Assignment: Build a Fact-Check AI Agent

Objective

Build an AI **Fact-Check Agent** using **LangChain**, **FastAPI**, **FastMCP**, and **Gemini API**.
 The agent must verify factual claims by **calling MCP tools** and returning a reasoned verdict.

Mandatory MCP Tools (Both Required)

🔍 MCP Tool 1: Web Search Tool

- Implemented using **FastMCP**

- Uses an **external web search API** (e.g. SerpAPI)

- Purpose:

  - Retrieve general web evidence related to a claim

🖼️ MCP Tool 2: News Search Tool

- Implemented using **FastMCP**

- Uses a **news API** (e.g. NewsAPI)

- Purpose:

  - Retrieve **recent or authoritative news articles**

Agent Behavior

1. Accept a **factual claim** from the user

2. Use LangChain reasoning to:

   - Decide search queries

   - Call **both MCP tools**

3. Combine results from:

   - Web search

   - News search

4. Analyze evidence using Gemini

5. Return a structured verdict

Verdict Classification (Required)

The agent must classify each claim as one of:

- ✅ **Likely True**

- ⚠️ **Uncertain**

- ❌ **Likely False**

Each verdict **must include justification** based on tool results.

API Specification

Endpoint

POST /fact-check

Input

{

```
  "claim": "string"
}
```

Output

```
{
  "verdict": "Likely True | Uncertain | Likely False",
  "explanation": "string",
  "sources": [
    {
      "title": "string",
      "url": "string",
      "type": "web | news"
    }
  ],
  "tools_used": ["web_search", "news_search"]
}
```

Technical Requirements

- Python

- LangChain ReAct agent (tool-calling required)

- FastAPI for API exposure

- FastMCP for **all MCP tools**

- Gemini API as LLM backend

- `.env` file for API keys

- No hardcoded secrets

Test Claims (They MUST Work)

- "The Earth is flat."

- "OpenAI released GPT-4 in 2023."

- "Drinking bleach can cure COVID-19."

- "Google is shutting down Gmail in 2025."

If the agent answers these **without MCP calls**, it fails.

Evaluation Criteria

- Proper MCP tool implementation

- Evidence-based reasoning (not hallucination)

- Clean LangChain agent logic

- Clear verdict explanation

- Code clarity & structure

Hard Rule

"If your agent produces a verdict without calling **both MCP tools**, the assignment is automatically rejected."