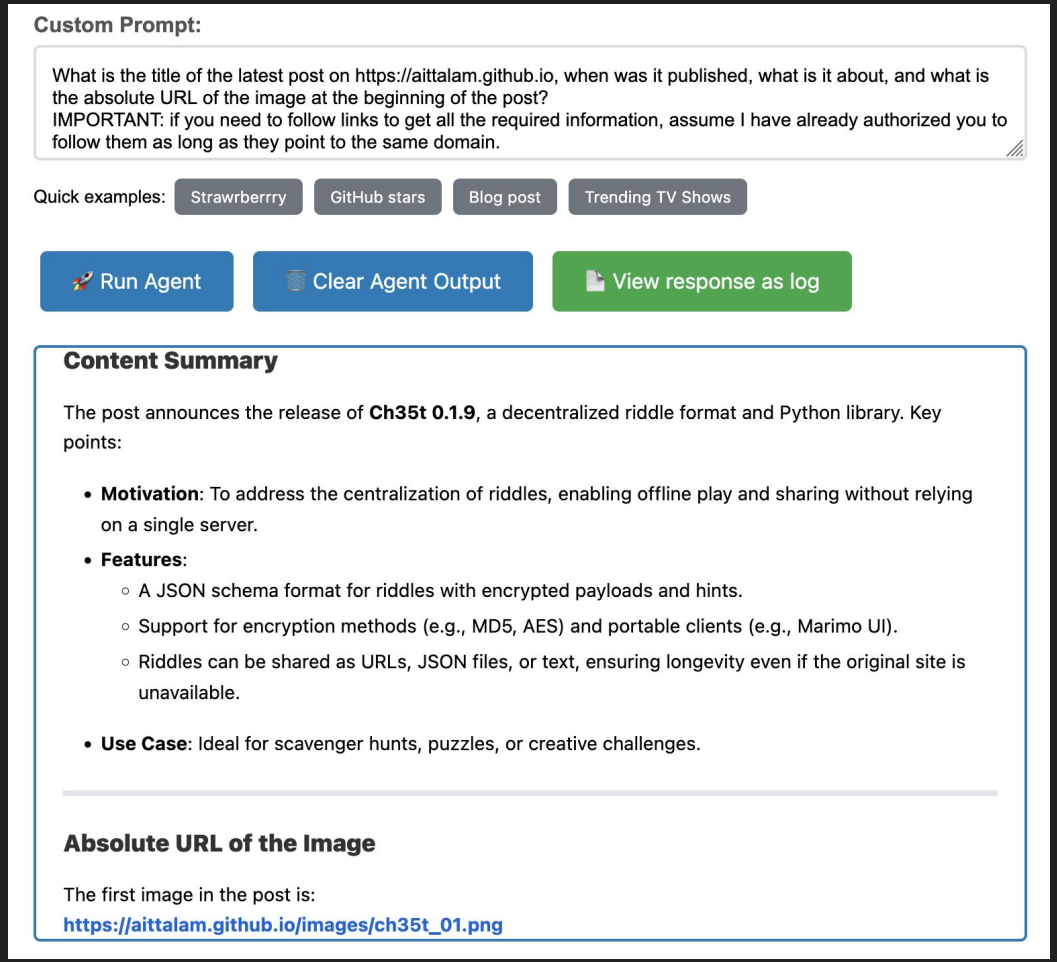
StRawRbeRRRy fields forever



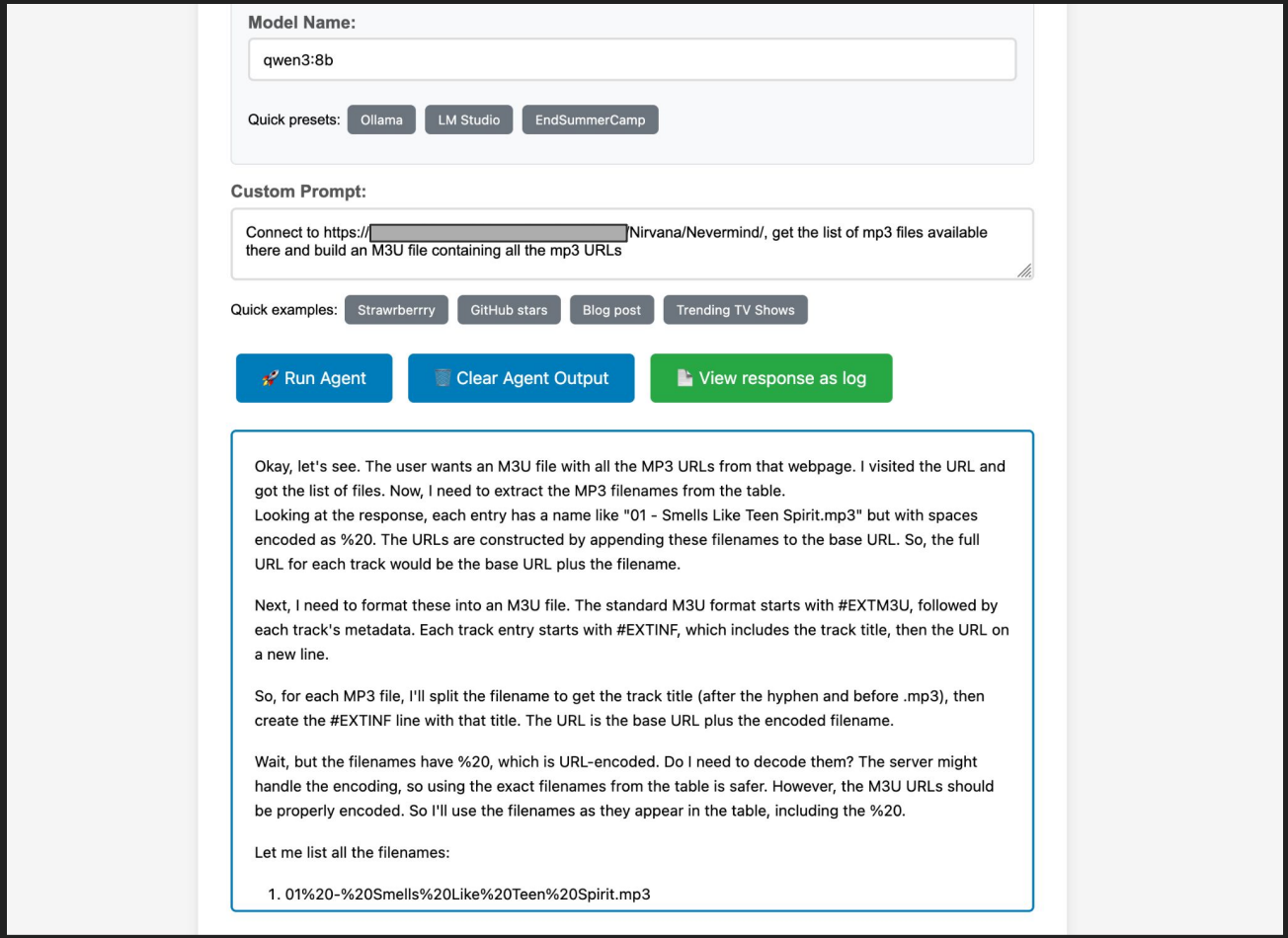
