A Framework for Integrated Digital Forensic Investigation Employing AutoGen AI Agents

Akila Wickramasekara, Mark Scanlon

Forensics and Security Research Group, University College Dublin, Ireland
(akila.wickramasekara@ucdconnect.ie, mark.scanlon@ucd.ie)

Abstract

The increasing frequency and rapidity of criminal activities require faster digital forensic (DF) investigations. Currently, most DF phases involve manual procedures, requiring significant human effort and time, often facing evolving requirements. This work proposes an integrated framework employing AutoGen Artificial Intelligence (AI) agents and Large Language Models (LLMs) such as LLAMA , StarCoder and WaveCoder. The suggested framework utilizes AI agents and LLMs to perform tasks articulated in natural language by a human agent. The proposed architecture presents a significant advantage by alleviating the investigative workload and shortening the learning curve for investigators [1]. However, it is still combined with risks such as information accuracy, hallucination impact, and legal barriers [3]. Although, this research contributes to the ongoing discourse on optimizing DF processes in response to the evolving landscape of criminal activities and the corresponding demands placed on investigative resources.

Contribution of this Work

- Design of a framework for DF investigations that operates based on natural language inputs
- Proposal of an innovative architecture for the reusability of subtasks, specifically tailored for repetitive prompts
- Introducing the concept of prompt engineering in the context of DF; generating DF specific subtasks

AI Agents - Roles

Task Translation Assistant (TTA)

- Translates complex task to set of subtasks.
- Keeps the communication with Chat Manager agent and the coder agent.
- Uses "5W1H" (Who, What, When, Where, Why, and How) for task decomposition

Chat Manager

- Manages the work-flow
- Prompts engineered to handle communication with TTA, Coder Agent and Report Agent

Coder Agent(s)

- Generates codes and executes them as per the provided instructions by the TTA and leverages deterministic DF "skills"
- Prompts engineered to behave as an experienced coder

Reporter Agent

- Generates reports as per the results given by the Coder Agent
- Prompts engineered to behave as an experienced forensic report writer.

