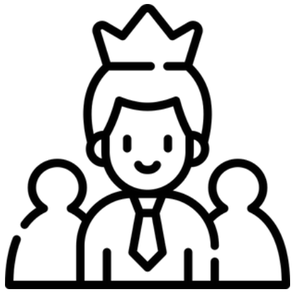
Hard Disk Forensics Automation System :

Analysis Assistant based on LLM with RAG

최경규*
강지혁
권승원
고은이

목차

팀원 소개



강지혁

역할

고은이

역할

권승원

역할

최경규

역할

LLM 모델 벤치마킹

RAG 흐름 설계

전체 시스템 통합 구현

발표 담당

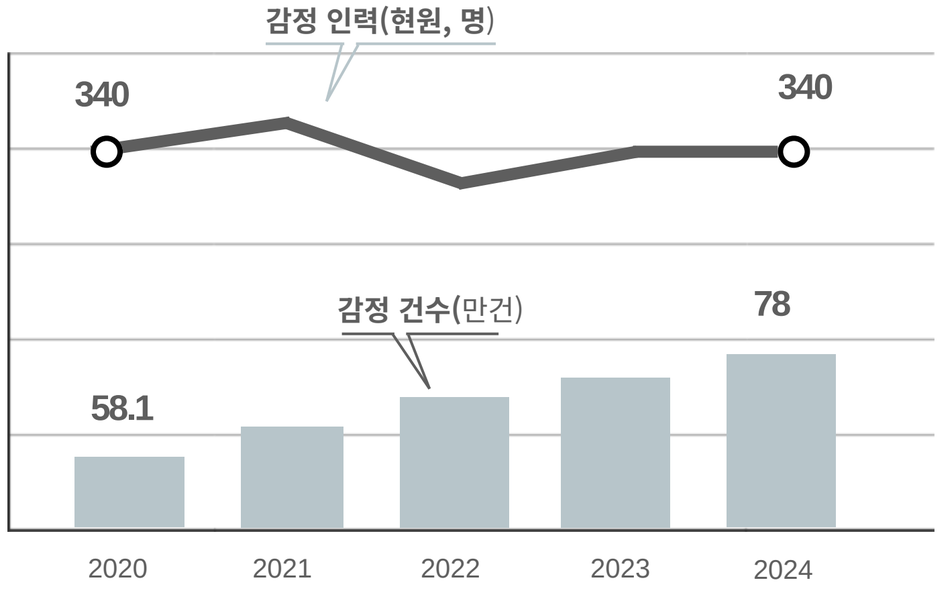
선정 이유

1. 기존 포렌식 도구의 한계

- 상용 도구들은 대부분 수동 또는 반자동 처리
- 대규모 환경에서의 효율적 분석 어려움

2. 자동화의 필요성

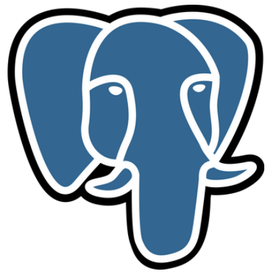
- 디지털 포렌식 업무의 약 2/3가 단순 반복 작업으로 구성
- 방대한 데이터를 신속·정확하게 분석하고, 사건별 증거 기반 추론 지원 필요
- 감정 건수는 매년 증가하지만 인력은 정체되어 1인당 분석 부담 증가

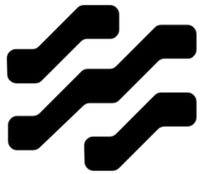


2024년 포렌식 감정 건수 2020년 대비 약 34% 증가

자료 출처: https://www.hankyung.com/article/202402273629i

기술 스택





Language

Python

DB

Milvus

PostgreSQL

LLM

Qwen3 4B

Gemini 2.5 Pro

cogito 671B

text-embedding-bge-reranker

text-embedding-paraphrase-multilingual-minilm-v2

etc..

