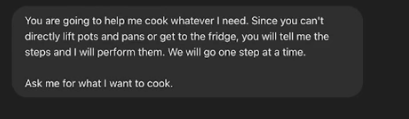
**Module1**

**Introduction:**

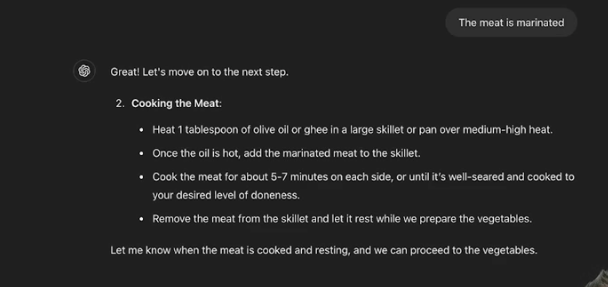


* Agentic Ai is basically a agency , you can also think of it as autonomy that can go and try to solve the problem. And react to different situations.
* Now ab basically yeh cheez toh humnay genAi mabi dekhi haka it can solve problem and can react to different situations but jo simple genAI hai it can generate solution for us but it cannot interact with other real-time system.
* Now the purpose of agentic Ai is to make genAi capable of interacting with other real-time systems.So it can take actions, then see the result of those actions and then respond based on that result.

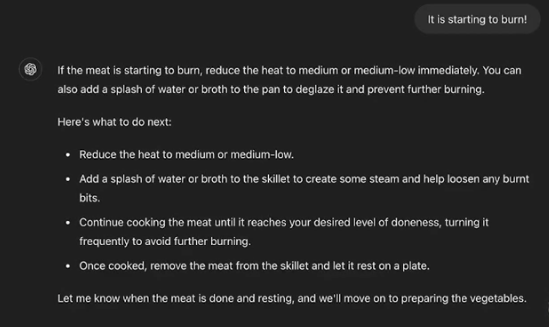
Now we are going to build agentic system but it is not fully agentic yet likin wo asa system hoga jisme hum AI ko btayeingay kay we want to do this and it will give us the instruction and we will perform the action .



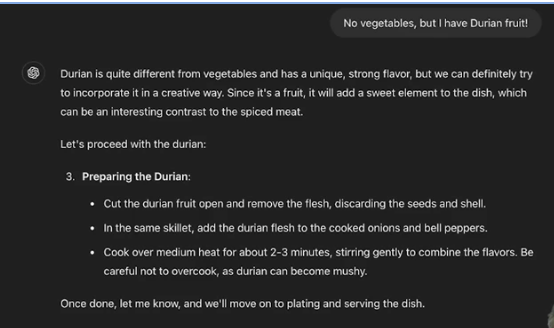
And basically above is the prompt that is kick starting the agentic system, where I am going to follow the instructions that it will tell me and also take action when it ask to me.But later on yehi kam jo abhi hum khud kr rhay hain wo **zapier** ka through krwayegay which means kay Gpt will give instruction to zapier and it take perform that actions.



Now in above SS you can see that gpt giving us instruction and we are performing them.



Now here in the above SS you can see that here comes its agentic aspect that how it react to different situation and provide instructions.



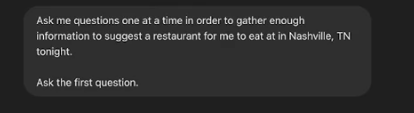
Now in above SS we have flipped the situation but still it responding now here the thing to notice is that we are not providing the instruction Gpt rather than it Gpt is providing instructions to us , this is how agentic Ai work that it gives instruction to human, software like zapier or any computer system and it will perform action.

Now basically the main purpose of genAi or agentic Ai is to make the computer systems capable of solving problems like the human .