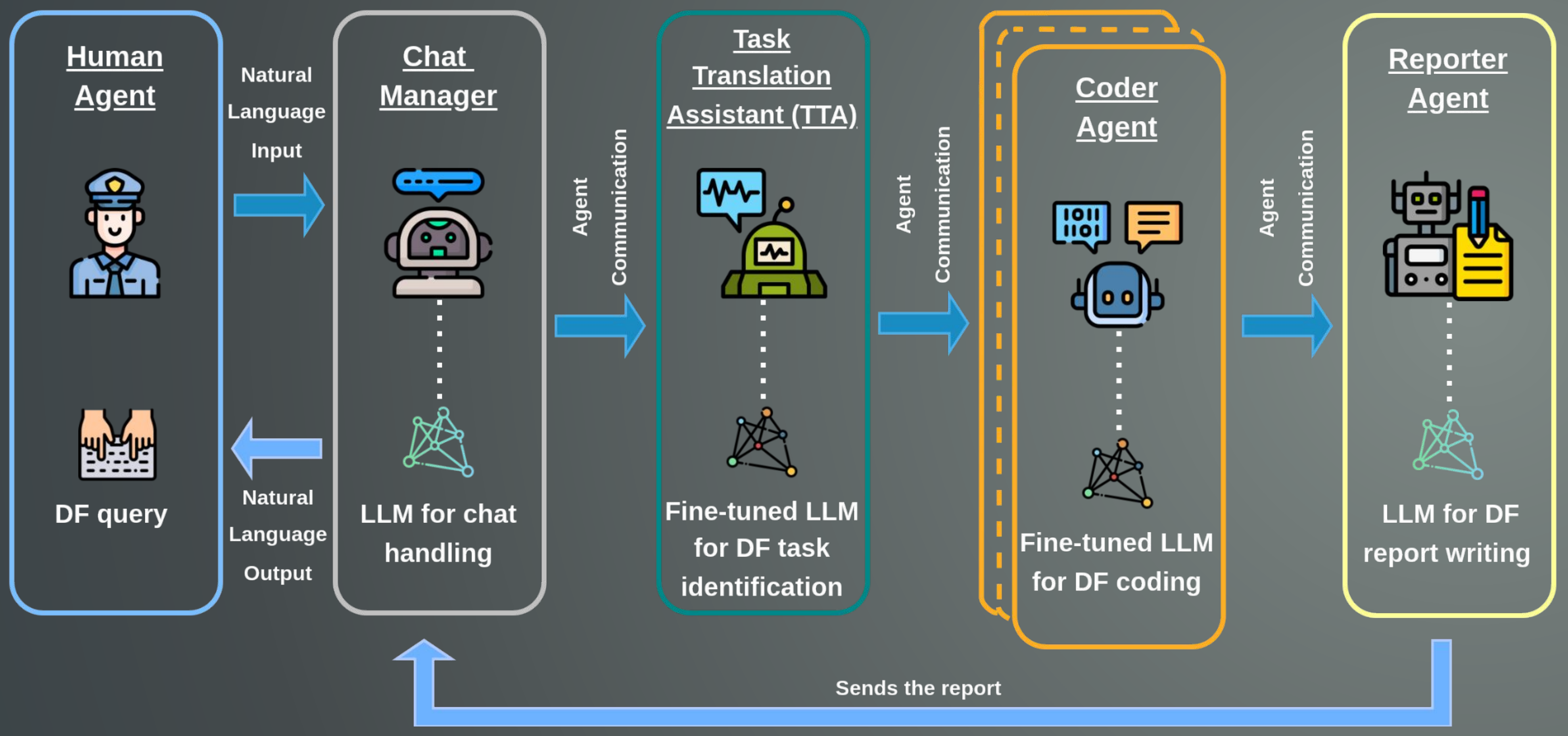

Figure 1. Architecture of the Proposed Framework.

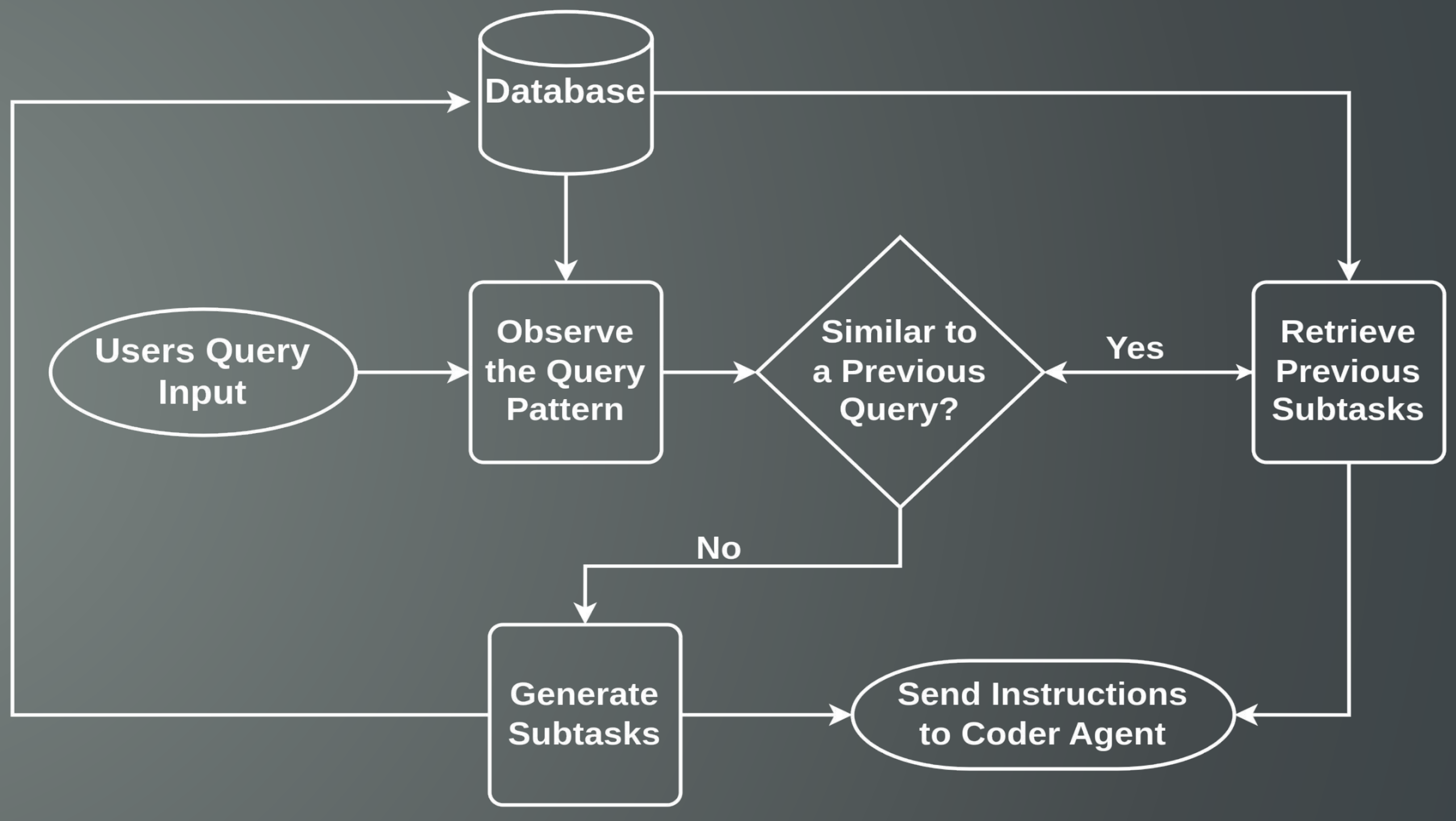
Database
Users Query Input
Observe the Query Pattern
Similar to a Previous Query?
Yes
Retrieve Previous Subtasks
No
Generate Subtasks
Send Instructions to Coder Agent