StRawRbeRRRy fields forever



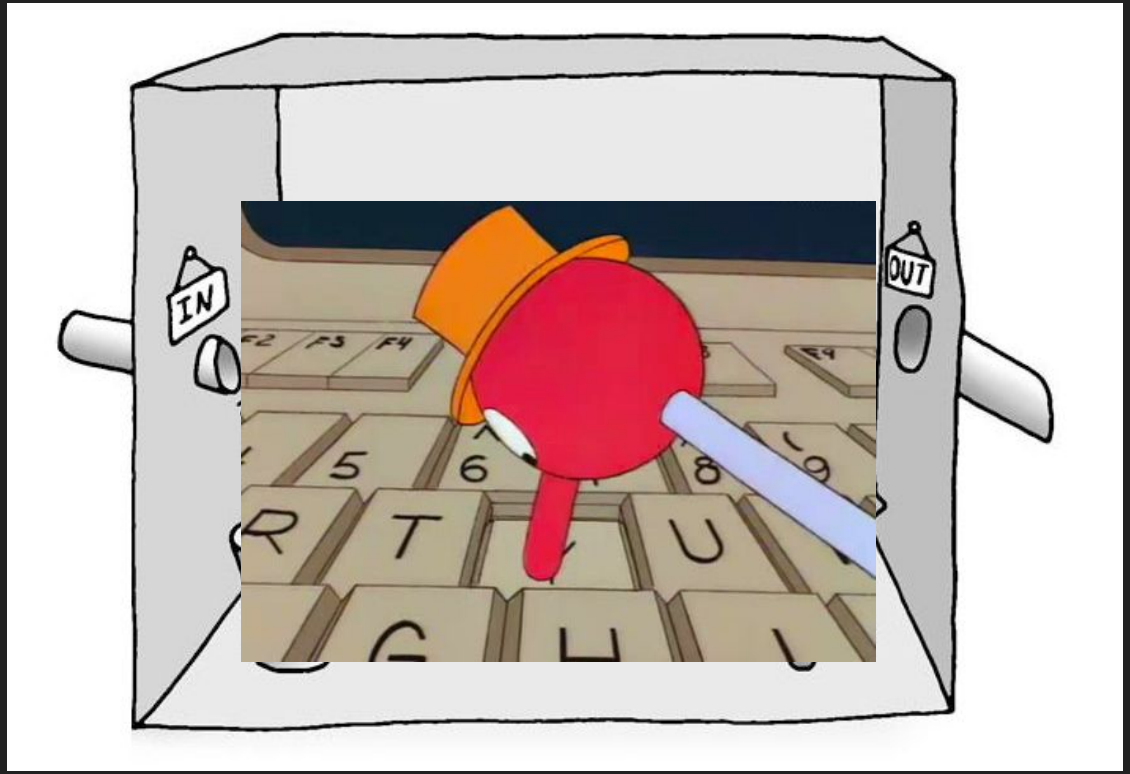
Monitor websites



Build M3U files

