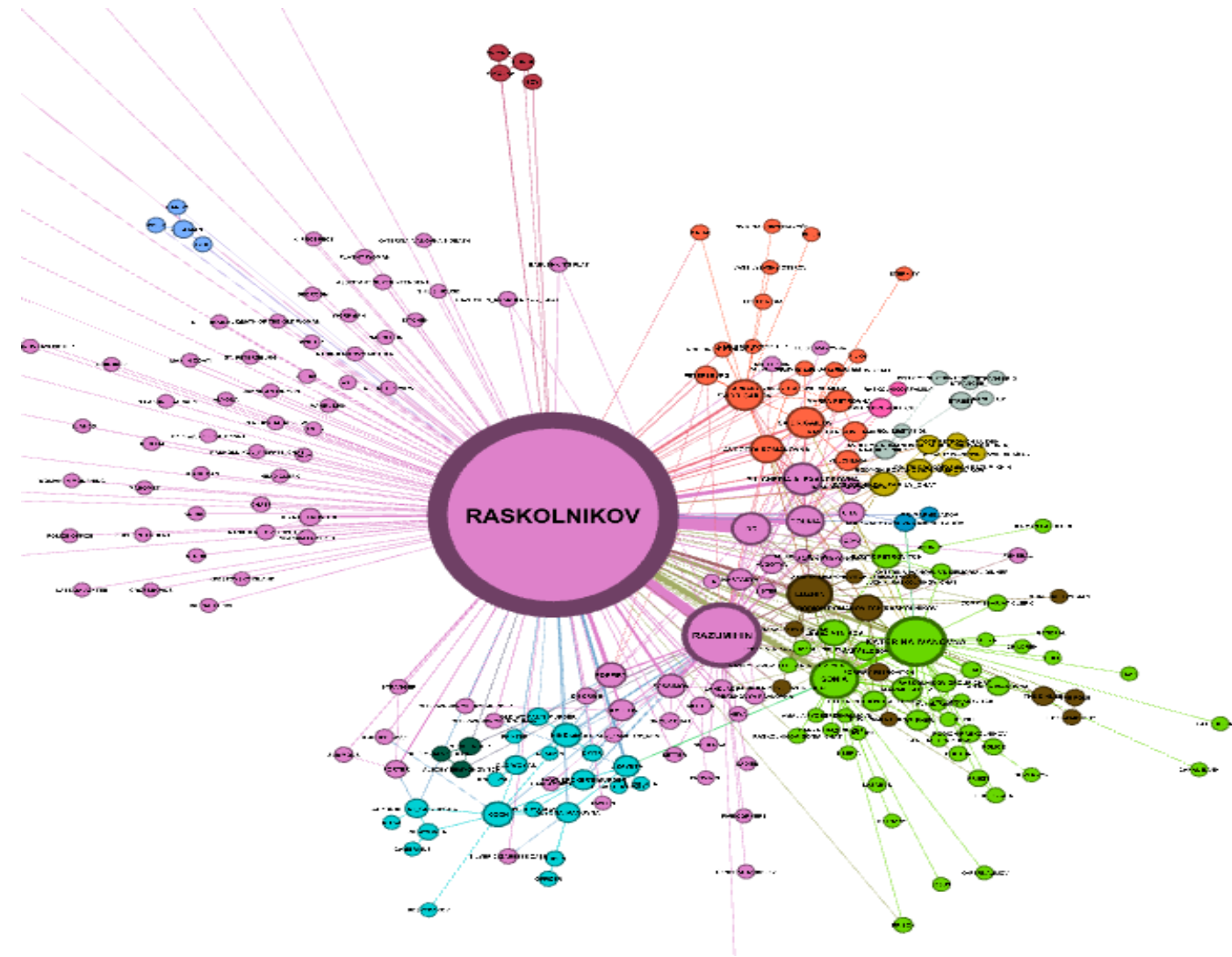


DF-Graph : Structured and explainable analysis of communication data for digital forensics

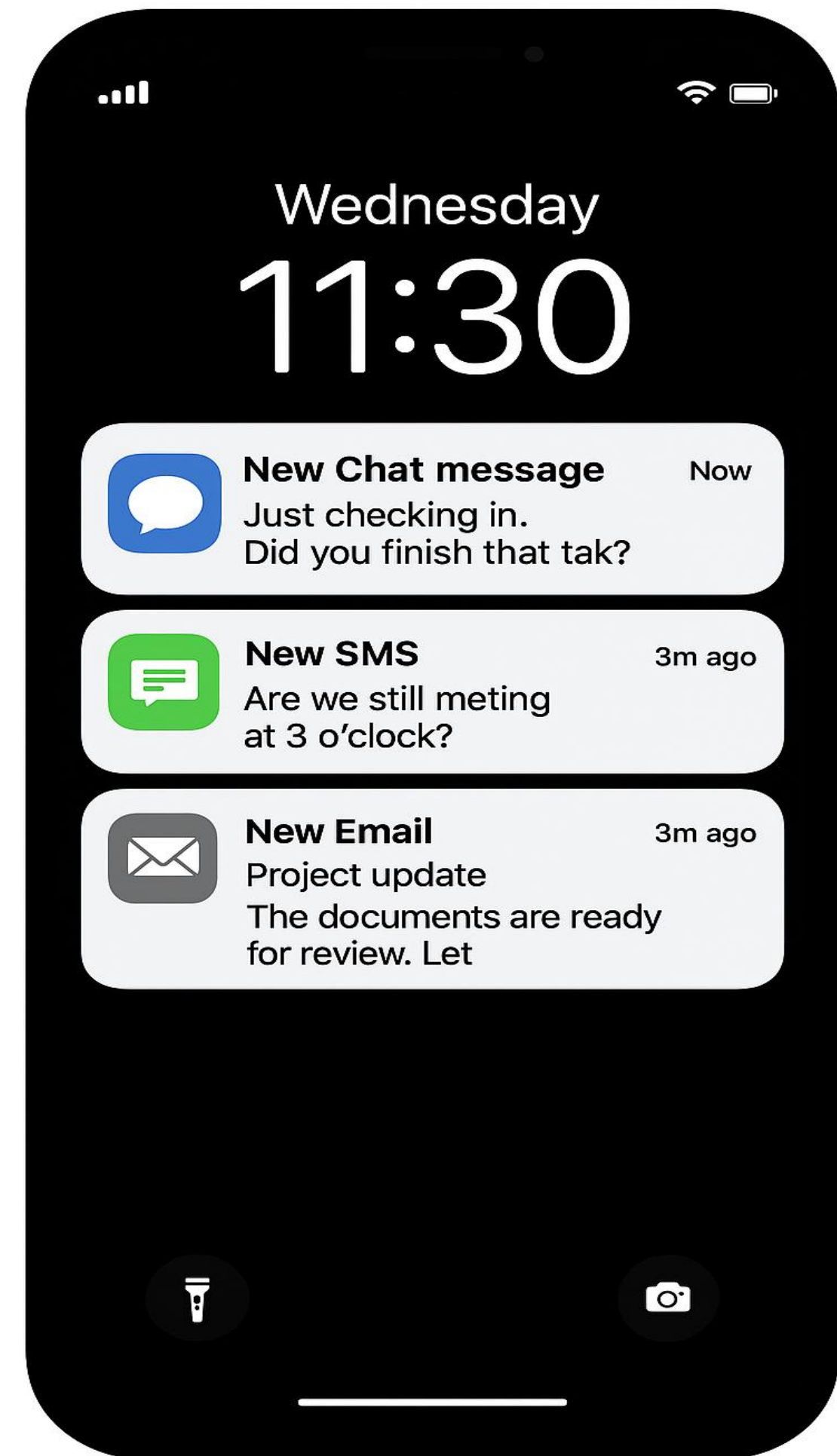


Motivation

Why communication data matters?

Communication data :
Chat messages, SMS logs, and emails

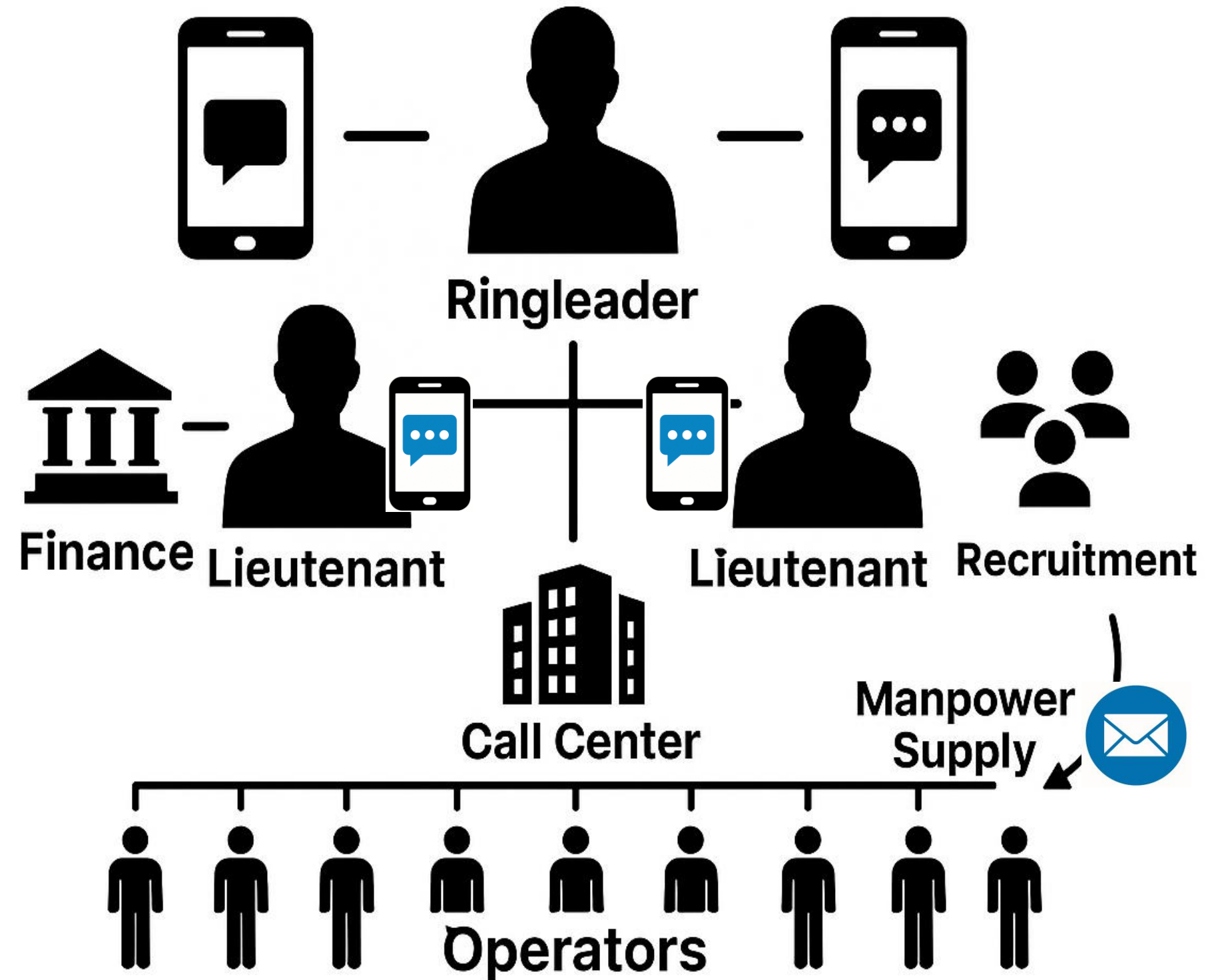
- Reveals motives, intent, relationships
- Rapidly increasing data volume
- Used as direct or indirect evidence