MCP (Model Context Protocol)

KAPE

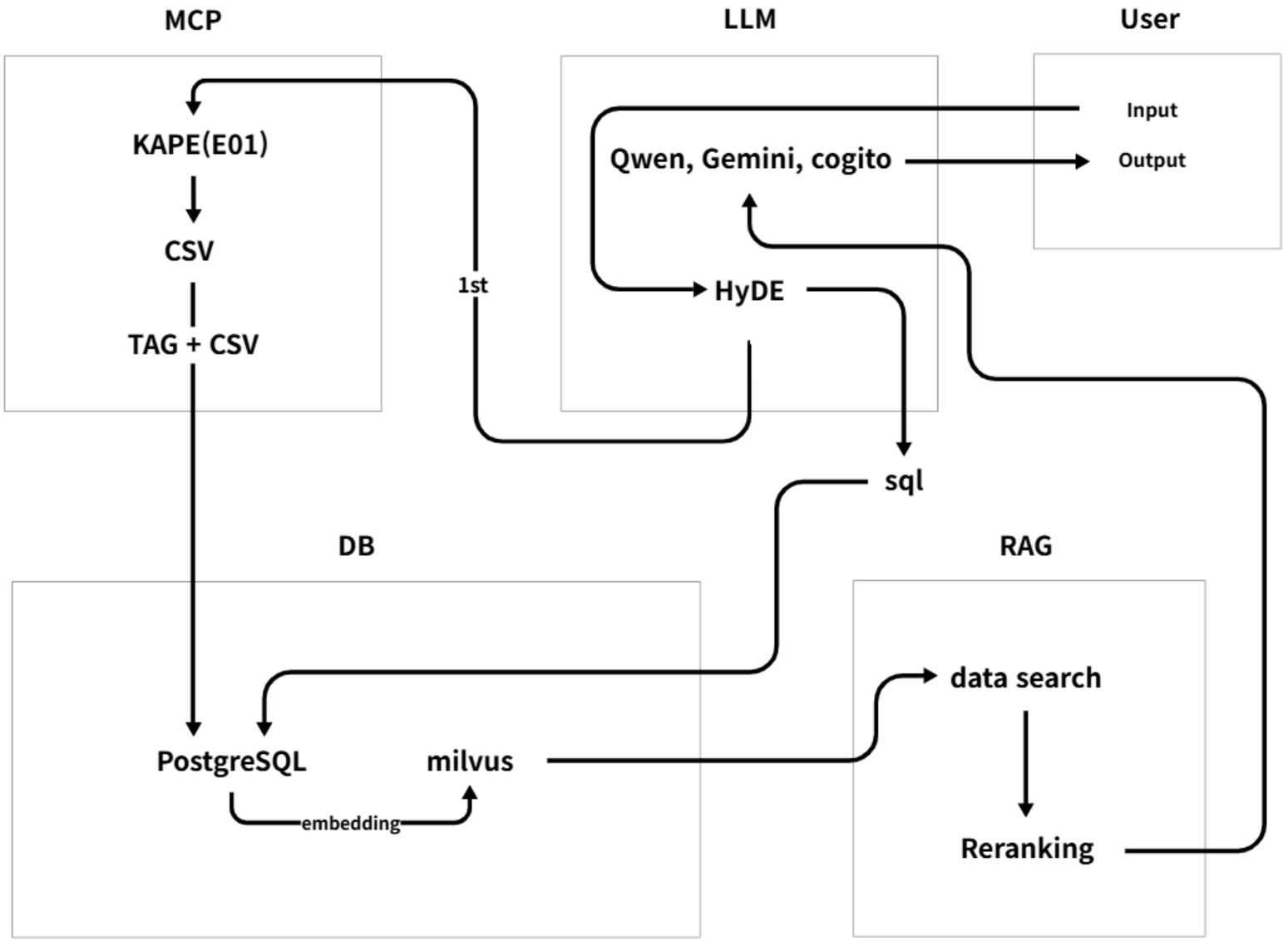
Arsenal Image Mounter

Langflow

LLM 모델 선정

구분	역할	모델/도구명	실행 형태	포맷/양자화	사용 목적/비고
LLM(벤치마킹)	로컬 후보 검증	qwen3 4B Thinking 2507 gguf	로컬 지향	GGUF(양자화)	로컬에서 돌릴 수 있는 LLM 기준선 확인 및 프롬프트 안정성/운영 가능성 평가
LLM(운영)	실제 분석 보조	Google Gemini CLI	클라우드	API/CLI	로컬 구축 난이도와 자원 제약으로 인해 실제 개발/실험 단계에서 활용
LLM(운영)	실제 분석 보조	Ollama cloud 모델: cogito-2.1:671b-cloud	클라우드	Ollama 런타임	로컬 한계를 보완하는 대체 실행 경로로 사용
Reranking	검색 결과 재정렬	bge-reranker-v2-m3-Q5_K_M-GGUF	로컬 지향	GGUF(양자화)	1차 검색 결과를 재정렬하여 근거 정확도 및 응답 신뢰도 개선
Embedding	임베딩(문서/쿼리 벡터화)	text-embedding-paraphrase-multilingual-minilm-v2.GGUF	로컬 지향	GGUF(양자화)	벡터DB에 저장할 문서 임베딩 생성 RAG 1차 검색 (Top-k) 품질 결정 요소