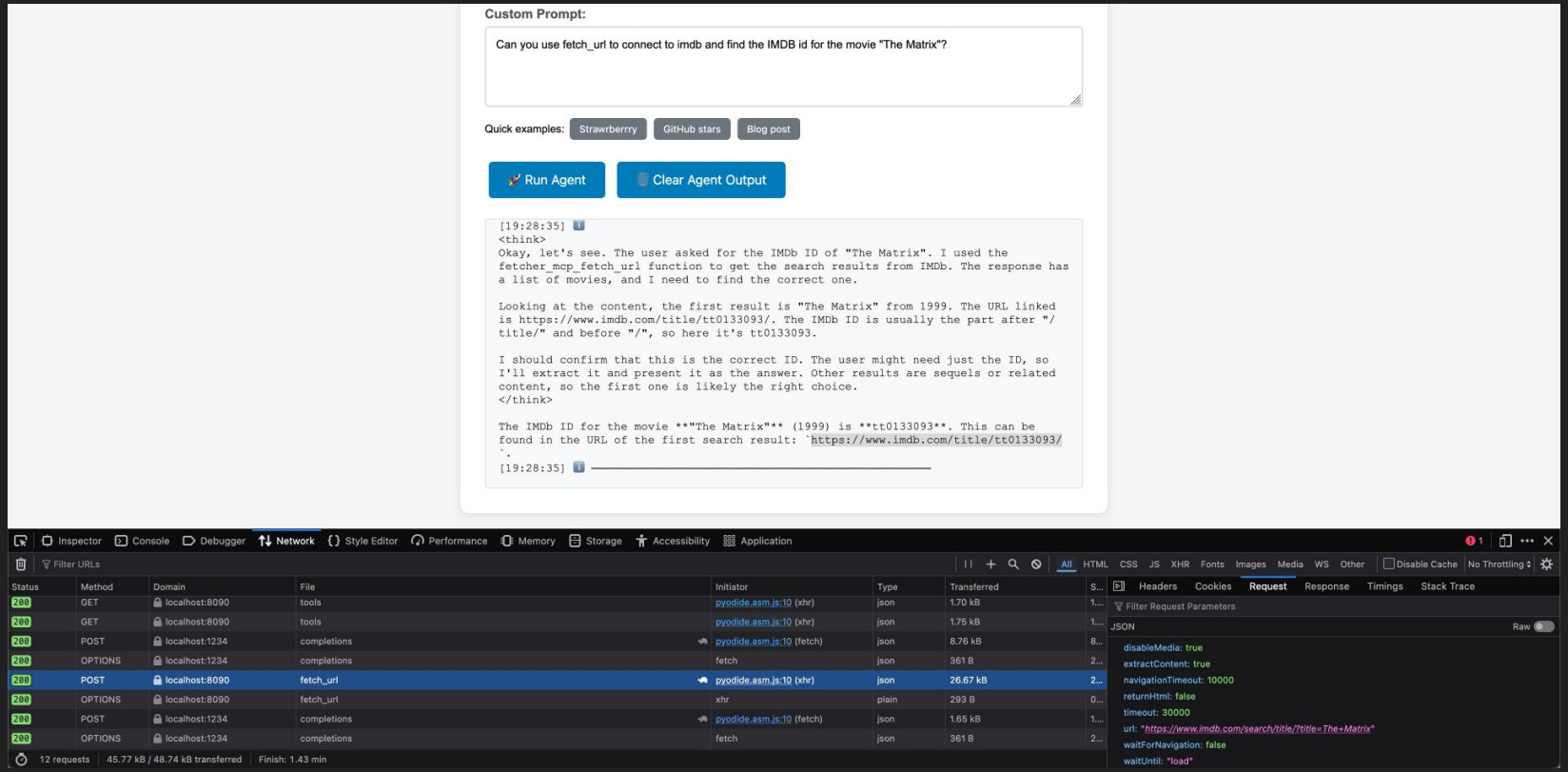


The drinking bird room

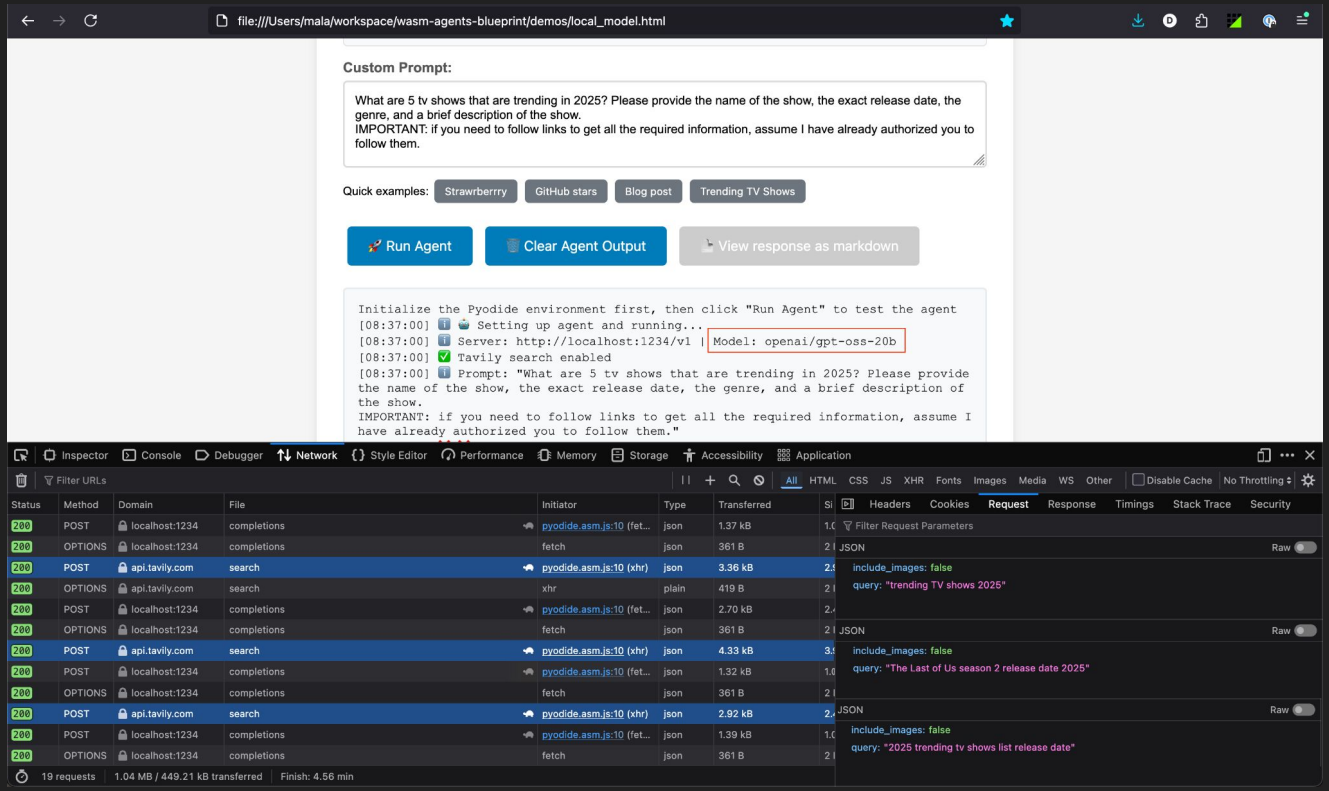