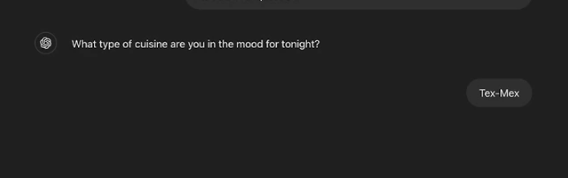
**Flipped Interaction Pattern:**

* Now we will see that what are the basis of this agentic.
* There are also prompt engineering patterns but the basis of this is **flipped interaction patterns** which means rather than us telling the system what to do, rather than us doing question with Gpt , it asks a question from us or it ask questions to the systems which are connected to it and also tell them to perform the action.

**Let look at the structure of this flipped interaction pattern:**

****

1. So the main structure or line is to saying Gpt that do a one question at a time with me. And one question at a time is the best practice for agentic system and the goal of this is we want to create a situation where it goes and create things that need to be done and create actions that need to be taken by us or software like zapier on behalf of the agent. And the trick of saying to ask one question at a time is so important in agentic system so that due to this approach it will do first question and then do the second question on the basis of first. And also saying to **ask the first question** at the bottom of prompt is to starting it in a steps.
2. Then, telling it to collect the info .
3. And basis of that info give us the suggestions



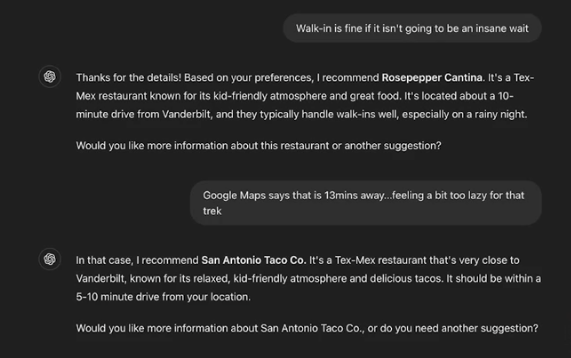
A screenshot of a chat

Description automatically generated

A screenshot of a chat

Description automatically generated

Now in the above chat you can see that its totally fluid and it is asking the next question on the basis of previous answer so that’s the magic of agentic that it is adapting the situation and responding. And this is most important work of LLM that they can handle input/prompt in so many different format / ways of expressing the info and idea.



Now in the above SS you can see that how it magically handle the situation like a real human agent.

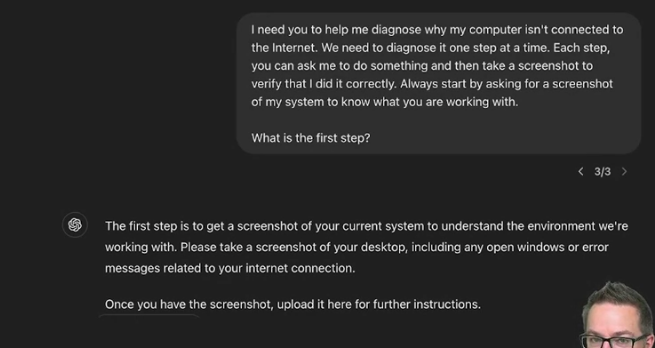
Now one thing is more that Agentic AI is doing that instead of only collecting the information from database and responding to user, it is also collecting the info from me/user by asking a question. This is also an difference b/w genAi and agentic based genAI .

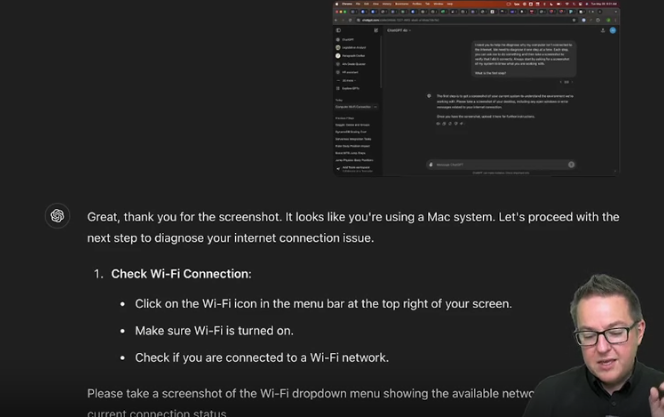
But the difference b/w collecting info from user and database is that when it collecting info from user so the language is different but when it collecting from db so the language is different and this is good thing about LLM is that they are extremely fast in translating and collecting the info in different languages.

