Session 6 – Agents Deep Dive

Learning Objectives

- Understand what AI agents are and why they matter.
- Learn the agent loop: Plan → Act → Reflect.
- Differentiate between reactive, proactive, and multi-agent systems.
- Run a simple demo with calculator and weather tools.
- Prepare for Session 7 on MCP.

Beginner-Level Explanation

- An AI agent is simply an LLM (like GPT) that can decide when to use a tool.
- Think of it like a junior analyst: it reads your question and decides whether to use a calculator, check the weather, or just answer directly.
- Tools are small helper functions or APIs (e.g., calculator, database, web search).
- The agent follows a loop: understand the query, decide if a tool is needed, call the tool, and return the result.

Expert-Level Explanation

- Agents implement a reasoning loop often described as Plan–Act–Reflect (or Plan–Act–Observe).
- Planning requires decomposing a problem into smaller steps and selecting the right tool for each step.
- Acting involves calling external functions or APIs with properly structured inputs.
- Reflection means evaluating results, possibly retrying or choosing an alternative approach.
- Advanced agents may maintain memory, arbitrate between multiple tools, and handle errors gracefully.

Types of Agents

- Reactive: Respond step-by-step without long-term planning.
- Proactive: Can form multi-step plans and anticipate needs.
- Single-agent vs multi-agent: Multi-agent systems can collaborate and specialize in different roles.

Demo Flow

- 1. User asks: 'What is 12 * 7 + 5?' → Agent decides this is a calculator query.
- 2. Agent calls the calculator tool, which safely evaluates the expression.
- 3. Tool returns the result (89).
- 4. Agent responds: 'Result: 89'.
- Another query: 'Weather in Berlin today?' → Agent calls the weather tool (mocked).

Enterprise Implications

- Agents are the building block for enterprise AI copilots.
- They allow controlled, auditable tool usage (critical for compliance).

- Examples: financial assistants, code review bots, customer service copilots.
- Sets the stage for MCP, which standardizes tool integration across the enterprise.

Wrap-Up

- Agents = LLMs that can act using tools.
- This session introduced the core loop and demoed calculator + weather tools.
- Next session: Tools & MCP – how to expose enterprise systems safely to agents.