The Simpsons S07E07 (Jim Reardon, 1995)

Do LLMs dream of databases?



Model-specific insights: abusing search



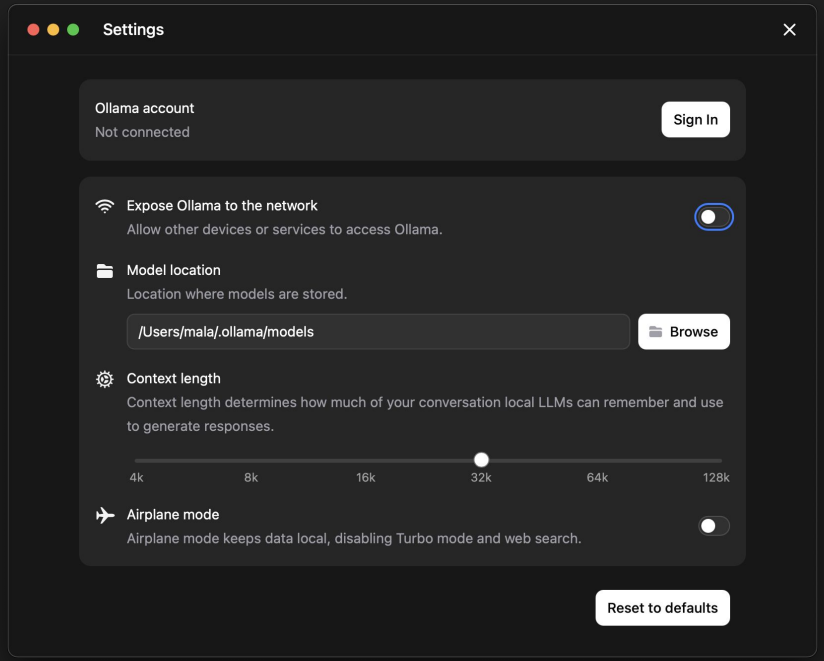
Problem: search tools

Welcome OpenAI's gpt-oss!