플로우 차트

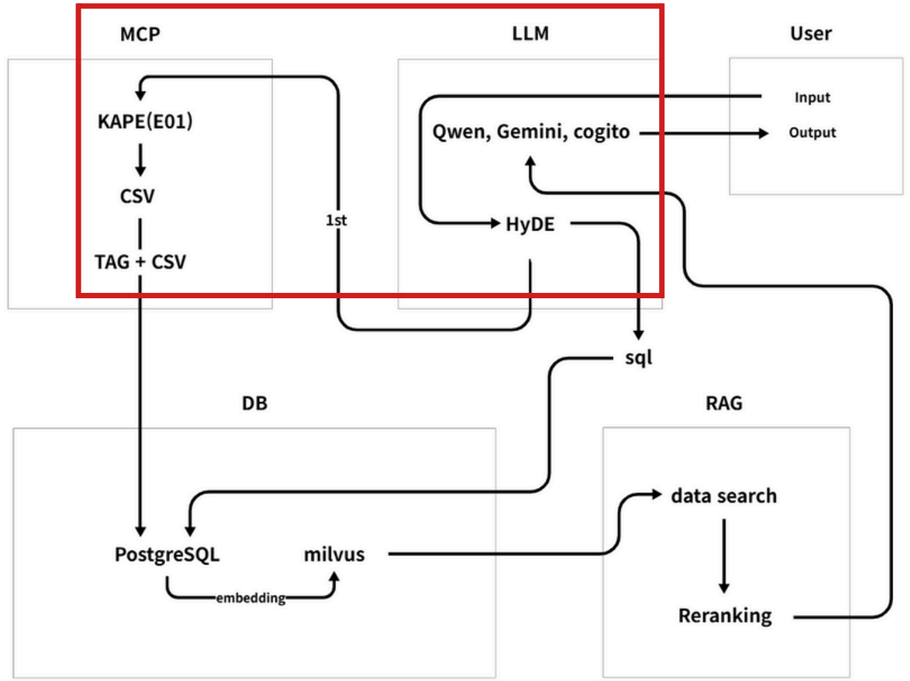

MCP
LLM
User
KAPE(E01)
CSV
TAG + CSV
1st
Qwen, Gemini, cogito
Input
Output
HyDE
sql
DB
RAG
PostgreSQL
milvus
embedding
data search
Reranking

MCP

MCP(호출 구간)

HyDE - 사용자의 질문에 대해서 LLM이 가상의 질문을 만들어
RAG 검색 성능을 향상 시키는 기법

사용자가 첫 질문 - HyDE 적용 후 MCP 자동 호출 - 분석 시작



HyDE 적용 전 질문

나는 흥분해서 서장에게 전화를 걸었다. "서장님, 거의 다 온 것 같아요!
채팅 하나만 더 하면 그녀의 마지막 위치를 알 수 있을 것 같습니다!"
그런데 딱 한 가지 문제가 있었다. 채팅 기록 전체가 암호화된 것 같았다.