Motivation

Communication data as evidence

- In *voice phishing case*, text messages reveal organizational hierarchy
- In *serial murders case*, victim messages expose criminal motives
- In *fraud case*, emails show intentional deception

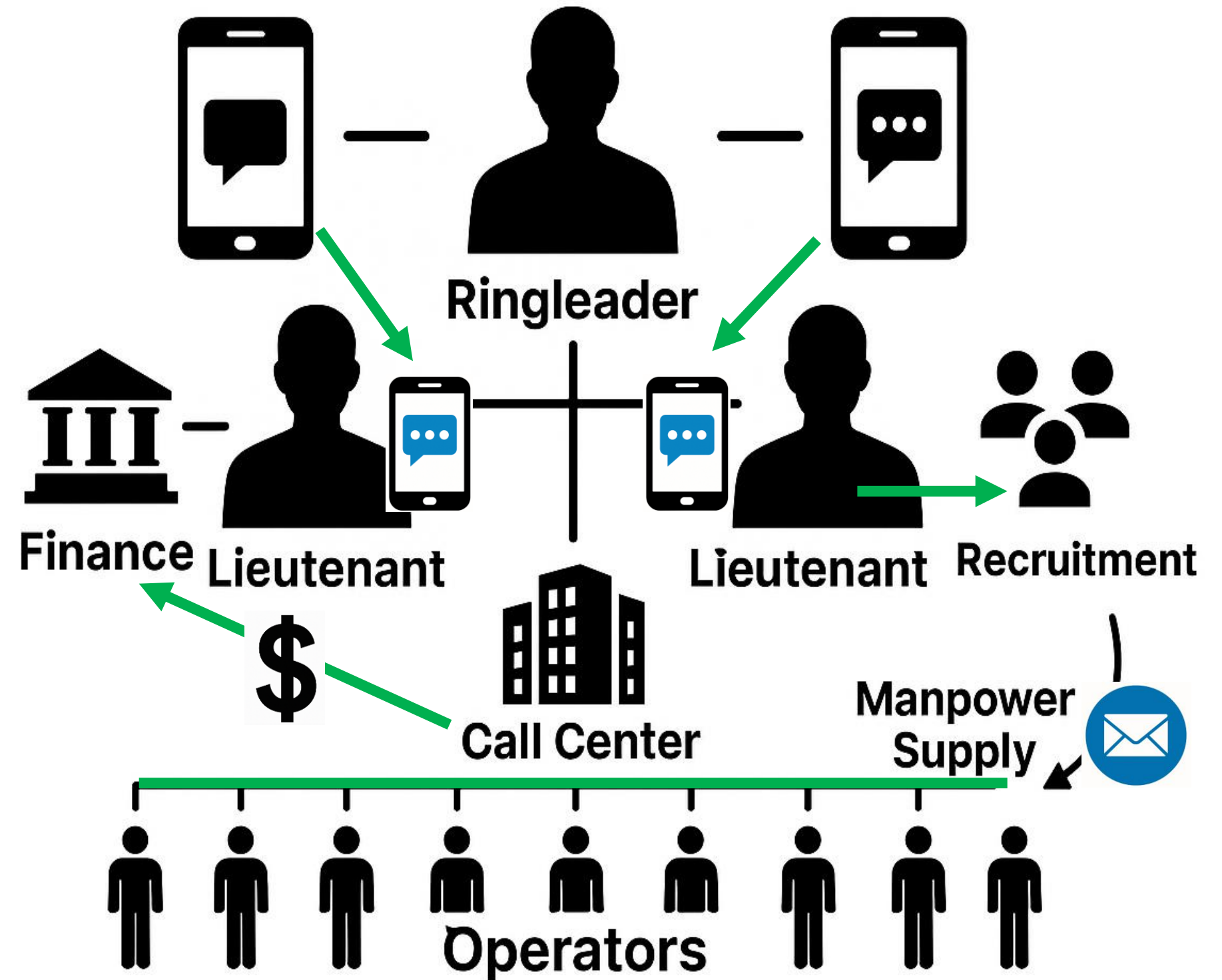


Criminal communication network
(e.g., a Voice phishing case)

Motivation

Communication data as evidence

- In *voice phishing case*, text messages reveal organizational hierarchy
- In *serial murders case*, victim messages expose criminal motives
- In *fraud case*, emails show intentional deception



Criminal communication network
(e.g., a Voice phishing case)

Motivation

Practical difficulties - Manual investigation

CALLS & IESSAGES ▾		III COLUMN ▾			
^ ⌵ ↺		Artifacts: 34			
Add custom time...		D	Time	Key details	To App
Locations ...			2021-03-07 A:03:32	Yep going back there soon. Know a...	📍
Open Maps			2021-03-07 0:38 I	Sell it... we need the cash	📍
Has Location			2021-03-07 0:38 I	Ok let's meet up today for the exch...	📍
Keyword search ...			2021-03-19 9:34 I	Ok I need time to find the cash	📍
cash			2021-01-99 9:38 I	Ok I can get the cash. Just need 48h...	📍
Categories ...			2021-01-97 7:30 :	I will be there bring the cash and yo...	📍
Calls			2021-01-31 12.43.	You there yet. Getting nervous carry...	📍
Contacts 3			2021-03-21 2 16h	Yer man. Which bit of that last mess...	📍
Files & media			2021-03-25 28:3h	Ok I can get the cash. Just need 48h...	📍
Messages 31			2021-03-25 301:1	Bring the cash Cooh meet at 6.	📍
			2021-03-25 08:3C	1000636914 1000636914	📍
			2021-03-25 02:31	1005369189 1605369189	📍
			2021-03-25 10:51	15631311822 1605396189	📍

Existing Tool: Keyword search (e.g., "cash") → Result list

Motivation

Practical difficulties - Manual investigation

CALLS & IESSAGES ▾

^

Add custom time...

Locations

Open Maps

Has Location

Keyword search

cash

Categories

Calls

Contacts3

Files & media

Messages31

III COLUMN ▾

Artifacts: 34

D	Time	Key details	To	App
	2021-03-07 A:03:32	Yep going back there soon. Know a...		
	2021-03-07 0:38	Sell it... we need the cash		
	2021-03-07 0:38	Ok let's meet up today for the exch...		
	2021-03-19 9:34	Ok I need time to find the cash		
	2021-01-99 9:38	Ok I can get the cash. Just need 48h...		

2021-03-25 20:31

2021-03-25 301:1

2021-03-25 08:30

2021-03-25 02:31

2021-03-25 10:51

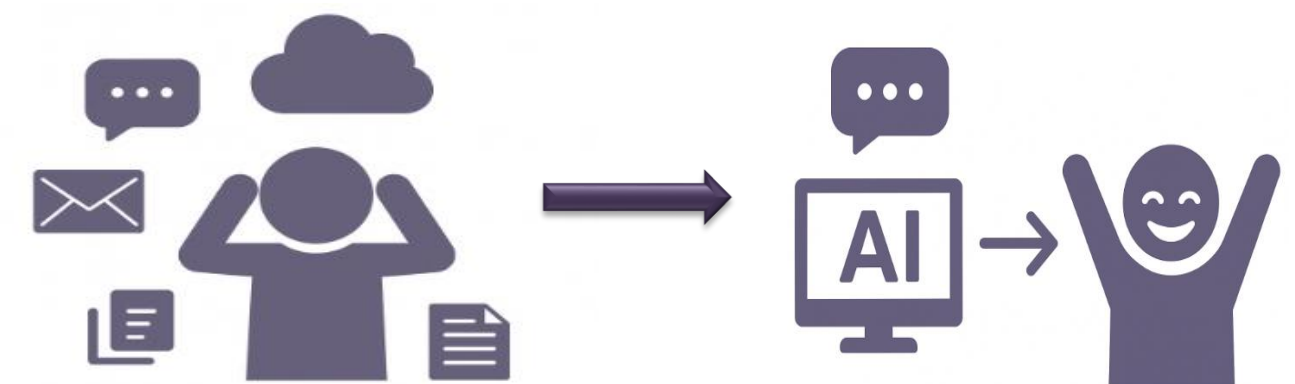
Investigator must open each item manually, read context, and connect related pieces to find real evidence.

Time-consuming, fragmented, and error-prone



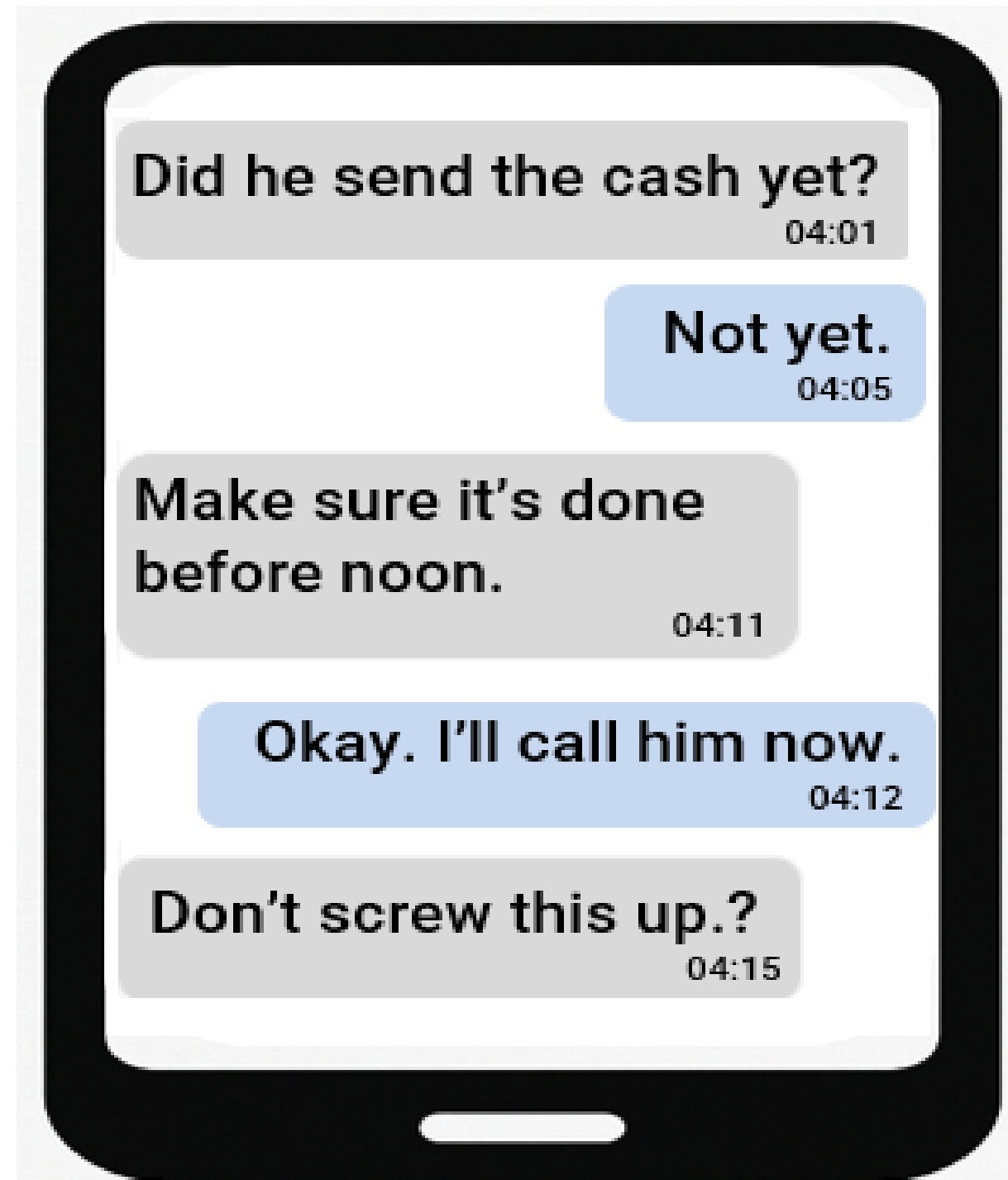
Existing Tool: Keyword search (e.g., “cash”) → Result list

