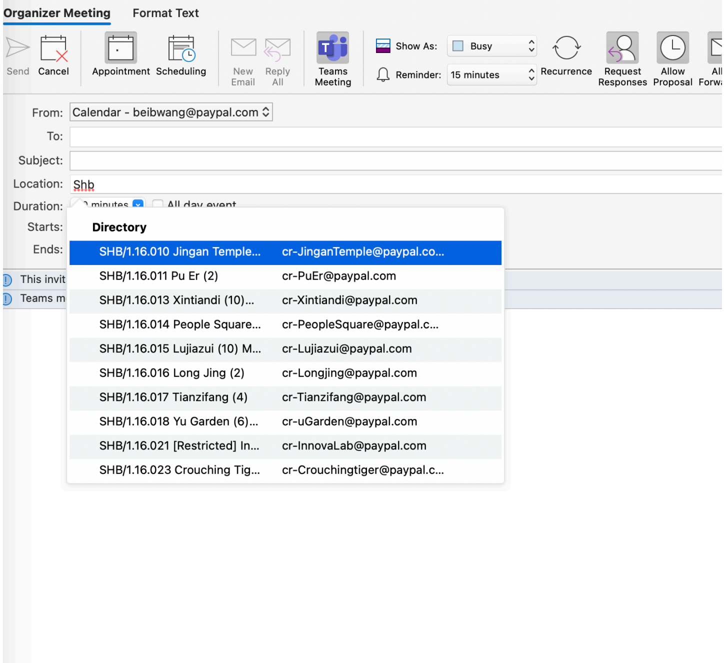
！！！ Phama db notes

Tuesday, May 13, 2025 16:23



From: Calendar - beibwang@paypal.com

To:

Subject:

Location: Shb

Duration: minutes ☑ □ All day event

Starts:

Ends:

This invit

Teams m

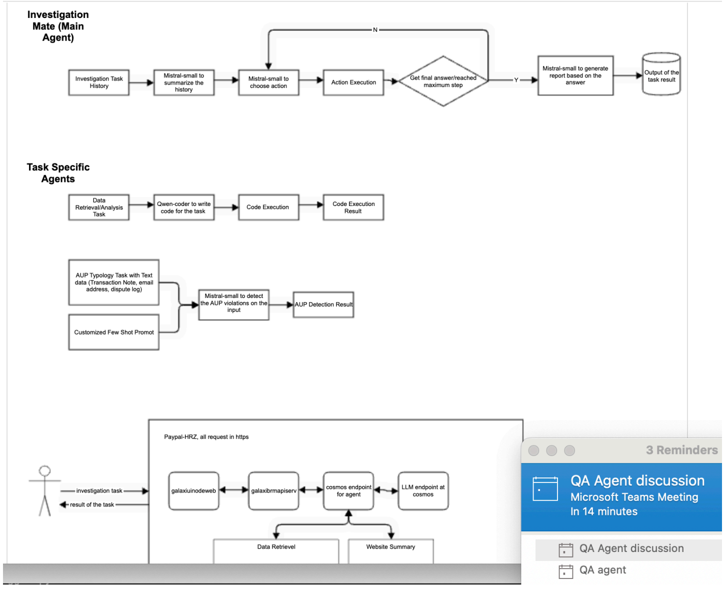
Directory

SHB/1.16.010 Jingan Temple...	cr-JinganTemple@paypal.co...
SHB/1.16.011 Pu Er (2)	cr-PuEr@paypal.com
SHB/1.16.013 Xintiandi (10)...	cr-Xintiandi@paypal.com
SHB/1.16.014 People Square...	cr-PeopleSquare@paypal.c...
SHB/1.16.015 Lujiazui (10) M...	cr-Lujiazui@paypal.com
SHB/1.16.016 Long Jing (2)	cr-Longjing@paypal.com
SHB/1.16.017 Tianzifang (4)	cr-Tianzifang@paypal.com
SHB/1.16.018 Yu Garden (6)...	cr-uGarden@paypal.com
SHB/1.16.021 [Restricted] In...	cr-InnovaLab@paypal.com
SHB/1.16.023 Crouching Tig...	cr-Crouchingtiger@paypal.c...

1. 重写问题
2. 判断第一个tool用啥
3. Transaction nodes+ restrictions+（Llm call prompt+ 关键词keyword match） 去phama db匹配，最相关的row。
4. 洗数据/写代码
5. 最后才是summary 去取图表

写代码

最少5步最多8步
找到match问他要不要做keyword inspection
无论前面走了几步，最终都要到summary这一步，写narrative，出highlight risk的点


Investigation Mate (Main Agent)
Investigation Task History
Mistral-small to summarize the history
Mistral-small to choose action
Action Execution
Get final answer/reached maximum step
N
Y
Mistral-small to generate report based on the answer
Output of the task result
Task Specific Agents
Data Retrieval/Analysis Task
Qwen-coder to write code for the task
Code Execution
Code Execution Result
AUP Typology Task with Text data (Transaction Note, email address, dispute log)
Customized Few Shot Promot
Mistral-small to detect the AUP violations on the input
AUP Detection Result
Paypal-HRZ, all request in https
investigation task
result of the task
galaxiuinodeweb
galaxibrmapiserv
cosmos endpoint for agent
LLM endpoint at cosmos
Data Retrievel
Website Summary
3 Reminders