질문: 채팅 비밀번호는 무엇인가요?
채팅 앱이 될 수 있는 모든 것을 파악하자

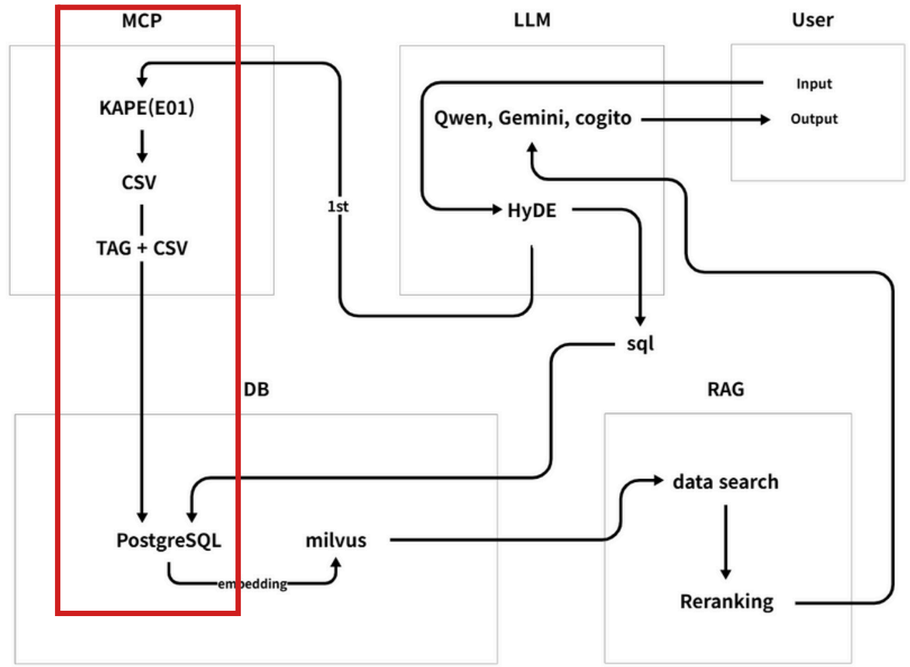
HyDE 적용 후 질문

"question": "암호화된 채팅 기록의 비밀번호를 알아내고,
해당 채팅 기록과 관련된 채팅 애플리케이션을 파악할 수 있을까?"

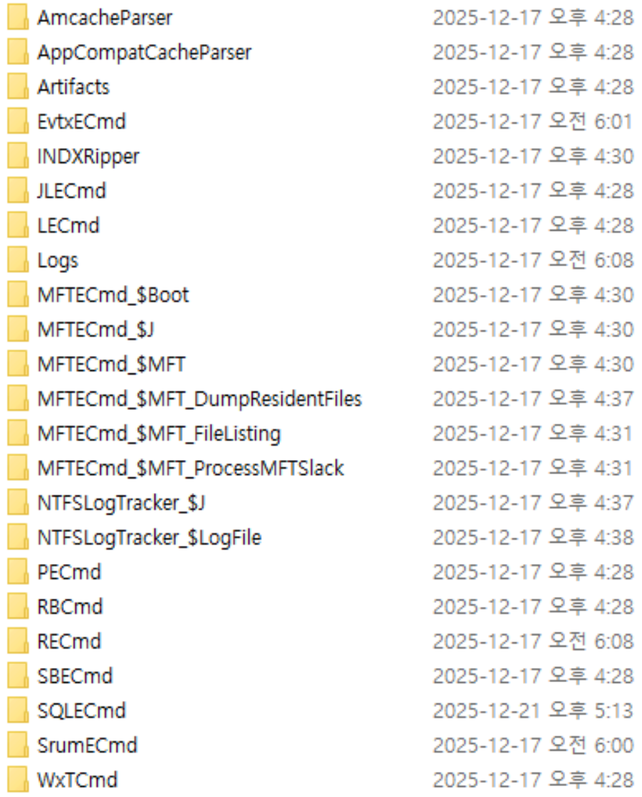
MCP

MCP(추출·정규화)

> Arsenal Image Mounter로 E01 이미지를 가상마운트
>
> 마운트 된 이미지에서 KAPE를 통해 아티팩트 추출 → **CSV 생성**
>
> CSV를 정규화 후 태그 부여
>
> 태깅된 아티팩트 CSV를 PostgreSQL에 적재



Colume	Type	Lastwritetimestamp	Description	Tags
설명	아티팩트 유형	마지막 작업 시간	로그 데이터	분석용 태그 데이터



추출된 아티팩트

E01 Image - CSV

273,273,2020-09-18 22:44:50.1930631,15,Info,SecurityCenter,Application,0,0,DESKTOP-SDN1RPT.C137.local,4,,Windows Security Center State Changed,,,Updated Windows Defender status successfully to SECURITY_PRODUCT_STATE_ON.,,,,,,,False,E:\Kape Output\G\Artifacts\G\Windows\System32\winevt\logs\Application.evtx,0x80000000000000,0,"{""EventData"":{""Data"":""Windows Defender, SECURITY_PRODUCT_STATE_ON"",""Binary"":""""""}}"