How can LLMs reduce the manual burden of investigators?

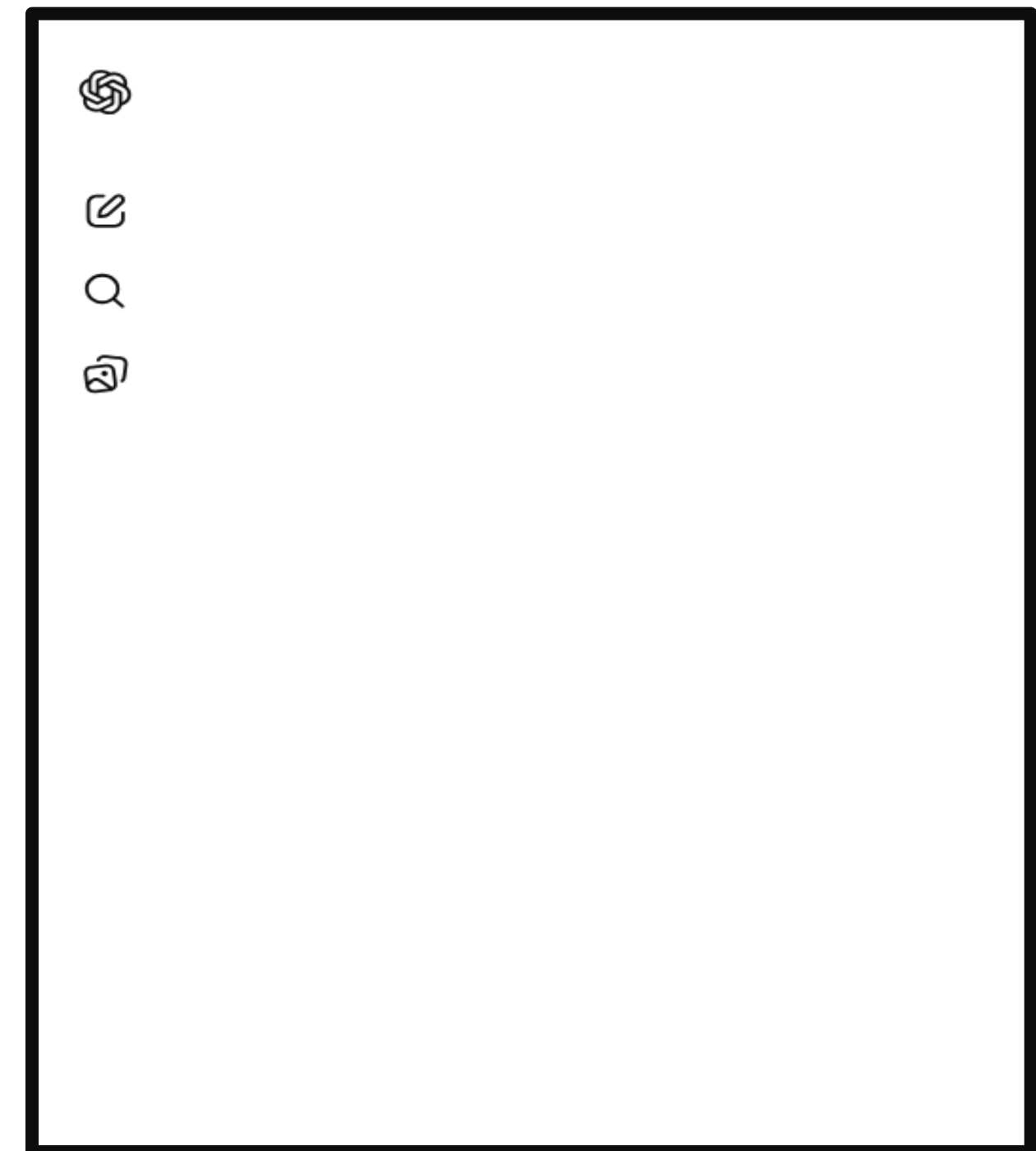


Challenges of applying LLMs in forensics

Real chat log (Voice phishing case)

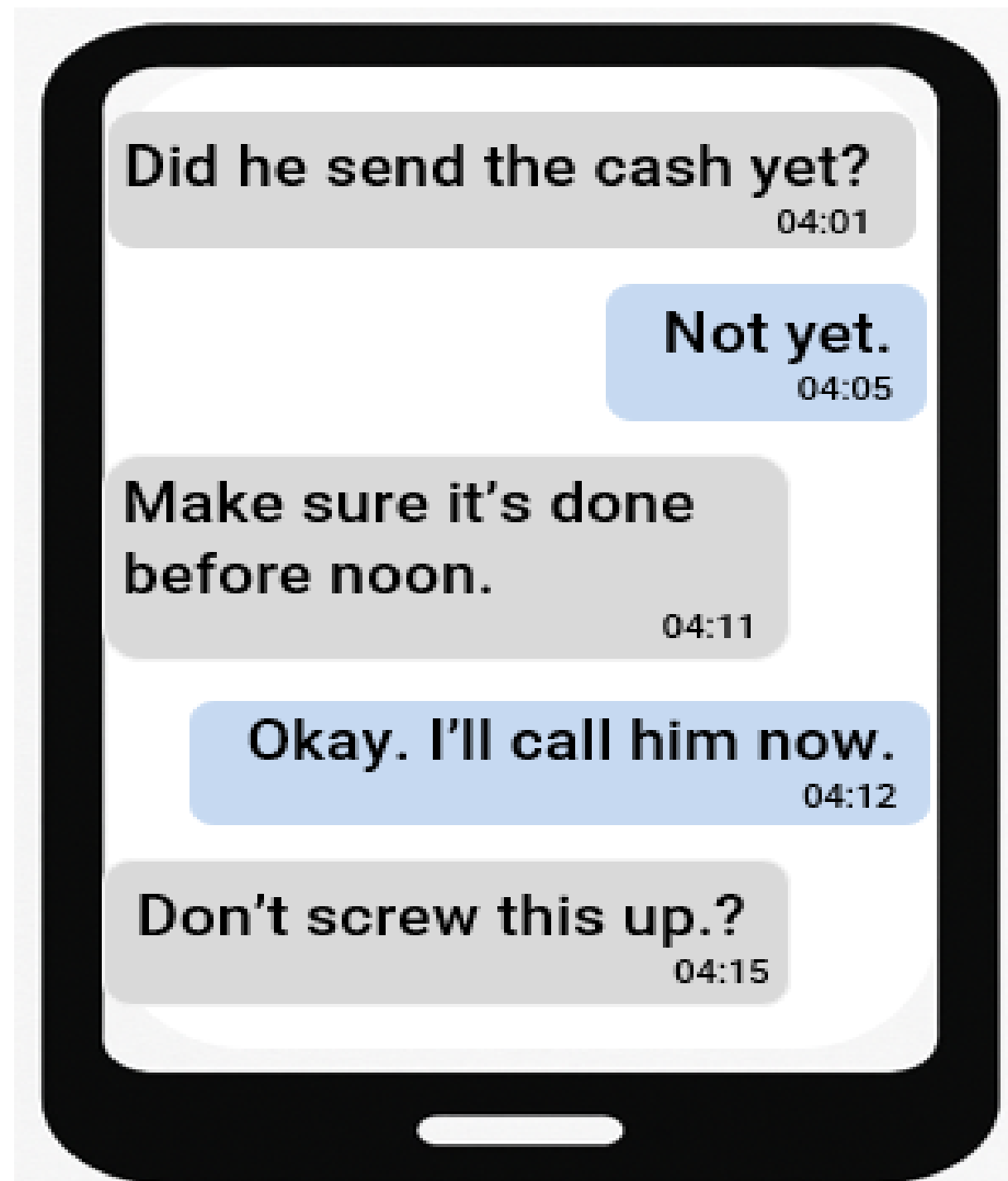


LLM's interpretation (AI's answer)