QA Agent discussion
Microsoft Teams Meeting
In 14 minutes

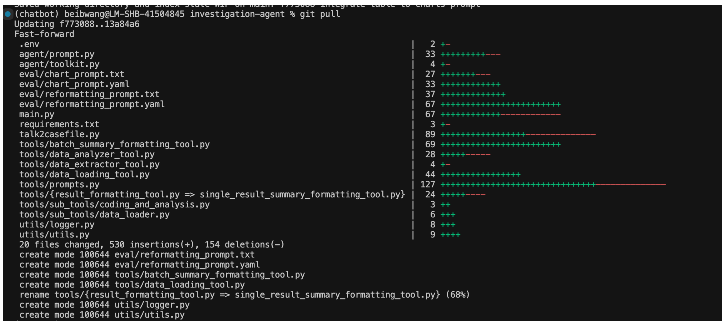
QA Agent discussion

QA agent

QA agent在output of the task result之前

预定义的问题，不经过llm；代码有，

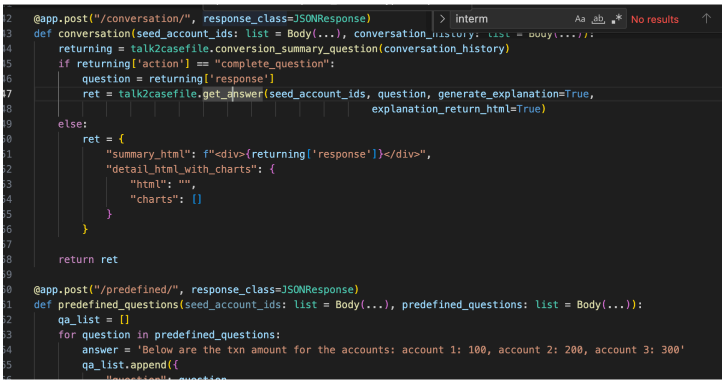
预定义的问题，prompt问问题里的notes



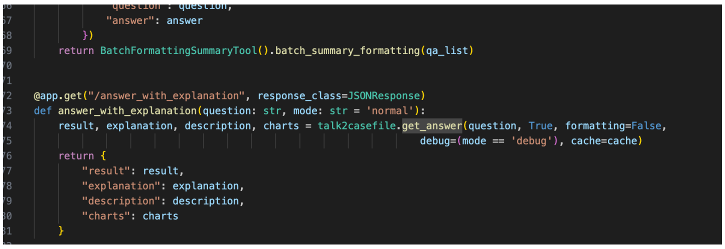
```
Saved working directory and index state WIP on main: f773088 integrate table to charts prompt
(chatbot) beibwang@LM-SHB-41504845 investigation-agent % git pull
Updating f773088..13a84a6
Fast-forward
 .env                                                                  |   2 +-
 agent/prompt.py                                                       |  33 +++++++++---
 agent/toolkit.py                                                      |   4 +-
 eval/chart_prompt.txt                                                 |  27 +++++++---
 eval/chart_prompt.yaml                                                |  33 ++++++++++++
 eval/reformatting_prompt.txt                                          |  37 +++++++++++++
 eval/reformatting_prompt.yaml                                         |  67 ++++++++++++++++++++++++
 main.py                                                               |  67 ++++++++++++------------
 requirements.txt                                                      |   3 +-
 talk2casefile.py                                                      |  89 +++++++++++++++++-------------
 tools/batch_summary_formatting_tool.py                                |  69 ++++++++++++++++++++++++
 tools/data_analyzer_tool.py                                           |  28 +++++------
 tools/data_extractor_tool.py                                          |   4 +-
 tools/data_loading_tool.py                                            |  44 ++++++++++++++++
 tools/prompts.py                                                      | 127 +++++++++++++++++++++++++++++++-------------------
 tools/{result_formatting_tool.py => single_result_summary_formatting_tool.py} |  24 +++++-----
 tools/sub_tools/coding_and_analysis.py                                |   3 ++
 tools/sub_tools/data_loader.py                                        |   6 +++
 utils/logger.py                                                       |   8 +++
 utils/utils.py                                                        |   9 ++++
 20 files changed, 530 insertions(+), 154 deletions(-)
 create mode 100644 eval/reformatting_prompt.txt
 create mode 100644 eval/reformatting_prompt.yaml
 create mode 100644 tools/batch_summary_formatting_tool.py
 create mode 100644 tools/data_loading_tool.py
 rename tools/{result_formatting_tool.py => single_result_summary_formatting_tool.py} (68%)
 create mode 100644 utils/logger.py
 create mode 100644 utils/utils.py
```