Tagging - CSV

Type : eventlog_15
Lastwritetimestamp: 2020-09-18 22:44:43
Description : "TimeCreated : 2020-09-18 22:44:43.6770729 | Channel : Application | Provider : SecurityCenter | EventID : 15 | Computer : DESKTOP-SDN1RPT.C137.local | Message : {""EventData"":{""Data"":""Windows Defender SECURITY_PRODUCT_STATE_ON"",""Binary"":""""""}}"
Tags: ARTIFACT_EVENT_LOG|EVENT_ACCESSED|STATE_ACTIVE|TIME_CREATED|TIME_OLD

DB

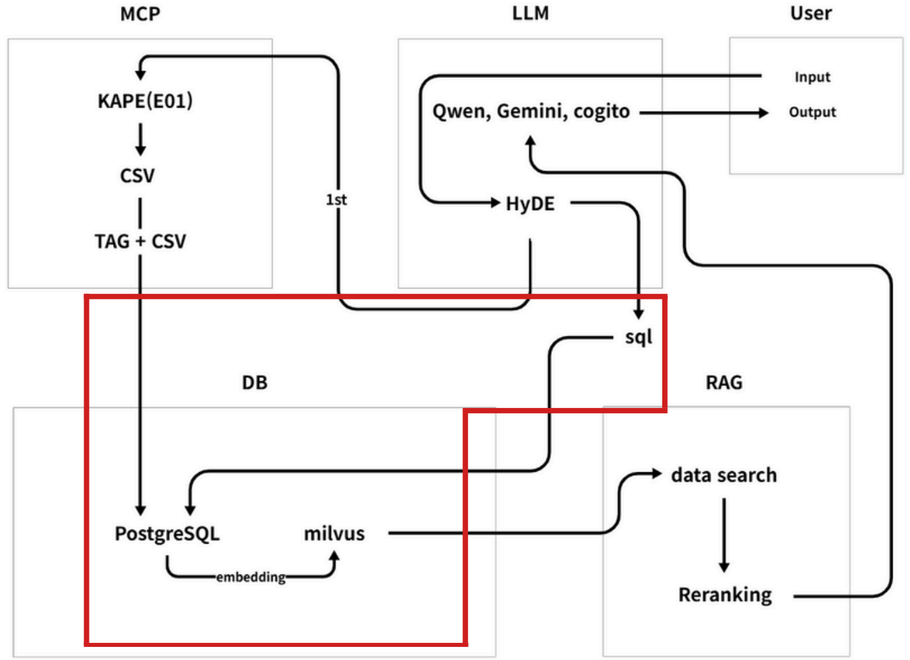
DB(1차 후보 축소·아티팩트 Embedding 구간)

HyDE 에서 만들어낸 태그 기반 SQL쿼리를 생성

PostgreSQL에 저장된 아티팩트를 1차 후보로 축소

↓

축소된 레코드를 벡터화(384차원) 시킨 데이터를 **Milvus(VDB)에 저장**




```
[INFO][Worker-3] 임베딩 완료 (96개, 9.76초, device=cpu)
[INFO][Worker-3] Milvus insert 완료 (96개) - 예: [7532648, 7532653, 7532658]...
[INFO][Worker-3] 96개 row 조회 (last_id=7533603, 누적=192)
[INFO][Worker-2] 임베딩 완료 (96개, 11.06초, device=cpu)
[INFO][Worker-2] Milvus insert 완료 (96개) - 예: [7532647, 7532652, 7532657]...
[INFO][Worker-2] 96개 row 조회 (last_id=7533602, 누적=192)
[INFO][Worker-0] 임베딩 완료 (96개, 11.36초, device=cpu)
[INFO][Worker-0] Milvus insert 완료 (96개) - 예: [7532645, 7532650, 7532655]...
[INFO][Worker-0] 96개 row 조회 (last_id=7533600, 누적=192)
[INFO][Worker-1] 임베딩 완료 (96개, 13.12초, device=cpu)
[INFO][Worker-1] Milvus insert 완료 (96개) - 예: [7532646, 7532651, 7532656]...
[INFO][Worker-1] 96개 row 조회 (last_id=7533601, 누적=192)
[INFO][Worker-4] 임베딩 완료 (96개, 13.68초, device=cpu)
[INFO][Worker-4] Milvus insert 완료 (96개) - 예: [7532644, 7532649, 7532654]...
[INFO][Worker-4] 96개 row 조회 (last_id=7533599, 누적=192)
```