Figure 2. Flow Diagram of the Task Translation Assistant.

AutoGen

Open-Source Programming Framework for Agentic AI

The proposed framework will be built upon the AutoGen framework, integrating LLaMA and StarCoder LLMs alongside four AI agents [2]. Figure 1 depicts the high-level architecture of the framework, and outlines the role definitions of the AI agents and specifying the respective LLMs they will utilize.

Agent Roles

Possible to define number of roles for each agent

Possible to define actions of each role

Possible to add skills for agents

Skills

Python function to provide special pre-defined abilities

Models

Possible to combine multiple LLMs with each role

Possible to configure parameters like temperature and timeout

Work-flows

Possible to create separate work-flows

Task Translation Assistant (TTA)

TTA plays a crucial role in discerning whether the natural language query necessitates decomposition or warrants a direct response for the human agent. Task decomposition in the DF framework systematically considers key factors like executor, task nature, timeframe, location, and methodology to enhance clarity and precision. To address time inefficiencies for repeated queries, pre generated task decompositions are stored in a memory-based NoSQL database (e.g., Redis). As depicted in Figure 2, the system detects query patterns and retrieves pre-stored subtasks for similar inputs, reducing costs and processing time while dynamically updating the database for new queries.

Benefits And Risks

- **Benefits**
  - Reduces the learning curve for investigators.
  - Reduces the need for in-depth technical knowledge.
  - The framework makes DF tools more accessible (eliminating the requirement for coding expertise).
  - Significantly improves the efficiency of DF investigations.
  - Ability to tracks and refine responses to user prompts through dynamic interaction with stored prompts and decomposed task.
- **Risks**
  - Accuracy of the results will depend on the language proficiency of the investigator.
  - LLM hallucinations could affect the accuracy of generated report.
  - Adversarial attacks targeting LLMs pose a risk to the integrity of the framework.

REFERENCES

1. A. Wickramasekara and M. Scanlon, "A Framework for Integrated Digital Forensic Investigation Employing AutoGen AI Agents," *2024 12th International Symposium on Digital Forensics and Security (ISDFS)*, San Antonio, TX, USA, 2024, pp. 01-06, doi: 10.1109/ISDFS60797.2024.10527235.
2. Q. Wu, G. Bansal, J. Zhang, Y. Wu, B. Li, E. Zhu, L. Jiang, X. Zhang, S. Zhang, A. Awadallah, R. W. White, D. Burger, and C. Wang, "AutoGen: Enabling Next-Gen LLM Applications via Multi-Agent Conversation," *COLM 2024*, August 2024
3. A. Wickramasekara, F. Breitinger, and M. Scanlon, "Exploring the Potential of Large Language Models for Improving Digital Forensic Investigation Efficiency," FSI: Digital Investigation, vol. 52, Article 301859, 2025.