**Multimodal Flipped Interaction :**

* Now the amazing thing about these multimodal and patterns is that they are not only stick with languages , These systems can interpret so many different types of information. It doesn't just have to be human language. And this is a key thing that we have to understand is we can go give it all kinds of information such as images, audio etc.
* So when we use the flipped interaction pattern where we have it go and

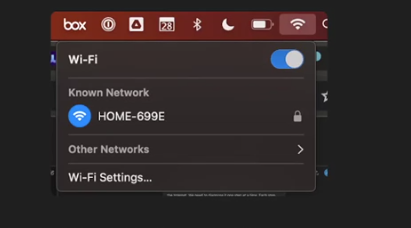
ask us questions or ask the database questions or tell us what to do, or tell the computer system what to do. It doesn't have to just get feedback in terms of language. It doesn't just have to be our human language. It can use all kinds of modalities of communication and we're going to take a look at an example of that. And that example we're going to provide is photographs



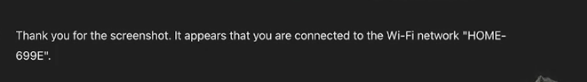


Now, notice what it did, right? It looked at this screenshot and said, hey, that looks like Mac. So it knows about my computer from the look of what it sees in the screenshot. It's not just me saying I have a Mac, this version or this information it's looking at and collecting rich information from that screenshot and then adapting based on what it sees in the screenshot. Iska mtlb yeh haka usme SS ko process kia and then it judges that it is a MAC. This proofs that these Multimodal can process and interpret images as well.

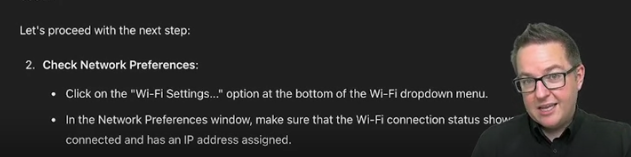
Now A/c to above SS its asking to send SS of wifi dropdown,



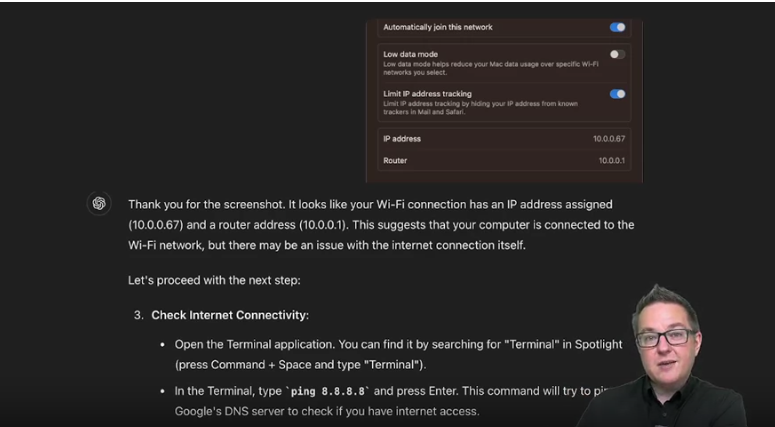
So I go and do what it says. Now, I didn't have an actual Internet connection issue, but I just wanted to get it to walk through and see if it could diagnose because I'm claiming that I have one. And so I wanted to see if it can get to the point where it actually understands that, no, I don't actually have an issue.