하이드에서 생성한 태그 기반으로 쿼리문 생성 → DB → 추출된 내용은 VDB에 저장

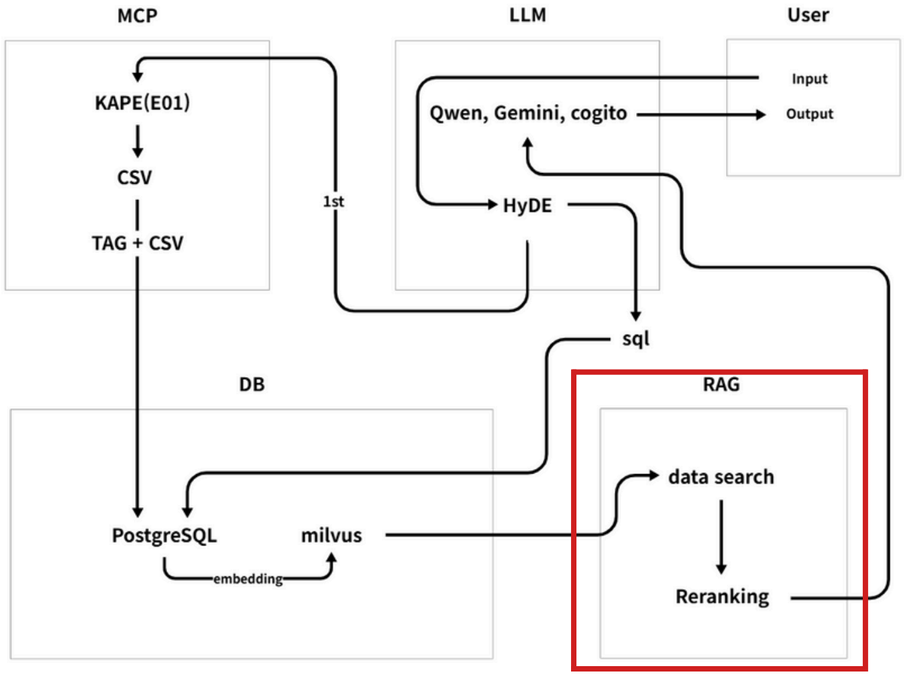

```
"keywords": [],
"ARTIFACT": ["ARTIFACT_AMCACHE","ARTIFACT_PREFETCH"],
"EVENT": ["EVENT_RECOVERED","EVENT_EXECUTED"],
"AREA": ["AREA_APPDATA_LOCAL","AREA_PROGRAMFILES"],
"SEC": ["SEC_CREDENTIAL_ACCESS"],
"FORMAT": ["FORMAT_DATABASE","FORMAT_LOG"],
"ACT": ["ACT_SEARCH","ACT_EXECUTE"],
"TIME": [],
"STATE": ["STATE_ENCRYPTED"],
"time_parsed": {"type": "none","start": null,"end": null}
```


하이드에서 나온 태깅된 아티팩트에 적용되는 쿼리문

```
  type,
  lastwritetimestamp,
  description,
  tag
FROM artifact_all
WHERE
  (
    type = ANY(ARRAY['ARTIFACT_AMCACHE','ARTIFACT_PREFETCH']::text[])
    OR regexp_split_to_array(replace(tag, ' ', ''), '[|,]') && ARRAY['ARTIFACT_AMCACHE','ARTIFACT_PREFETCH']::text[]
  )
  AND
  (
    regexp_split_to_array(replace(tag, ' ', ''), '[|,]') && ARRAY['EVENT_RECOVERED','EVENT_EXECUTED']::text[]
    OR regexp_split_to_array(replace(tag, ' ', ''), '[|,]') && ARRAY['AREA_APPDATA_LOCAL','AREA_PROGRAMFILES']::text[]
    OR regexp_split_to_array(replace(tag, ' ', ''), '[|,]') && ARRAY['FORMAT_DATABASE','FORMAT_LOG']::text[]
    OR regexp_split_to_array(replace(tag, ' ', ''), '[|,]') && ARRAY['ACT_SEARCH','ACT_EXECUTE']::text[]
    OR regexp_split_to_array(replace(tag, ' ', ''), '[|,]') && ARRAY['SEC_CREDENTIAL_ACCESS']::text[]
    OR regexp_split_to_array(replace(tag, ' ', ''), '[|,]') && ARRAY['STATE_ENCRYPTED']::text[]
  )
ORDER BY lastwritetimestamp;
```