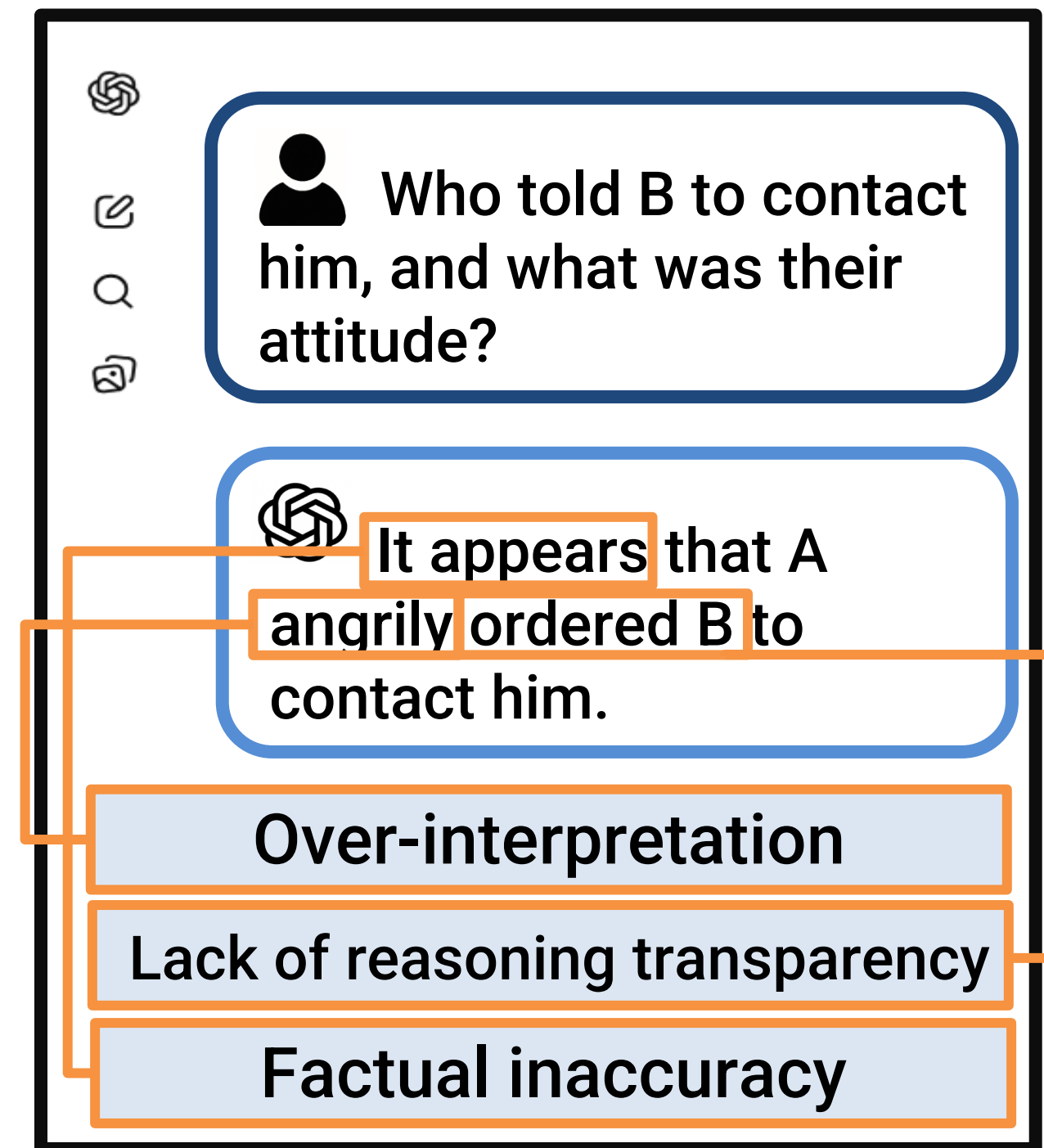


Challenges of applying LLMs in forensics

Real chat log (*Voice phishing case*)



LLM's interpretation(AI's answer)

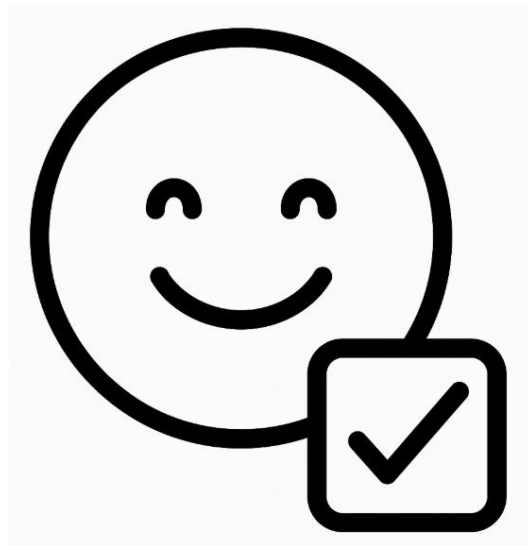


Can AI provide source-verifiable and trustworthy digital evidence analysis?



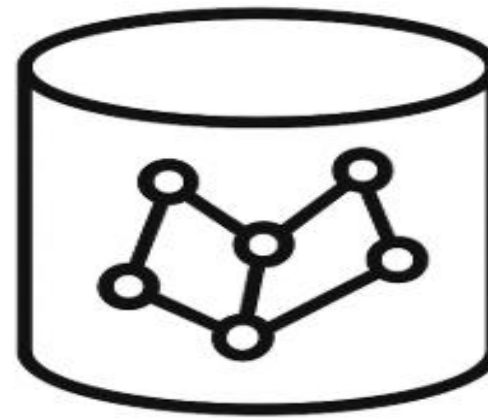
Design principles for DF-Graph

Explicit reasoning path



Explainability

Scalable reasoning over
communication graphs



Structure

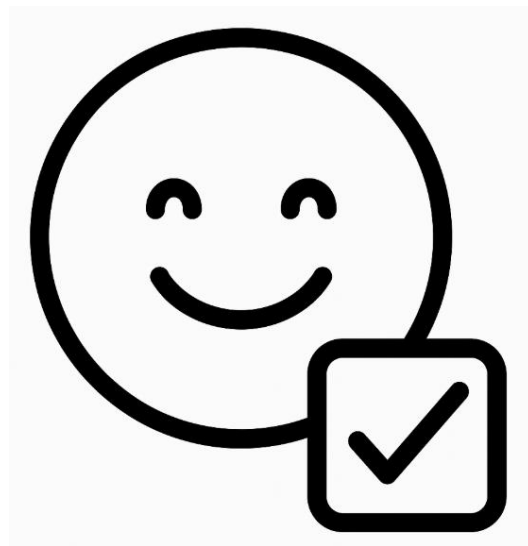
Evidence-grounded answer
generation



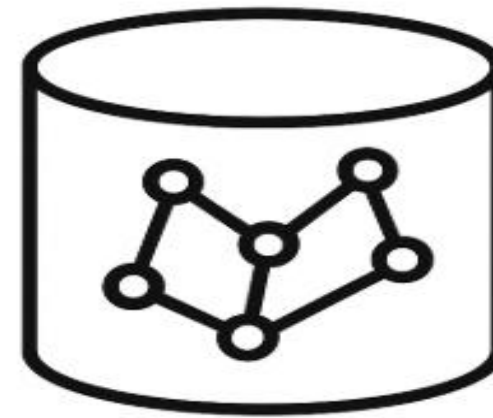
**Evidentiary
admissibility**

Design principles for DF-Graph

Explicit reasoning path



Scalable reasoning over communication graphs



Evidence-grounded answer generation



DF-Graph : Structured and explainable analysis of communication data for digital forensics

System design

System design : A structured and explainable solution

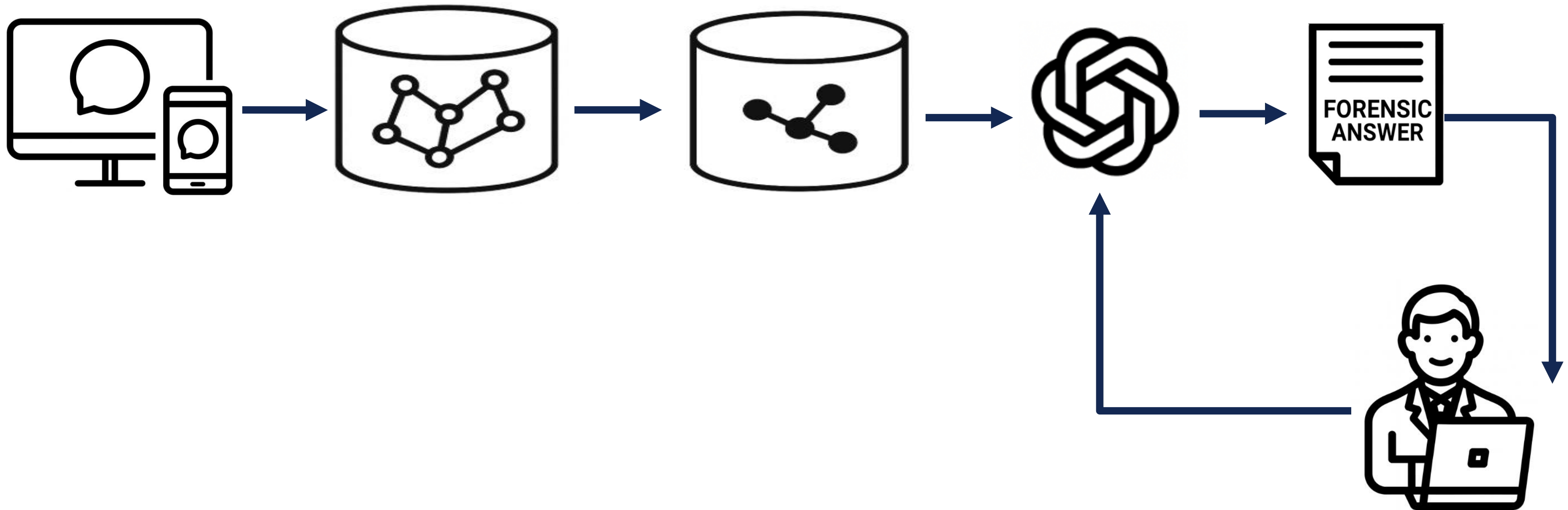
1.Data Acquisition
& Preprocessing

2.Graph
construction

3.Subgraph
retrieval

4.Evidence-guided
answer generation

5.Explainable
reasoning traces



Data Acquisition and Preprocessing

(1) Data Acquisition



(2) Data preprocessing : Parsing & Normalization

Sender	Receiver	Timestamp	Message Content
Raskolnikov	Sonia	2025-11-13 09:01:42	I couldn't sleep again last night.
Sonia	Raskolnikov	2025-11-13 09:02:15	You should come by the chapel today.
Raskolnikov	Psychologist	2025-11-13 09:03:28	I keep seeing her face – the old woman
Psychologist	Raskolnikov	2025-11-13 09:04:10	That's your conscience speaking, not her.
Raskolnikov	Psychologist	2025-11-13 09:05:22	The sound of the axe... sometimes just the word
Porfiry	Raskolnikov	2025-11-13 09:06:33	Care to finish our conversation, Mr. Raskolnikov?

Data Acquisition and Preprocessing

(1) Data Acquisition

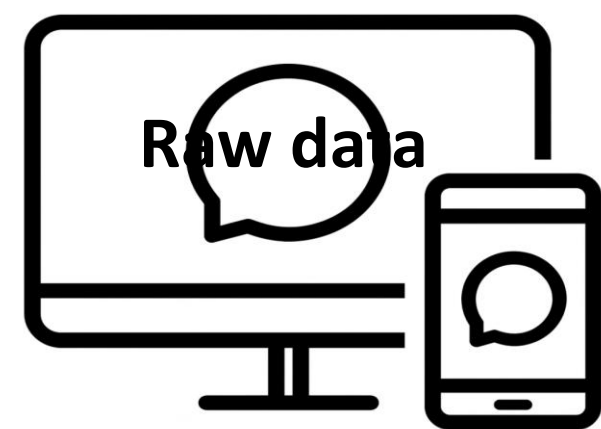


(2) Data preprocessing : Parsing & Normalization

Sender	Receiver	Timestamp	Message Content
Raskolnikov	Sonia	2025-11-13 09:01:42	I couldn't sleep again last night.
Sonia	Raskolnikov	2025-11-13 09:02:15	You should come by the chapel today.
Raskolnikov	Psychologist	2025-11-13 09:03:28	I keep seeing her face – the old woman
Psychologist	Raskolnikov	2025-11-13 09:04:10	That's your conscience speaking, not her.
Raskolnikov	Psychologist	2025-11-13 09:05:22	The sound of the axe... sometimes just the word
Porfiry	Raskolnikov	2025-11-13 09:06:33	Care to finish our conversation, Mr. Raskolnikov?