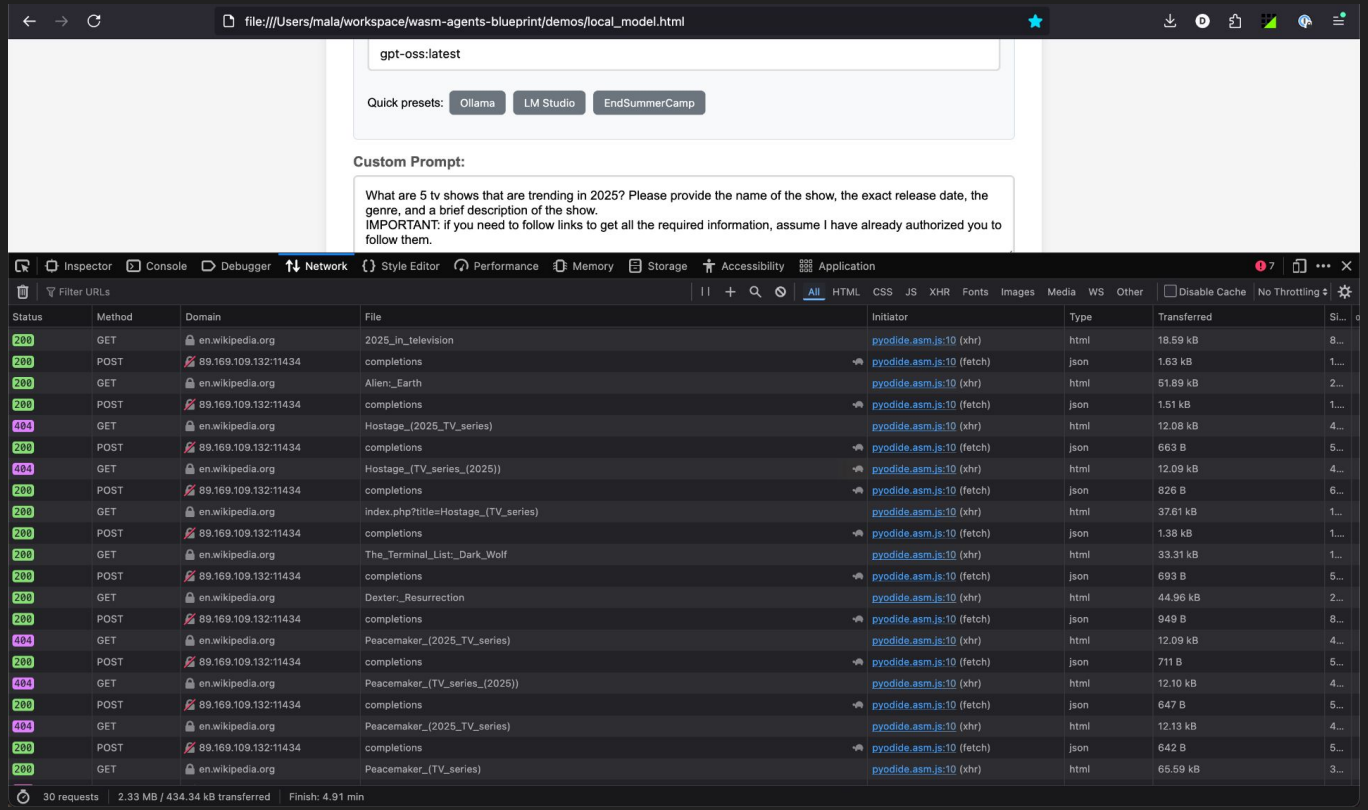
Ollama partners with OpenAI to bring its latest state-of-the-art open weight models to Ollama. The two models, **20B** and **120B**, bring a whole new local chat experience, and are designed for powerful reasoning, agentic tasks, and versatile developer use cases.

Feature highlights

- **Agentic capabilities:** Use the models' native capabilities for function calling, web browsing (Ollama is providing a built-in web search that can be optionally enabled to augment the model with the latest information), python tool calls, and structured outputs.