RAG

벡터 검색 1000개 ➡ Reranking 100개



Milvus(VDB)에서 질문과 유사한 아티팩트를 1차 검색

⬇

Reranking 모델이 **질문-근거 쌍을 다시 평가**해 근거로 압축

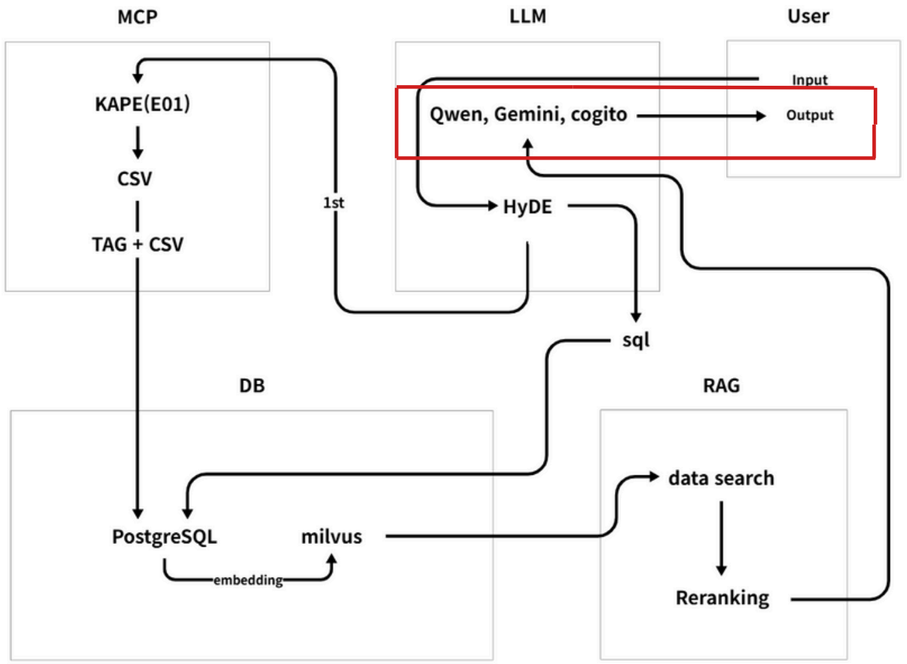
⬇

최종 K개를 LLM에 제공해 근거 기반 요약/해석 수행

RAG - 유사도 검색 - Reranking

LLM

Qwen, Gemini, Cogito



1. 근거로 사용된 원본 아티팩트 정보

2. result.txt - 출력 결과

번호	Type	Time	Description (요약)	원본 파일 경로	행번호	매칭률	상태
1	REG_UNKNOWN	2024-04-06 15:23	KeyPath : ROOT\Microsoft\Windows NT\Curr	D:₩Kape Output₩E₩RECmd₩Registry₩20251216170553_F	24	100%	찾음
2	REG_UNKNOWN	2024-04-06 15:23	KeyPath : ROOT\Microsoft\Windows NT\Curr	D:₩Kape Output₩E₩RECmd₩Registry₩20251216170624_F	161	100%	찾음
3	REG_BASIC_SYST	2024-04-06 15:23	KeyPath : ROOT\Microsoft\Windows NT\Curr	D:₩Kape Output₩E₩RECmd₩Registry₩20251216170637_F	60	100%	찾음