Data Acquisition and Preprocessing

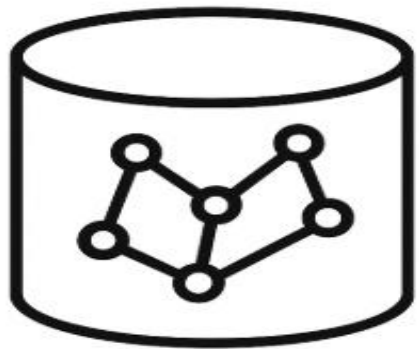
(1) Data Acquisition



(2) Data preprocessing : Anonymization

Sender	Receiver	Timestamp	Message Content
P_001	P_002	2025-11-13 09:01:42	I couldn't sleep again last night.
P_002	P_001	2025-11-13 09:02:15	You should come by the chapel today.
P_001	P_003	2025-11-13 09:03:28	I keep seeing her face – the old woman
P_003	P_001	2025-11-13 09:04:10	That's your conscience speaking, not her.
P_001	P_003	2025-11-13 09:05:22	The sound of the axe... sometimes just the word
P_004	P_001	2025-11-13 09:06:33	Care to finish our conversation, Mr. P_001 ?

Graph Construction



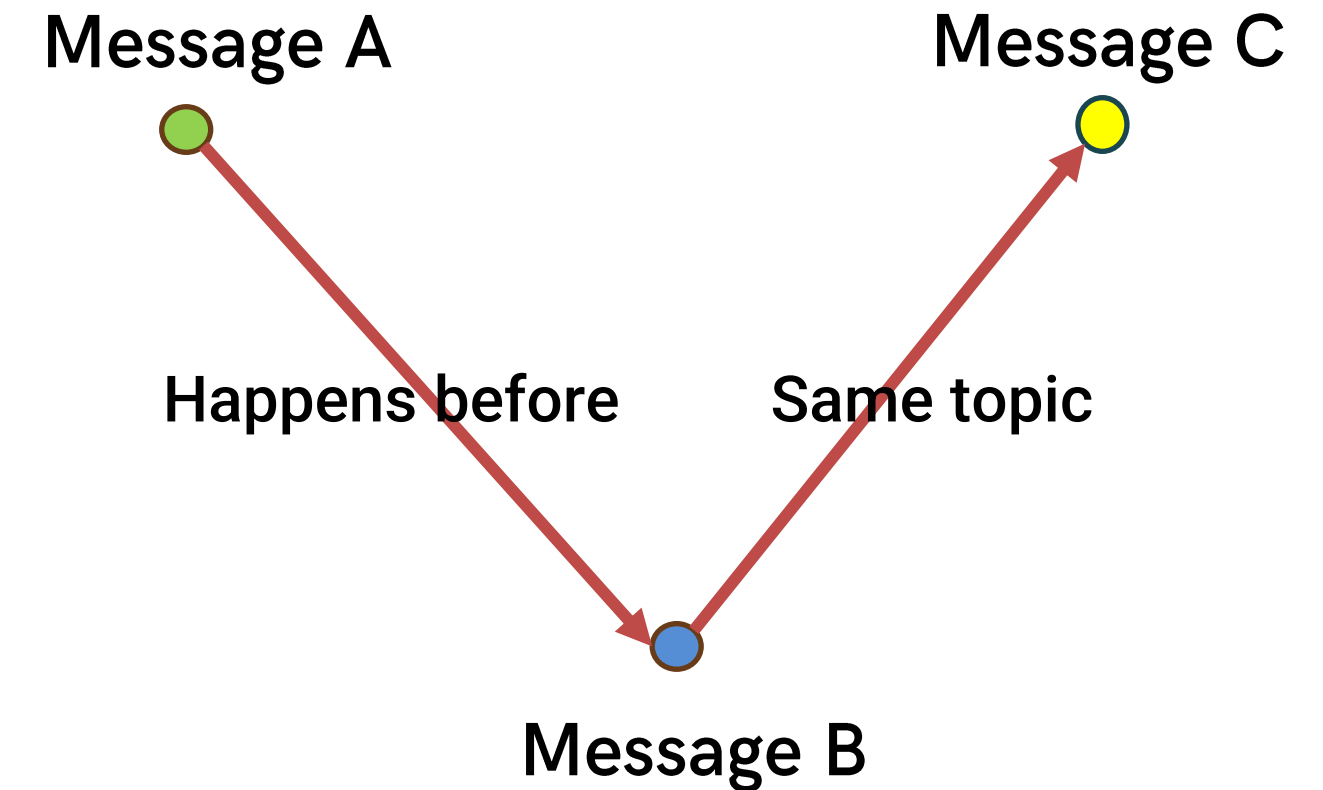
$$G = (V, E)$$

Node generation

- Messages
- Utterances

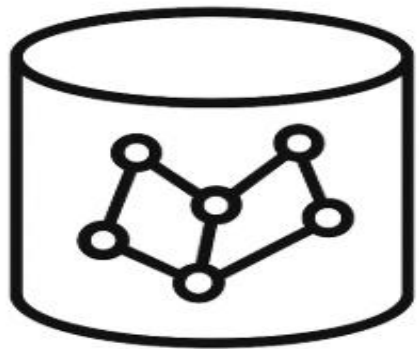
Edge generation

- Temporal edge:
chronological order
- Communication edge:
conversational continuity
- Semantic edge



Temporal & Communication edge

Graph Construction



$$G = (V, E)$$

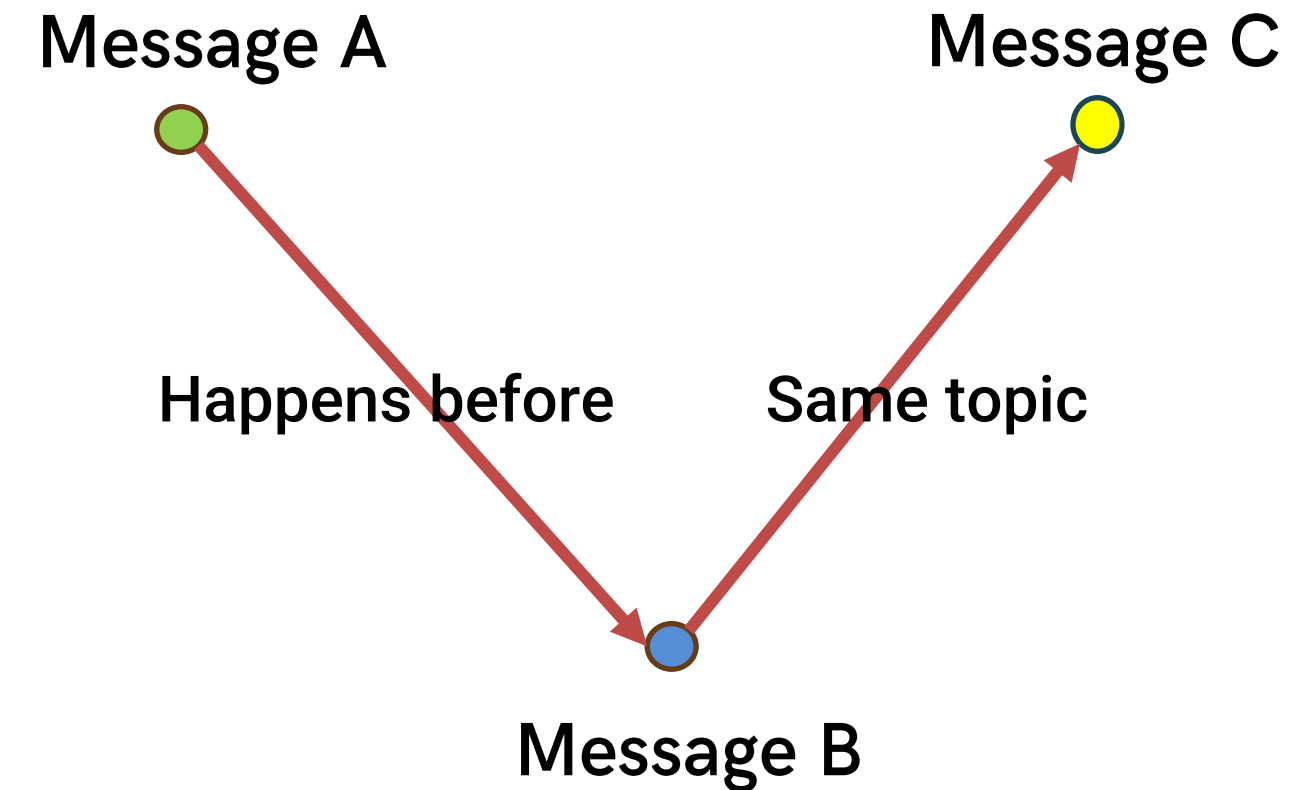
Node generation

- Messages
- Utterances

Edge generation

- Temporal edge:
chronological order
- Communication edge:
conversational continuity

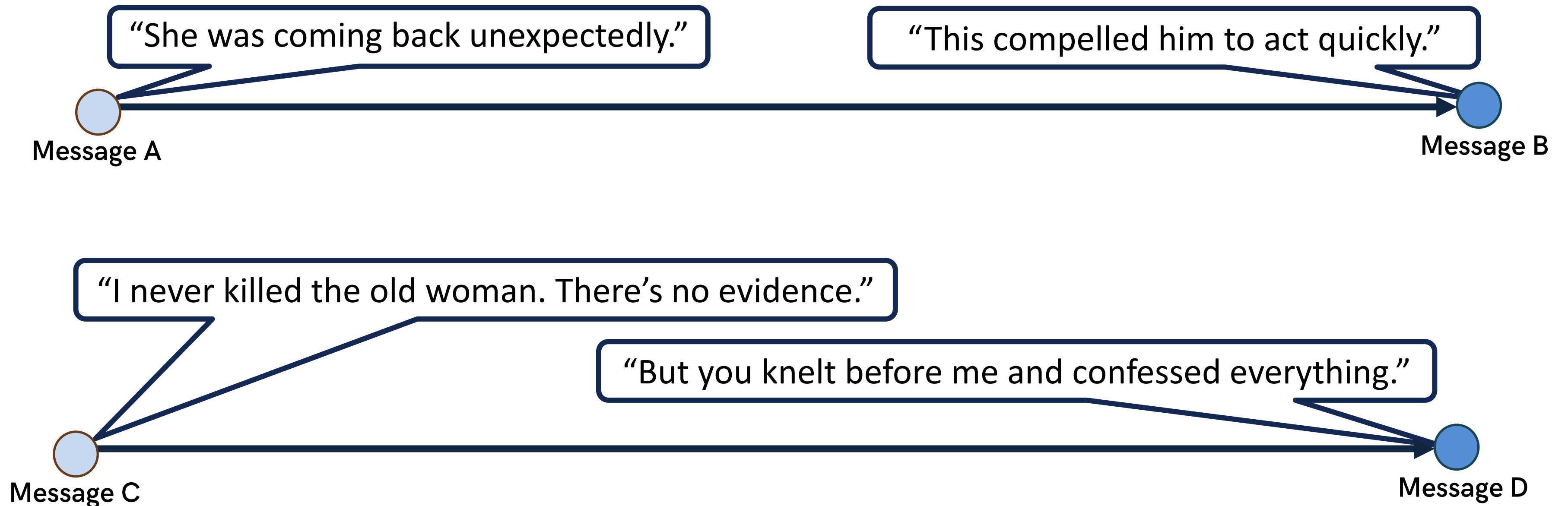
- Semantic edge → CAUSES, SUPPORTS, MENTIONS, and CONTRADICTS