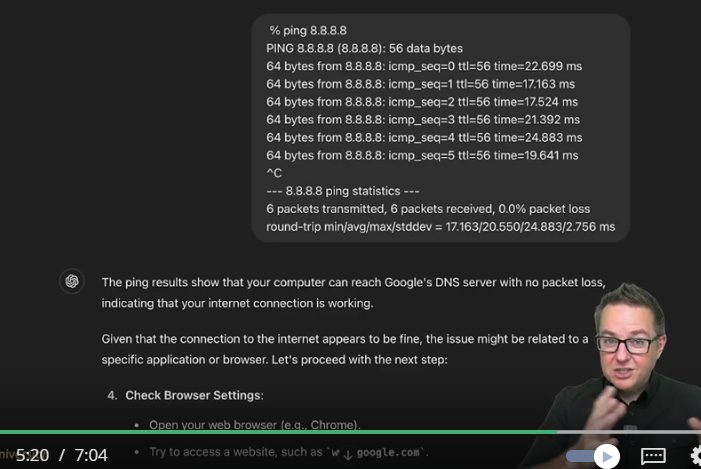
now you can see that it automatically identifies that I am already connected to some internet. It doesn't require me to tell it, it simply collects the information that it needs from the feedback that I'm giving it.



So again, telling me an action to take, telling me to give it back a screenshot.



Now notice what it's done. It now needs to get a command run on the system. And so it's translated that high level task of check Internet connectivity into a command, a language that the computer understands. So it is doing that translation step. It's not only identifying what needs to be done, but it's identifying how to translate that specifically into the language that it can use to communicate with the computer to find out the information it needs.



Now, I didn't take a screenshot of it. I actually just copied and pasted it back into the prompt. I should have probably done it as a screenshot, but I wanted to see how it would respond if I suddenly throw it a curveball(flip the instruction) by not giving it a screenshot anymore, but actually giving it the text. And this is the raw text that was output by running that command. You notice this is all, this is something that makes sense to me as a programmer. If you are in IT, it may make sense to you. If you are not into this stuff, you're going to look at this and you're going to say it looks like a foreign language and it is. It's a language that many people understand how to speak, but if you don't know this language, you don't know how to speak it. It looks very foreign, but gpt understands how to then translate this back into meaning. And it says, the ping results show that your computer can reach Google's DNS server with no packet loss, indicating that your Internet connection is working.

Now above explanation means that you can see how it handles another format and also it translate the not-understandable format into the understandable format so that anyone can understand.

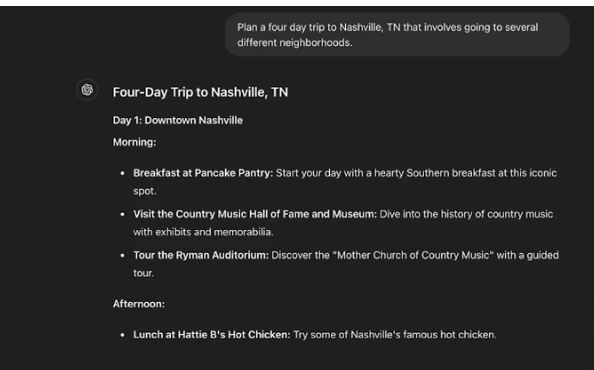
 Now you have seen that how it would keep going, trying to help me diagnose the supposed Internet connectivity problem with my computer that I don't actually have. But you see how it's adapting. It can adapt to many different types of responses. That flipped interaction where we say, here's the pattern, go do one step at a time, I'm going to give you the result. Every time it takes what it gets back, it responds, it adapts, it translates, it can interface with different systems. Now we're still using manual interfacing. We're having a human provide the interface. But rather than interface to the world of cooking, we're now interfacing to the world of machines and to world of computers, which is eventually where we're going to go with these agentic systems is. We are going to allow them to directly talk to those machines or software like zapier in order to carry out tasks, in order to obtain information that the agent needs in order to reach some overall goal.

**Planning**



Now, agents don't just have to go and do everything one step at a time. They can actually go and build rich plans. And this is one of the capabilities that really underlies all this, is their ability to take a goal that you're trying to achieve, some high level task, and decompose it into a series of subtasks or goals in order to form a plan to accomplish it. And that is a fundamental capability. Now, one way that we can have agents work is we can have them go and interactively, one task at a time, go and take steps and perform actions and respond. And that's a really powerful way to do it. Another way that we can do it is the complete opposite. We can have it build out the whole plan in advance and then go and send it off to be executed.