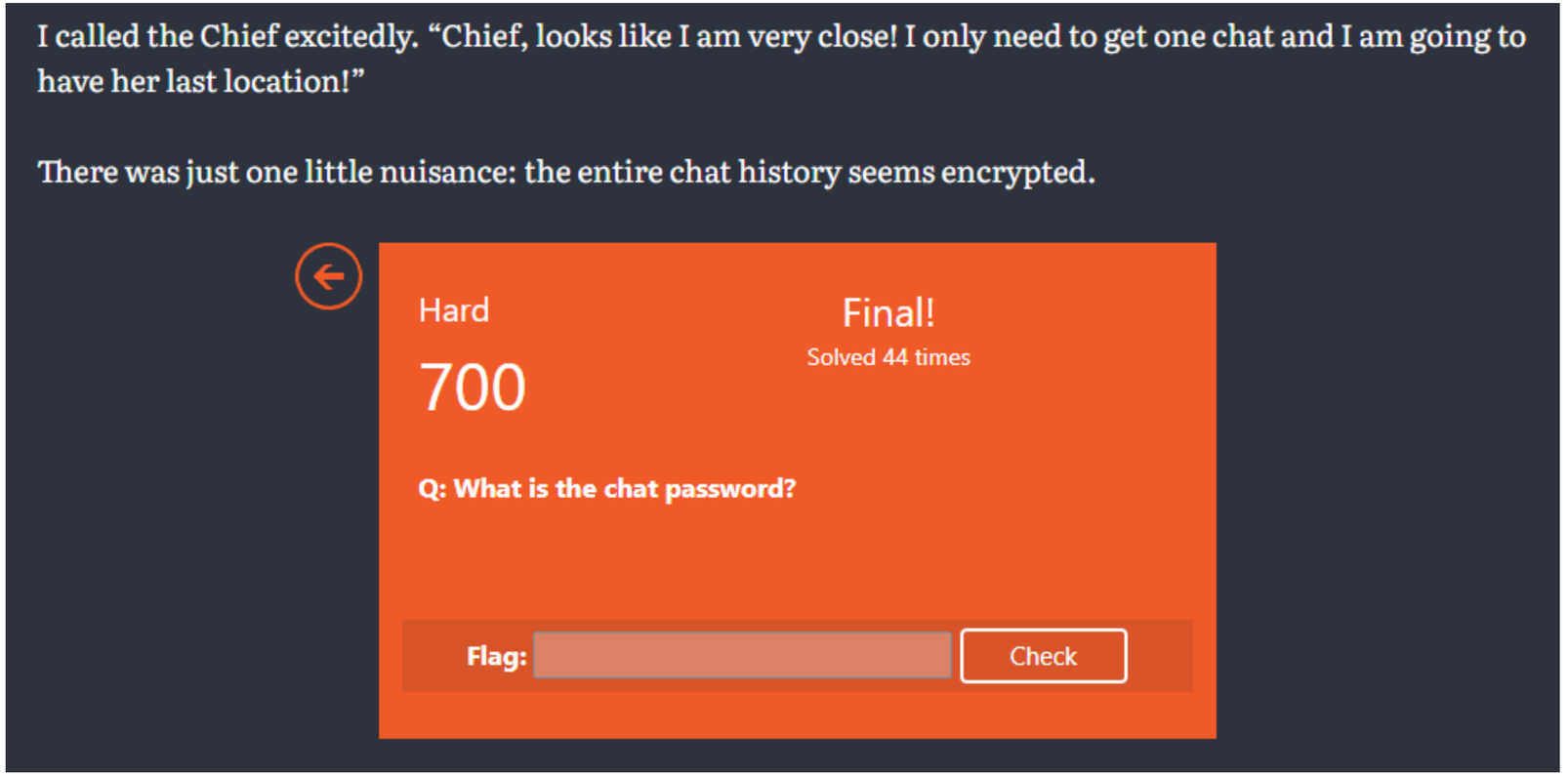
문제 풀이 통계

난이도	문제 수	풀이 성공	풀이 실패	통계(%)
하	16	16	0	99.99999
중	11	10	1	90.90
상	4	3	1	75

데모 문제

I called the Chief excitedly. “Chief, looks like I am very close! I only need to get one chat and I am going to have her last location!”

There was just one little nuisance: the entire chat history seems encrypted.



데모 영상

데모

영 상 넣 을 자 리

아쉬운 점

1. 로컬 환경 제약

- 로컬 환경의 제약으로 성능 좋은 LLM을 다루지 못함

2. 원래 추구했던 방향성

- 완전 자동화 포렌식 시스템을 만드는 것이 목표

→ 한계점 (계획했던 프로젝트의 규모가 큰 만큼 시간 문제나 데이터 유출이나 지속성 등)

향후...

1. 네트워크, 메모리 아티팩트 분석

- 네트워크 확장: PCAP을 Zeek/Suricata 로그로 표준화해 네트워크 증거 분석 기능 추가
- 메모리 확장: Volatility3 결과로 프로세스-네트워크-디스크 상관분석 강화

2. 일반 파일 내용 확인 기능 개선

- 텍스트 파일은 문자열을 추출해 내용 확인 기능 추가
- 일반 파일은 메타데이터 중심으로 정보를 제공하는 기능을 추가

Q&A

Question & Answer

감사합니다

Thank you for watching