Temporal & Communication edge

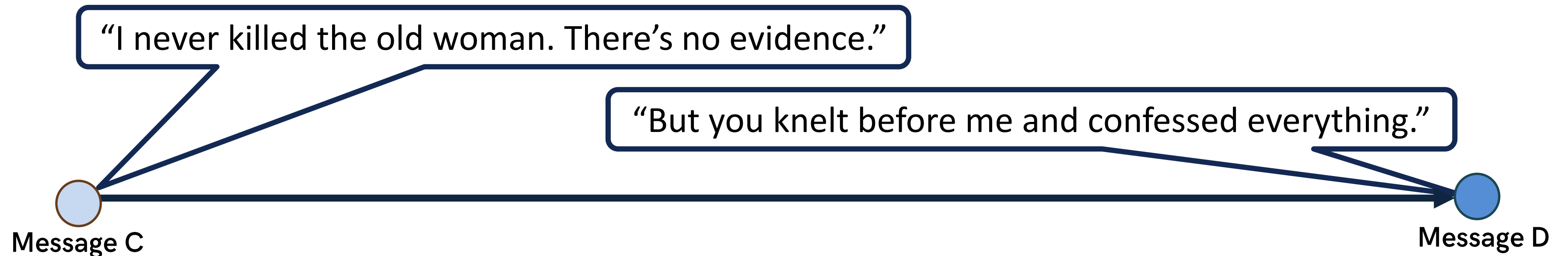
Graph Construction

Semantic edge : Meaning-based Connection



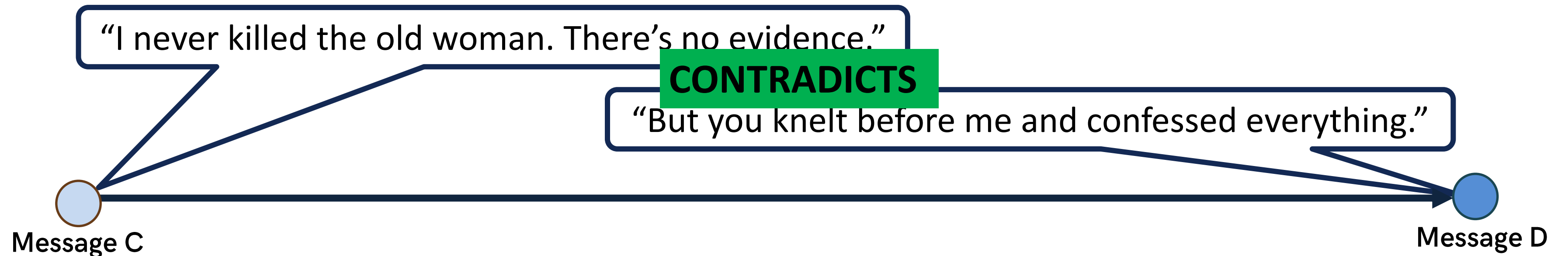
Graph Construction

Semantic edge : Meaning-based Connection

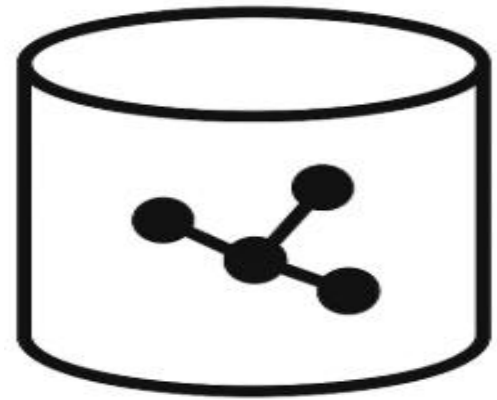


Graph Construction

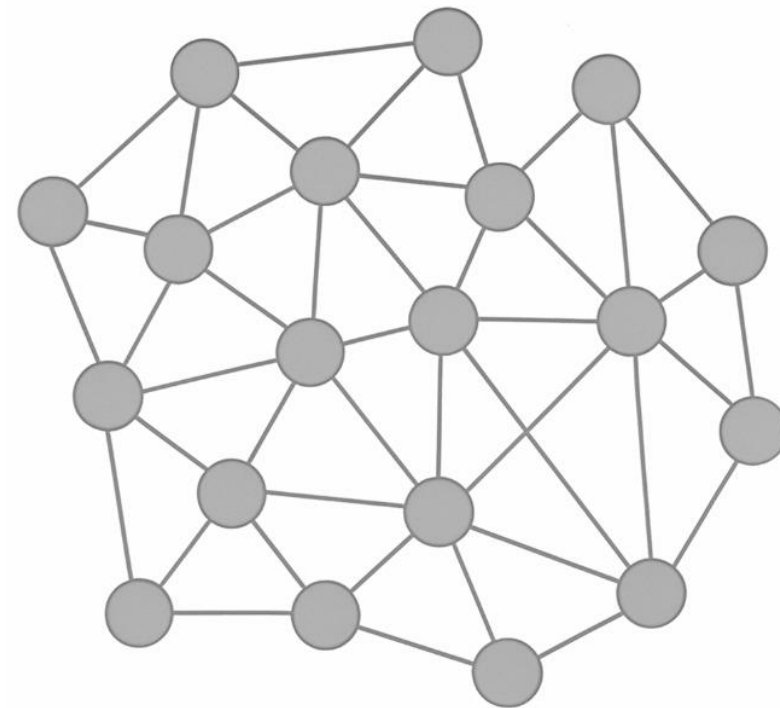
Semantic edge : Meaning-based Connection