/Users/beibwang/Downloads/chatbot/investigation-agent/tools/TextAUPViolationTool.py

```
from langchain.tools import BaseTool
from utils import aup_violation_utils
from mlorchsdk import RaptorCallClient
class TextAUPViolationTool(BaseTool):
    name: str = "text_aup_violation_tool"
    description: str = f"""
    Useful when you need to detect the texts (dispute, limitation, transaction notes, email address, paypal me slug etc.) are related to AUP violations (weapon, pharma, drug, Adult etc.).
    The input of the function contains three parameters.
    texts: list, which contains a list of texts.
    text_type: the type of the text, possible values: dispute, limitation, transaction_note, email_address, paypal_me_slug
    aup_violation_categories: the aup violation categories to do the detection. the possible values can be selected from the list {aup_violation_utils.categories}

    The output will be the texts that hit the specified AUP violation categories.
    """
#keyword + phama db 两路匹配，; prompt通过description ，选tool
RaptorCallClient{
    url = "",

} #https://github.paypal.com/edp-aiml/ml-orch-sdk
#test, phama db link,
#solution


    def _run(
            self,
            texts: list[str],
            text_type: str,
            aup_violation_categories: list[str]
    ) -> list:
        return [f"there's no AUP violations for the given {text_type} texts for {aup_violation_categories}"]
    # post method
    async def _arun(
            self,
            texts: list[str],
            text_type: str,
            aup_violation_categories: list[str]
    ) -> list[str]:
        return [f"there's no AUP violations for the given {text_type} texts for {aup_violation_categories}"]
```



```
@app.post("/conversation/", response_class=JSONResponse)
def conversation(seed_account_ids: list = Body(...), conversation_history: list = Body(...)):
    returning = talk2casefile.conversion_summary_question(conversation_history)
    if returning['action'] == "complete_question":
        question = returning['response']
        ret = talk2casefile.get_answer(seed_account_ids, question, generate_explanation=True,
                                       explanation_return_html=True)
    else:
        ret = {
            "summary_html": f"<div>{returning['response']}</div>",
            "detail_html_with_charts": {
                "html": "",
                "charts": []
            }
        }

    return ret

@app.post("/predefined/", response_class=JSONResponse)
def predefined_questions(seed_account_ids: list = Body(...), predefined_questions: list = Body(...)):
    qa_list = []
    for question in predefined_questions:
        answer = 'Below are the txn amount for the accounts: account 1: 100, account 2: 200, account 3: 300'
        qa_list.append({
            "question": question
```



```
                "question": question,
                "answer": answer
            })
    return BatchFormattingSummaryTool().batch_summary_formatting(qa_list)


@app.get("/answer_with_explanation", response_class=JSONResponse)
def answer_with_explanation(question: str, mode: str = 'normal'):
    result, explanation, description, charts = talk2casefile.get_answer(question, True, formatting=False,
                                                                        debug=(mode == 'debug'), cache=cache)
    return {
        "result": result,
        "explanation": explanation,
        "description": description,
        "charts": charts
    }
```

AUP_VIOLATION_VERIFICATION_LLM_MODEL

@app.post("/conversations

Debug=True 看有没有用到description

verification不属于agent
QA agent prompt放到agent下面的prompt.py里面

Transaction id
Transaction Amount
Date notes
主题
Transaction 表主体 seed
Casefile linked account id 在请求里发过去，casefile里把linked account作为seed account
casefile不区分seed还是link
Transaction
Phama db 都在回答里

Hover

取casefile 数据，怎么取比较hei
现在不能把she j

z z z z z z z z z z z z z z z z z z z z z z z z z z z z z z z z z z z z z z z z z z z z z z z zw w w w w w w w w w w w w w w w w w w w w w w w w w w w w w w w w
w w w w w wCcts

Apply similar logic 怎么访问大户家
对话爱好，对话爱好

cct先指定aacx

显示地
Intrr

对xiaoshihou

一起返回

主要数据

最啊==

入股

有没有办法

time put -> product 给个提示
300m

先设置一个time out
看
CETS try
只拿u parent； auth特殊情况，

想要跟
Time out先设一个

是否只取u

Populate u
Review 所有question- comment

A
C
A
A
B
B
A
A
C

A
B
A
A
B
B
C

A
A
C
A
B
C
B
B
B

```
curl --location 'http://localhost:8090/galaxi/api/v1/brm/pharma-info/' \
--header 'Content-Type: application/json' \
--data '{
   "product": "advanced turmeric",
   "limit": 5
}'
```

```
curl --location 'https://te-iaodplatform.qa.paypal.com:21777/galaxi/api/v1/brm/pharma-info/' \
--header 'Content-Type: application/json' \
--data '{
   "product": "advanced turmeric",
   "limit": 5
}'
```

```
curl --location 'https://te-iaodplatform.qa.paypal.com:21777/galaxi/api/v1/brm/pharma-info/' \
--header 'Content-Type: application/json' \
--data '{
   "product": "advanced turmeric",
   "manufactures": ["Solnutra"],
   "limit": 5
}'
```

Paypal phama aup violation category
公网有人讨论
Paypal 关于phama
自己生成一段，只利用了open source llm，并没有利用内部文档（如果觉得类似的，就用llm生成；
甚至对paypal 有sense 的paypal phama aup violation 生成一段（如何测，大方向上对不对？待定）
； 没有经过review还是经过review

洗图