```
#!/usr/bin/env python

import argparse
import json
import xml.etree.ElementTree as ET

import requests

URL_OLLAMA = "http://localhost:11434/api/chat"
URL_MCP_SERVER = "http://localhost:5000/mcp"


def get_system_prompt(tool_name, tool_desc, tool_input):
    SYSTEM_PROMPT = f"""You are an AI quiz assistant.
Please present a quiz to the user and evaluate their input as either correct or incorrect.
The correct answer to the quiz must be one of the following: dog, cat, horse, or giraffe.

## Message Format

Your response must follow the XML format shown below.
Only two tags are allowed within the <response> tag: <message> and <call>.
The <message> tag is mandatory, while the <call> tag is optional.

Follow this format strictly and do not add any extra lines.
Do not wrap the reply message in a Markdown code block.
If the user's answer is incorrect, provide additional hints and continue the quiz until the correct answer is given.

## Example Response

Replace %TOOL_NAME%, %PARAM_NAME%, and %PARAM_VALUE% according to the MCP Tools section.

<response>
<message>Correct! Cool answer!</message>
<call><name>TOOL_NAME</name><arguments><%PARAM_NAME%>%PARAM_VALUE%</%PARAM_NAME%></arguments></call>
</response>

Sample <call> Tag

<call><name>add</name><arguments><lhs>1</lhs><rhs>2</rhs></arguments></call>

## MCP Tools

You can use the following MCP Tools.

### TOOL_NAME: {tool_name}

Description:
{tool_desc}

Input Schema:
{tool_input}

    args = parser.parse_args()
    return args


def get_response(model, messages):
    data = {
        "model": model,
        "messages": messages,
        "stream": False,
    }
    response = requests.post(URL_OLLAMA, json=data)
    if not response.ok:
        print(f"request failed due to {response.status_code}")
        raise Exception("invalid response")

    return response.json()["message"]


def init_mcp_server(mcp_session, url):
    """
    Init MCP server and get its tools.

    Continue MCP session with id = 2.

    Parameters
    ----------
    mcp_session: requests.Session
    url: MCP server URL

    Returns
    -------
    Tools List Response
      See https://modelcontextprotocol.io/docs/learn/architecture
      Tools Discovery > Tools List Response
    """
    mcp_session.headers.update({
```

```
        "Content-Type": "application/json",
        "Accept": "application/json, text/event-stream",
    })

    # initialization
    mcp_init_msg = {
        "jsonrpc": "2.0",
        "id": 1,
        "method": "initialize",
        "params": {
            "protocolVersion": "2025-06-18",
            "capabilities": {
                "elicitation": {}
            },
            "clientInfo": {
                "name": "example-client",
                "version": "1.0.0"
            }
        }
    }
    res0 = mcp_session.post(url, json=mcp_init_msg, stream=True)
    if not res0.ok:
        raise Exception("fail to initialize MCP server")

    mcp_session.headers.update(
        {
            "mcp-session-id": res0.headers["mcp-session-id"]
        }
    )

    # notification
    mcp_notification_msg = {
        "jsonrpc": "2.0",
        "method": "notifications/initialized",
    }
    res1 = mcp_session.post(url, json=mcp_notification_msg, stream=True)
    if not res1.ok:
        raise Exception("notifications/initialized failed")

    # get MCP tools
    mcp_list_tool_msg = {
        "jsonrpc": "2.0",
        "id": 2,
        "method": "tools/list",
        "params": {
            "cursor": "optional-cursor-value",
        },
    }
    res2 = mcp_session.post(
        URL_MCP_SERVER,
        json=mcp_list_tool_msg,
    )
    if not res2.ok:
        raise Exception("tools/list failed")

    return res2


def call_mcp_tool(mcp_session, url, mcp_id, tool_name, tool_args):
    """
    Call MCP tool.

    Parameters
    ----------
    mcp_session: requests.Session
    url: MCP server URL
    mcp_id: mcp message id
    tool_name: tool name
    tool_args: xml.etree.ElementTree.Element
    """
    params = {
        "name": tool_name,
        "arguments": {c.tag: c.text for c in tool_args},
    }

    body = {
        "jsonrpc": "2.0",
        "id": mcp_id,
        "method": "tools/call",
        "params": params,
    }

    # print(f"call MCP tool: {body=}")

    res = mcp_session.post(url,
                           json=body)
    if not res.ok:
        raise Exception("tools/call failed")
```

```
177
178
179 def main():
180     args = parse_args()
181
182     # init MCP server
183     mcp_session = requests.Session()
184     res2 = init_mcp_server(mcp_session, URL_MCP_SERVER)
185
186     print("---- res2 -----")
187     print(res2.text)
188     print("---- res2 -----")
189     print("")
190
191     tools_json = json.loads(res2.text.split("¥r¥n")[1][6:])
192
193     # get first tools
194     assert len(tools_json["result"]["tools"]) == 1
195     tool = tools_json["result"]["tools"][0]
196
197     tool_name = tool["name"]
198     tool_desc = tool["description"]
199     tool_input = tool["inputSchema"]
200
201     # send system prompt to get first quiz
202     messages = [
203         {
204             "role": "system",
205             "content": get_system_prompt(tool_name, tool_desc, tool_input)
206         }
207     ]
208
209     res_msg = get_response(args.model, messages)
210     # Uncomment the line below to display the first quiz
211     print(res_msg)
212     messages.append(res_msg)
213     assistant_msg = res_msg["content"]
214
215     mcp_id = 2
216     while True:
217         root = ET.fromstring(assistant_msg)
218         msg = root.find("message").text
219
220         # call MCP tool
221         call = root.find("call")
222         if call is not None:
223             tool_name = call.find("name").text
224             tool_args = call.find("arguments")
225
226             call_mcp_tool(mcp_session, URL_MCP_SERVER,
227                           mcp_id, tool_name, tool_args)
228             mcp_id += 1
229
230         # show chat message
231         print(msg)
232         user_input = input("input answer: ")
233         user_input.strip()
234
235         # append user message
236         messages.append(
237             {
238                 "role": "user",
239                 "content": user_input,
240             }
241         )
242
243         res_msg = get_response(args.model, messages)
244         # Uncomment the line below to display the raw response
245         # print(res_msg)
246         assistant_msg = res_msg["content"]
247
248         # append agent message
249         messages.append(res_msg)
250
251
252
253 if __name__ == "__main__":
254     main()
```