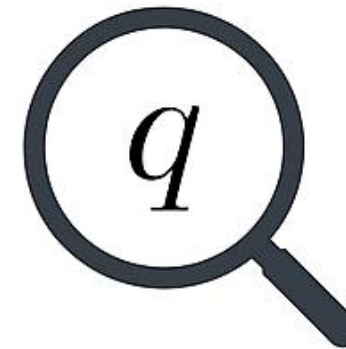
Query-Guided Subgraph Retrieval



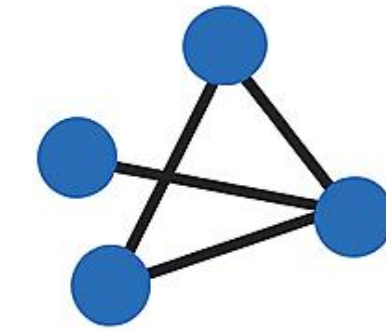
$$G_q = (V_q, E_q)$$



Full communication
graph G

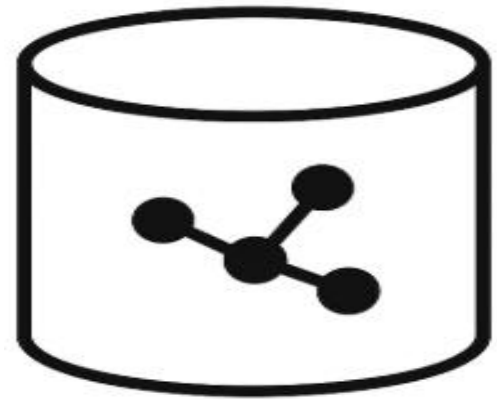


q :
specific forensic query

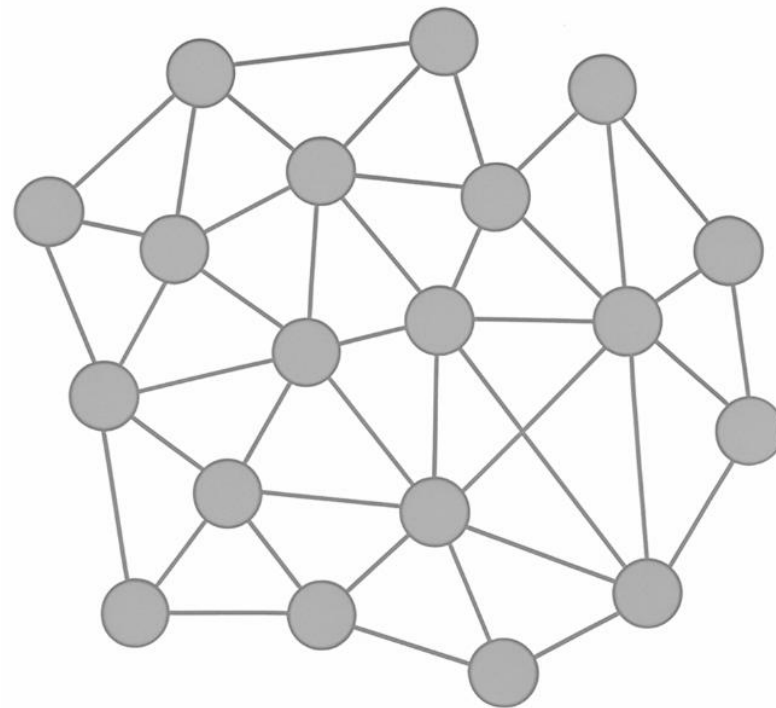


Retrieved subgraph
 $G_q = (V_q, E_q)$

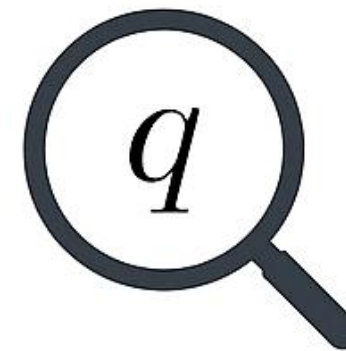
Query-Guided Subgraph Retrieval



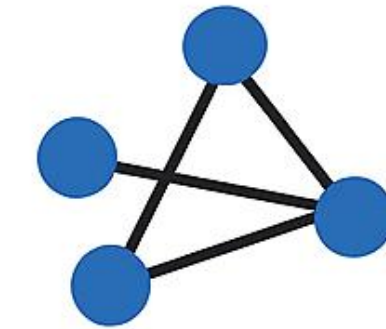
$$G_q = (V_q, E_q)$$



Full communication
graph G



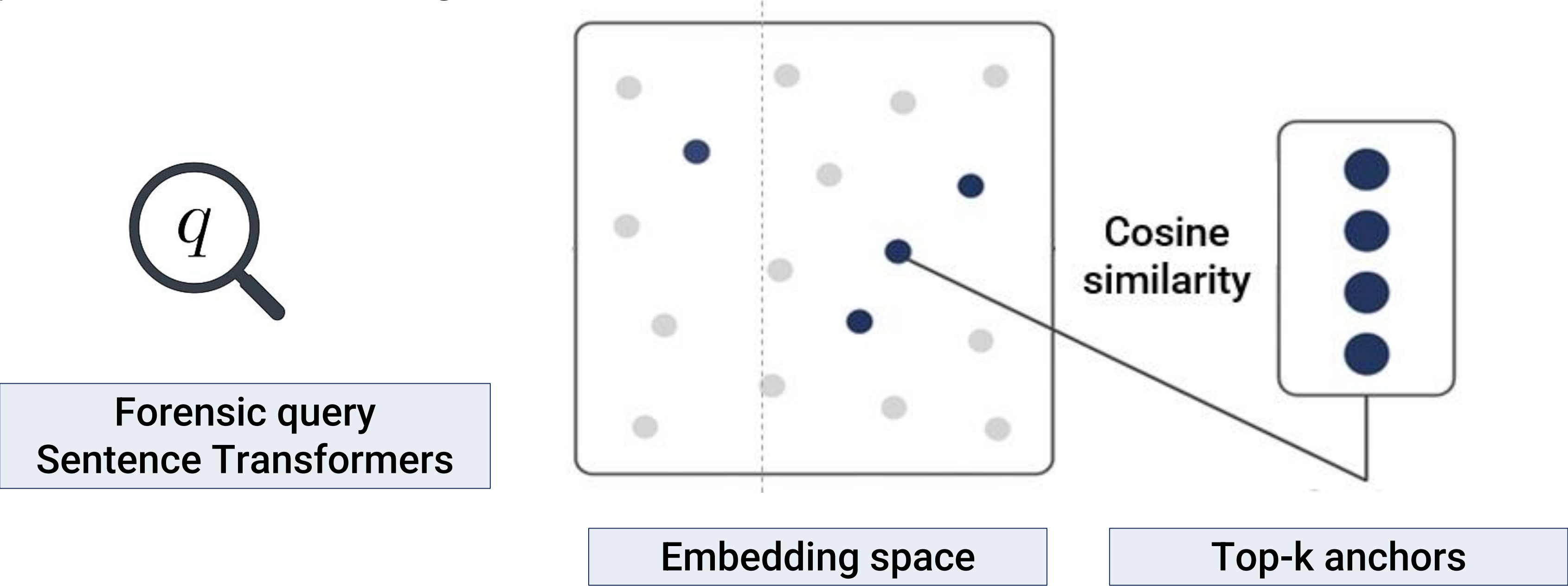
q :
specific forensic query



Retrieved subgraph
 $G_q = (V_q, E_q)$

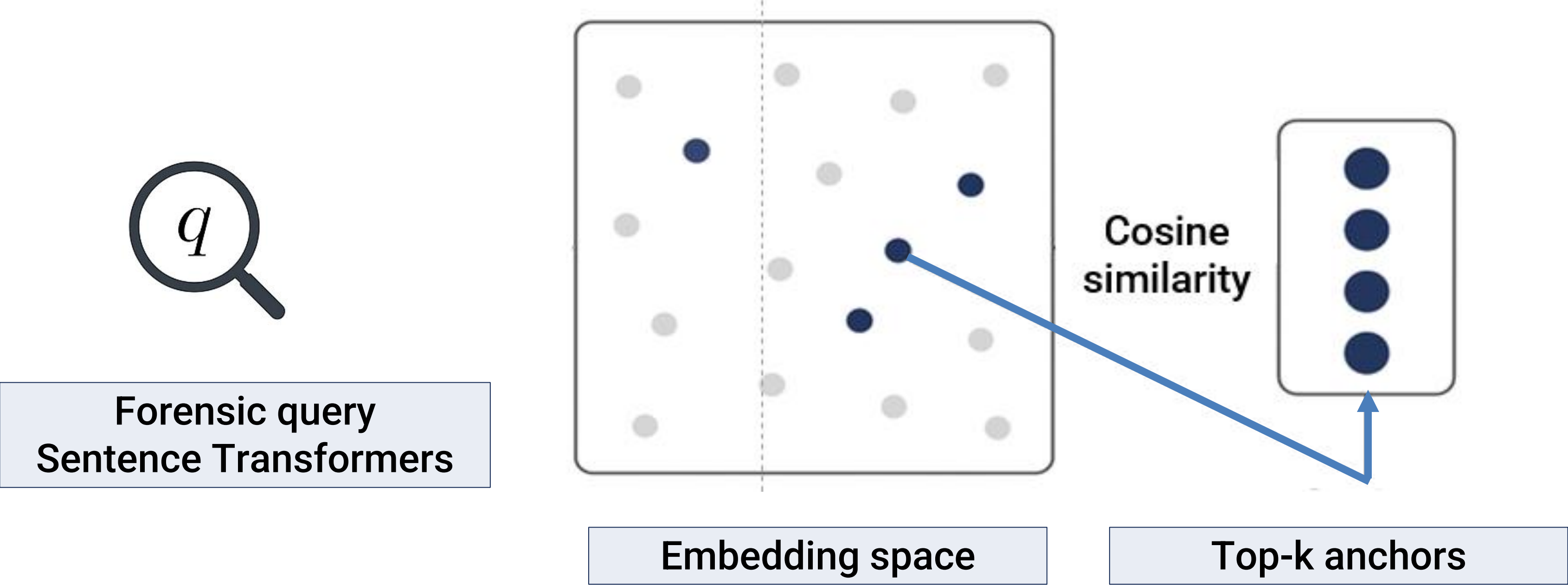
Query-Guided Subgraph Retrieval

Step1. Semantic filtering



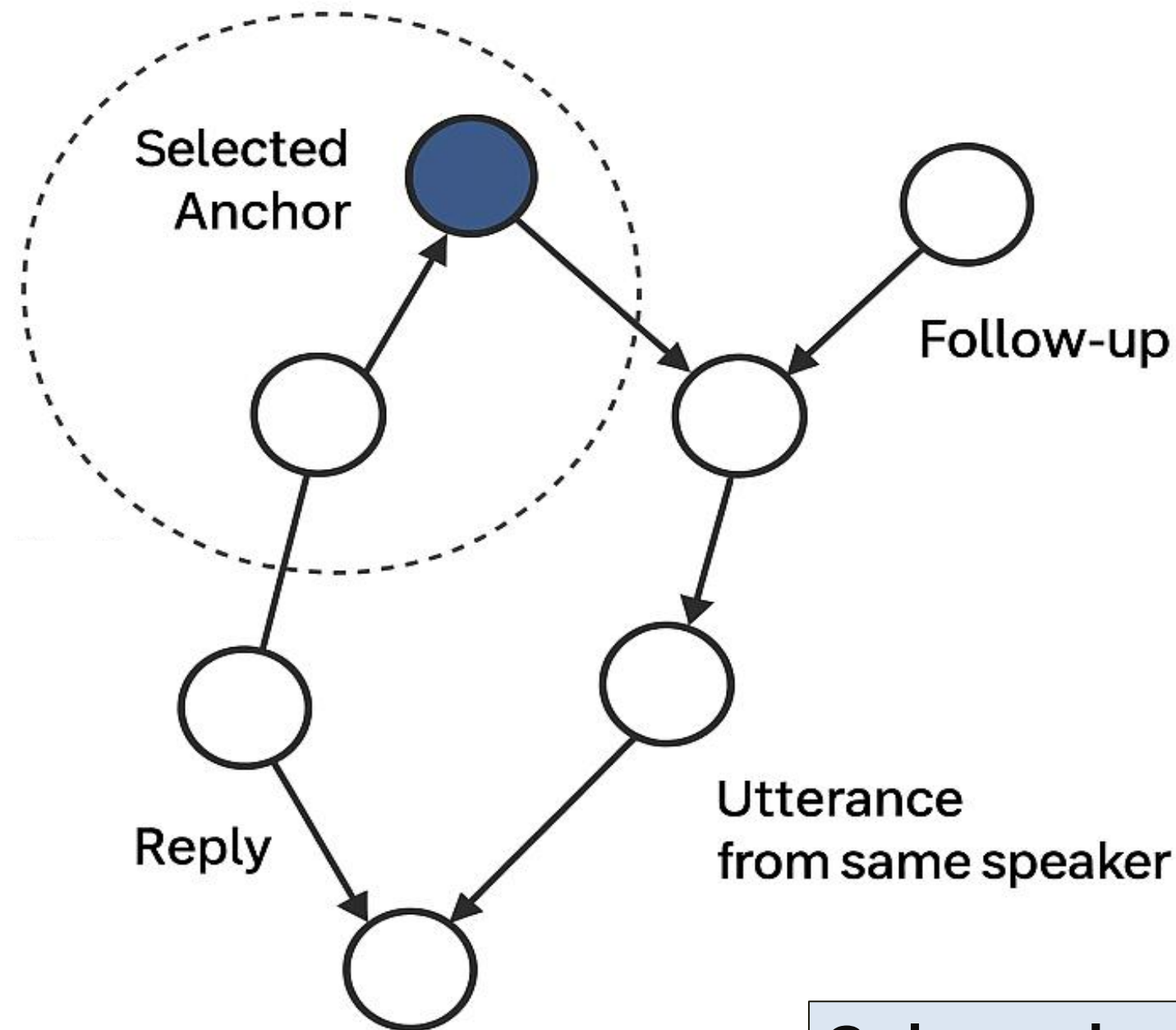
Query-Guided Subgraph Retrieval

Step1. Semantic filtering



Query-Guided Subgraph Retrieval

Step2. Graph expansion & Citation preservation



Subgraph generated via citation-guided expansion

Evidence-Guided Answer Generation



- $Gq \rightarrow$ Relevant messages
- $Cq \rightarrow$ Chronologically ordered evidence context
- Combine Cq with forensic question $q \rightarrow$ Input prompt

Forensic Answer Prompt Rules

Instruction

1. The model must answer only based on the given evidence, without speculation.
 2. It must cite each piece of evidence explicitly — using message IDs or document references.
 3. The response must be concise, interpretable, and legally admissible.
- ⋮

Evidence-Guided Answer Generation



 RUNNING... Stop Deploy

DFgraph Query

GraphRAG Index Path:

D:I20250507_DFgraph

☒ local

☒ global

☒ drift

Did Raskolnikov plan the murder in advance?