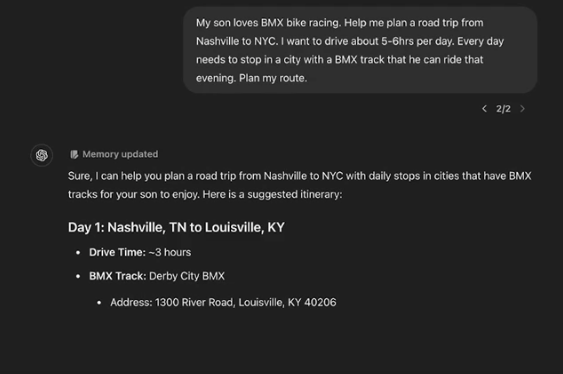
so let's do the planning where a human being is going to go and execute the whole plan. So here's my goal. Plan a four day trip to Nashville that involves going to several different neighborhoods.

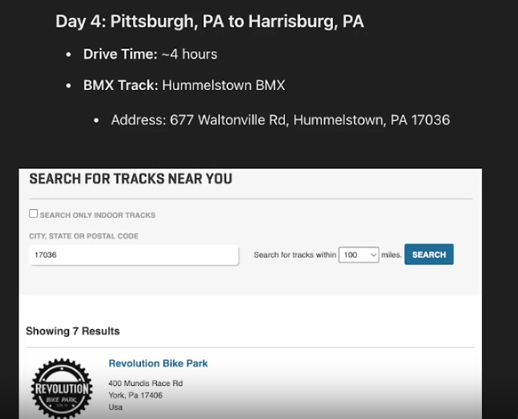


Now in the above img you can see that it create Day1 plan for us and further , but the plan here it provided is great A/c to its perspective but from my perspective its not much good bcuz here may be I don’t like country music hall. So this is the main difference when we plan it go **step by step** as we have done in previous examples above so in that way it adapt our requirements more efficiently and response on the basis of that But when we provide the **complete plan to it at once** ! so does not adapt it more efficiently and cannot respond more efficiently.

But there's some complexity when we are working with **Step by step** **approach**?  it may forget steps or it may lose track of what it was trying to do or something like that. On the other hand if we go with **Whole plan at once**, we can go, we can have it so it never loses track of what it's going to do. It can build out the full plan in advance, and then it just gets sent off to execute multiple steps. And it doesn't have to remember what it said or anything like that makes it an advance.

Now it depends on us that which type of planning we want to do **Step by step** or **Whole plan at once .**





Now in the above pics you can see that I am asking it to plan a four days trip now the planning for Day1 Is OK But if you see the day 4 track which it recommended so its not OK bcuz the track it is asking for that is Hummelstown BMX does not exist which means it providing wrong info also known as **AI hallucination.**

Now A/C to the above e.g it proves when plan it to do all at once, So it can cause Hallucination also which is dangerous bcuz let suppose if I agree with and go to that track which he is asking me to go So I can fell into a danger bcuz in reality that track does not exist.

Now, how do we overcome issues like this? Well, so far, what we've done is just given it sort of open ended prompts, but we can start to add in information. Upfront we can give it information that we want it to work with, constraints that we want it to work with, to try to bound what it does and what it reasons about. And this is really, really important when we start thinking about agents information, giving the agent access to the information it needs to accomplish the task is critically important. Now, some cases, it can go and fetch the information for itself if we explicitly tell it to do that and when to do it.

Now basically the above text is asking that it is very important to tell agent that from which information it has to extract the respond , so to overcome the above problem we have to explicitly provide it information and ask to give me respond using this info like in the below respond , first we have provided it the tracks which are currently active and exist in Canada so now it respond the accurate results in the below picture.