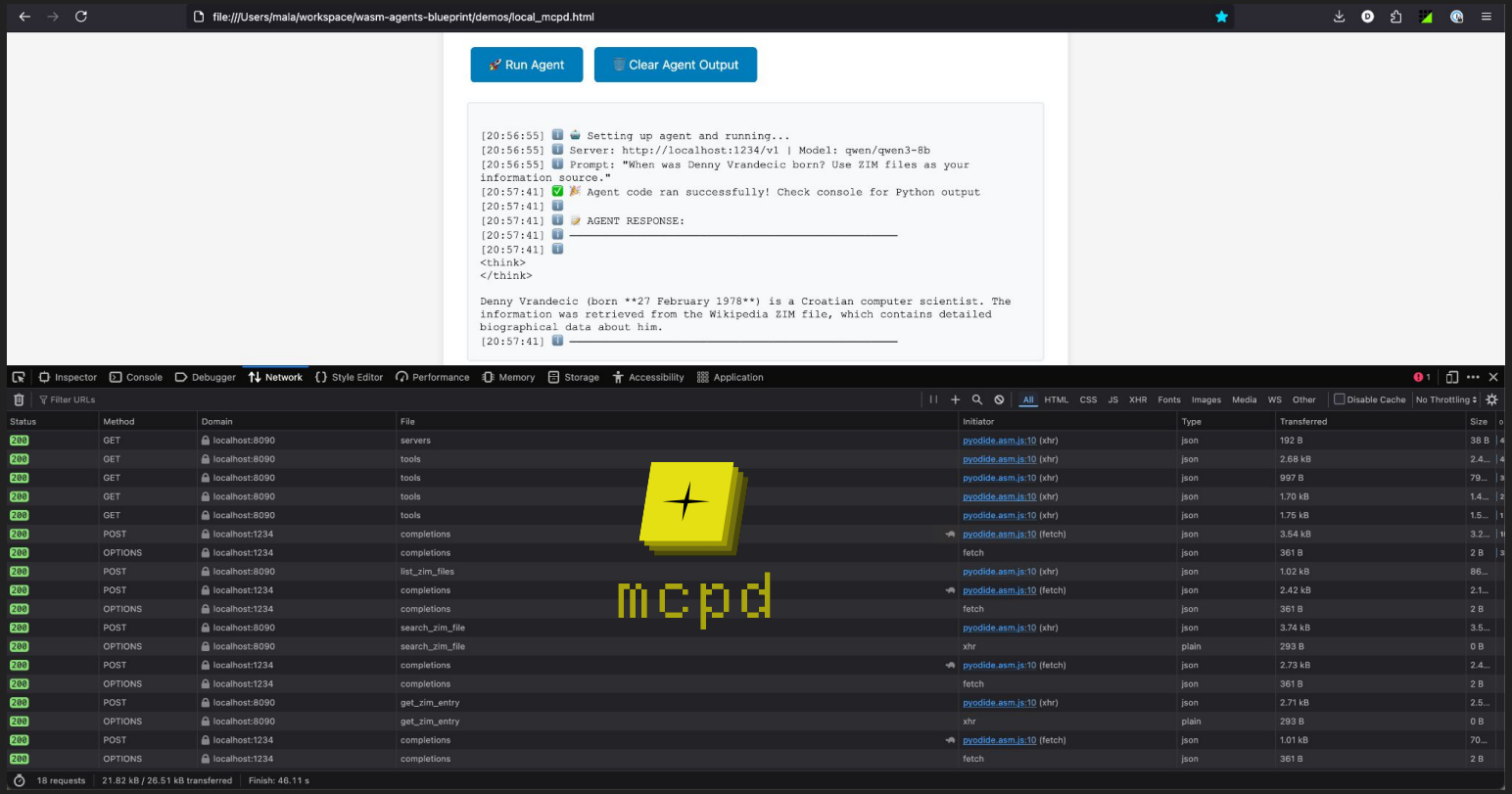
Model-specific insights: will it work without search?



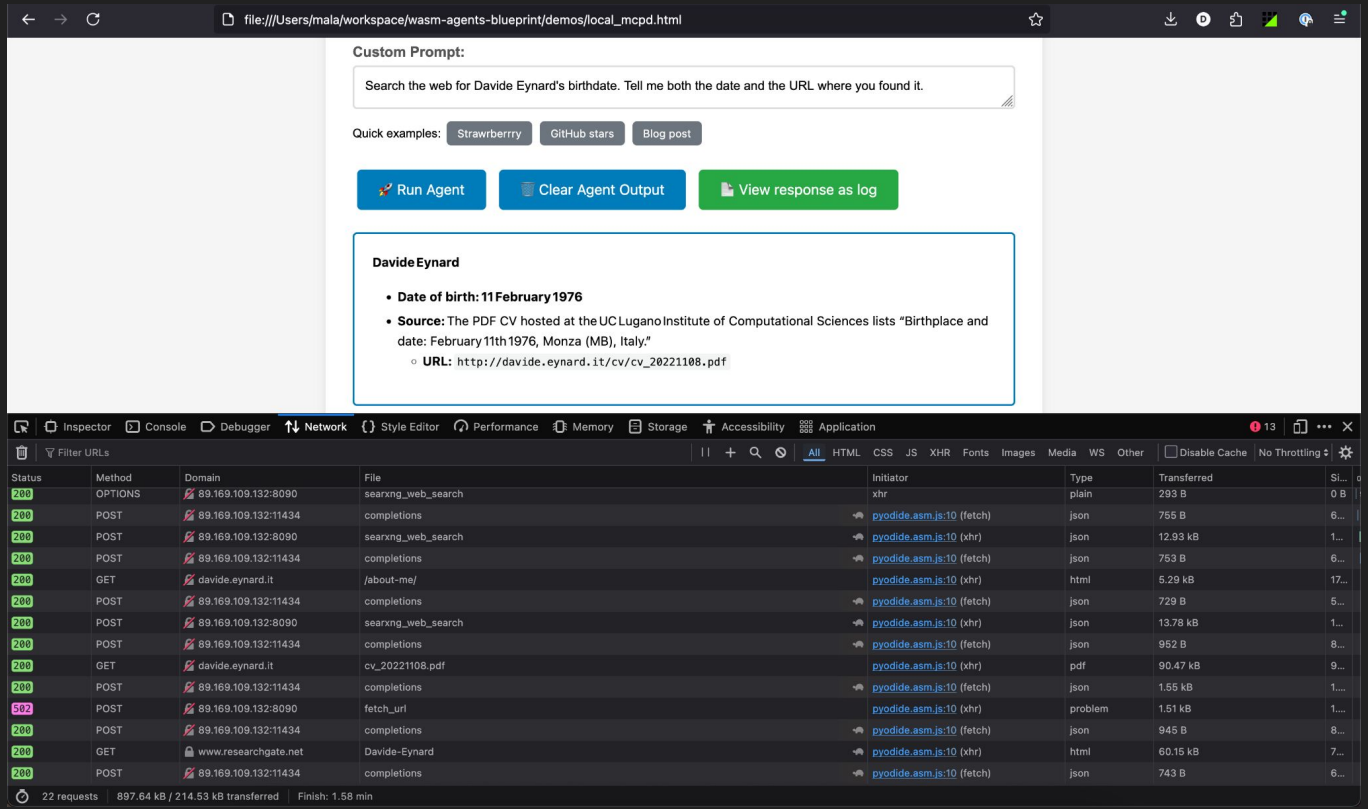
Problem: defaults

- Now it is Wikipedia
  - … is that ok?
  - What happens when it is not Wikipedia anymore?
- What is the default for *x* ?
- Who chooses it?

Adding MCP tools: ZIM



Problem: stalking agents



Learnings

- Ever-changing ecosystem
  - Builders often delegate problem resolution to “the next model”
  - *Share* the burden of being interoperable
- Easy, schmeasy: “friendly” vs actually useful
  - UX is only now evolving from chat to agents
- Smaller is better
  - Limit context growth
  - Few tools bring you a long way
- ~~LLMs~~ Agents will always give you an answer
  - It’s up to you to understand whether it’s the right one!
- ~~LLMs~~ Agents are slot machines
- Owning your tech is hard (but not impossible!)