Query Execution

Explainable Reasoning Traces



DFgraph Query

Answer :

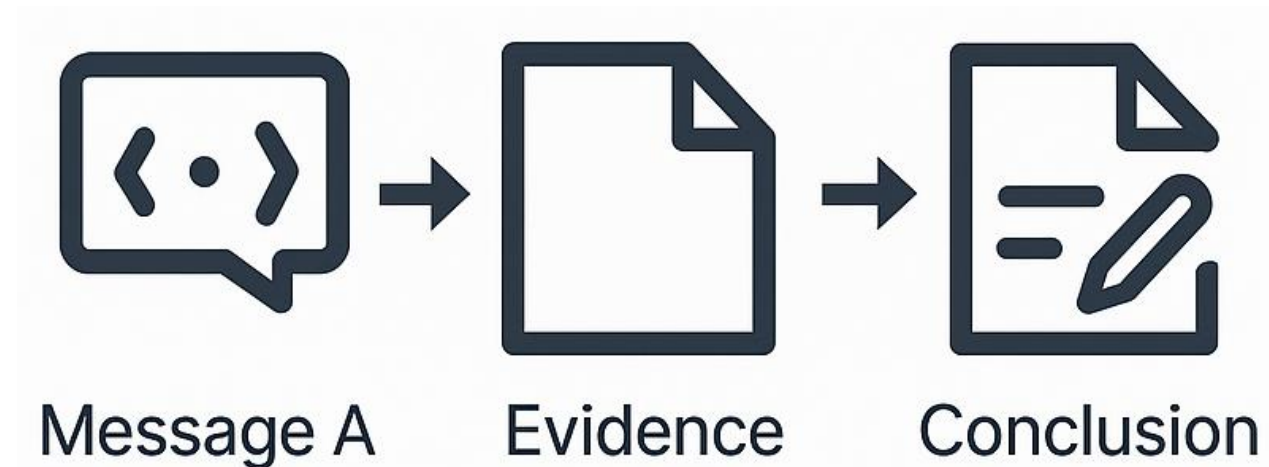
Yes.

Msg#A shows that Raskolnikov intentionally chose a time when Alyona would be alone, while **Msg#B** confirms that he had concealed a weapon in advance. **Msg#C** further indicates that he was aware the act had already been carried out. Taken together, these messages provide verifiable evidence of premeditation and preparation, thereby supporting a legally defensible conclusion. [Source Information: Reports (7, 21); Entities (3157, 2726, 2962); Relationships (1106, 1218,999); Sources (Msg#A, Msg#B, +more)]

Explainable Reasoning Traces

Reasoning trace

- Tracing logical links between evidence and conclusion



How do we generate this trace?

- Retrieve relevant subgraph
- Analyze logical and temporal links
- Construct an evidence-aligned reasoning trace

This is why DF Graph adopts a graph-based structure

Evaluation

Evaluation : Dataset overview

Three complementary datasets used for model evaluation



Real-Case Dataset

- ≈ 2.95 MB
- 18,653 messages
- Forensic Investigation Reports



Public Dataset

- ≈ 0.91 MB
- 6,667 messages
- NIST Messenger Dataset (*The Cornell Movie Dialog Corpus, Stockholm Stealer*)



Synthetic Dataset

- 345 KB
- 2,367 messages
- Dostoevsky's *"Crime and Punishment"*

Evaluation : Comparison of models

Comparison with Baseline Models



GPT

No retrieval,
no structure



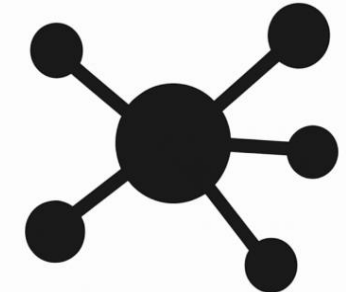
GPT+BERT

Intent-aware,
but structure-free



Naïve RAG

Retrieval-based,
but structurally flat

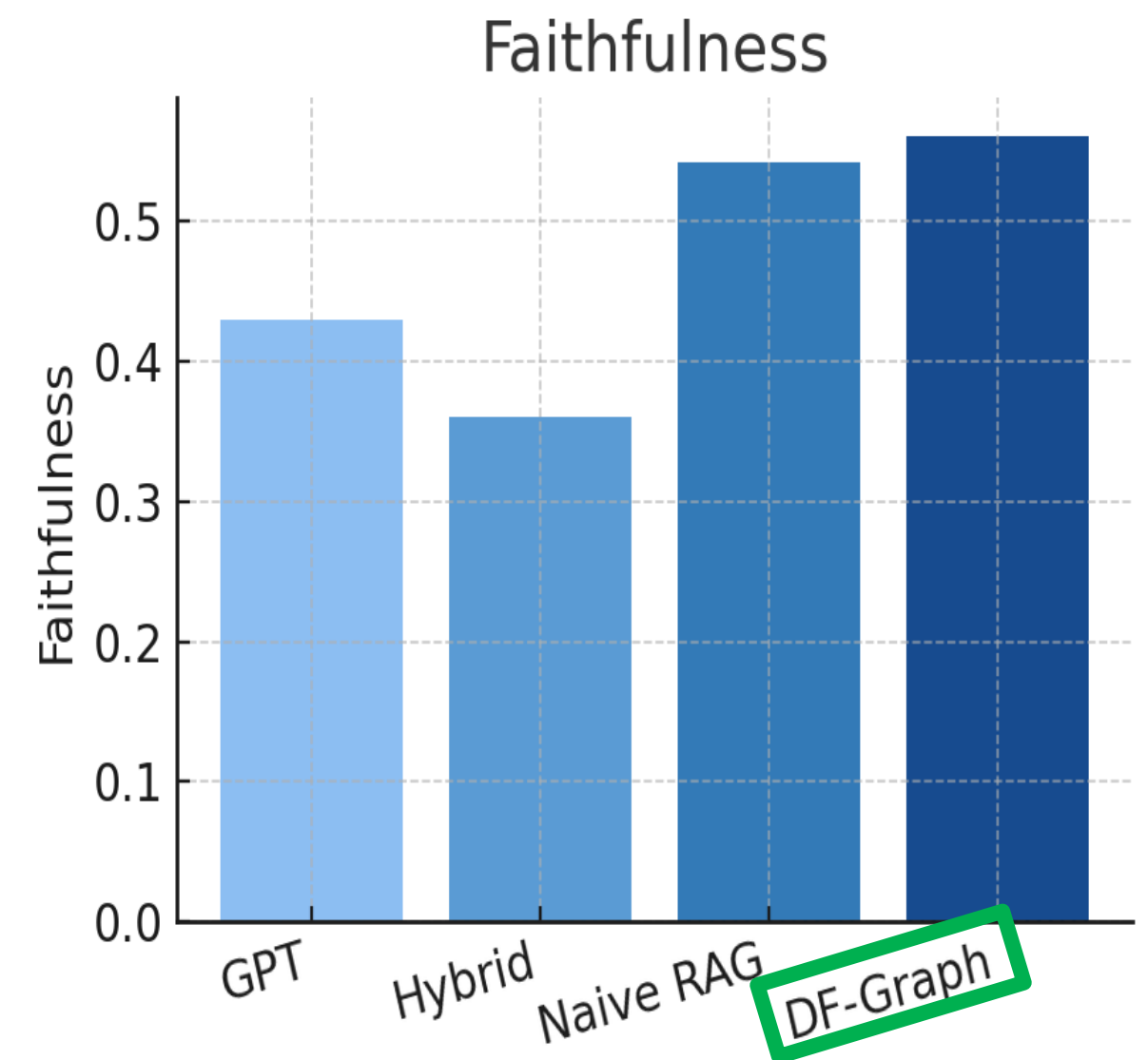
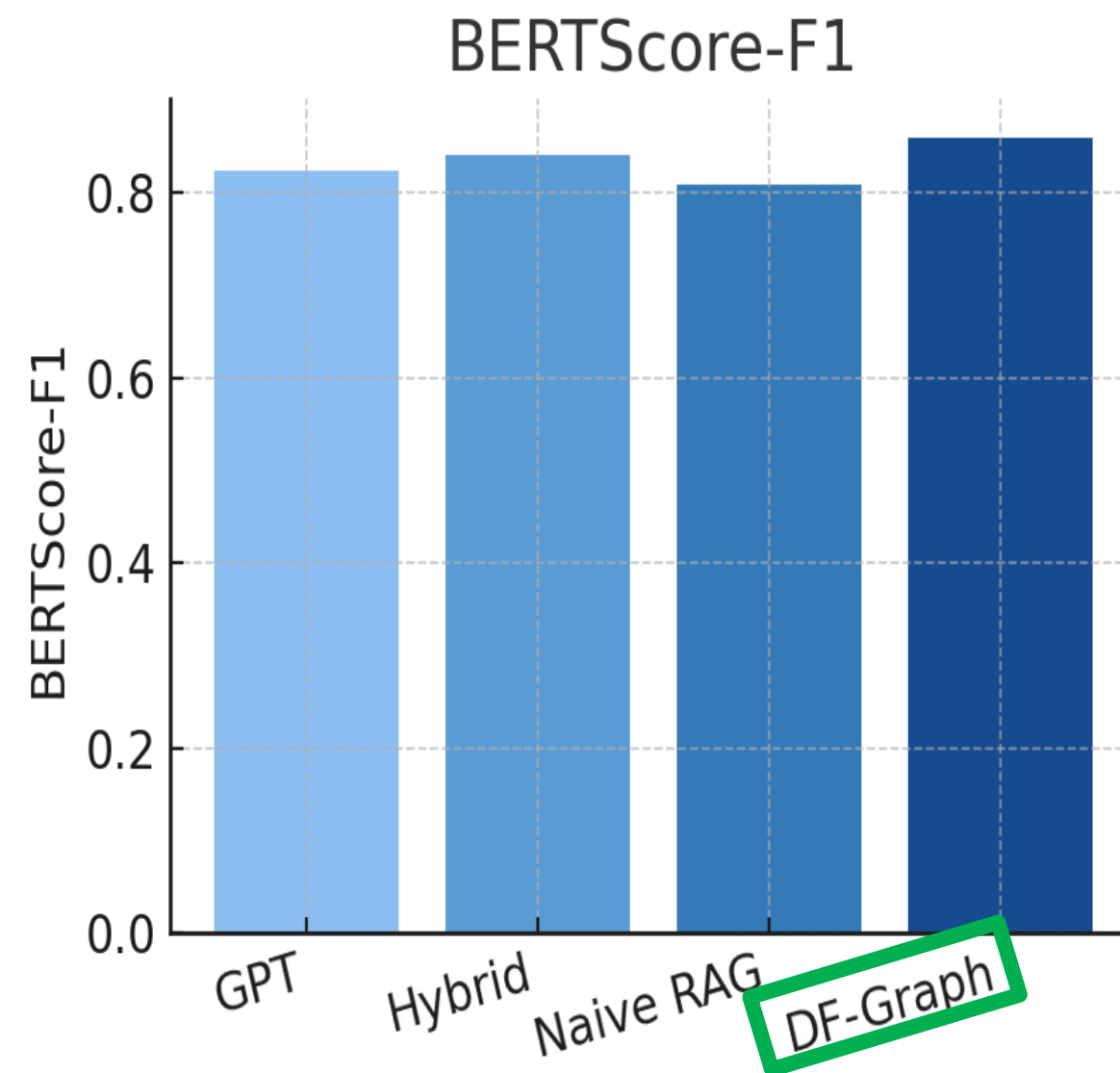
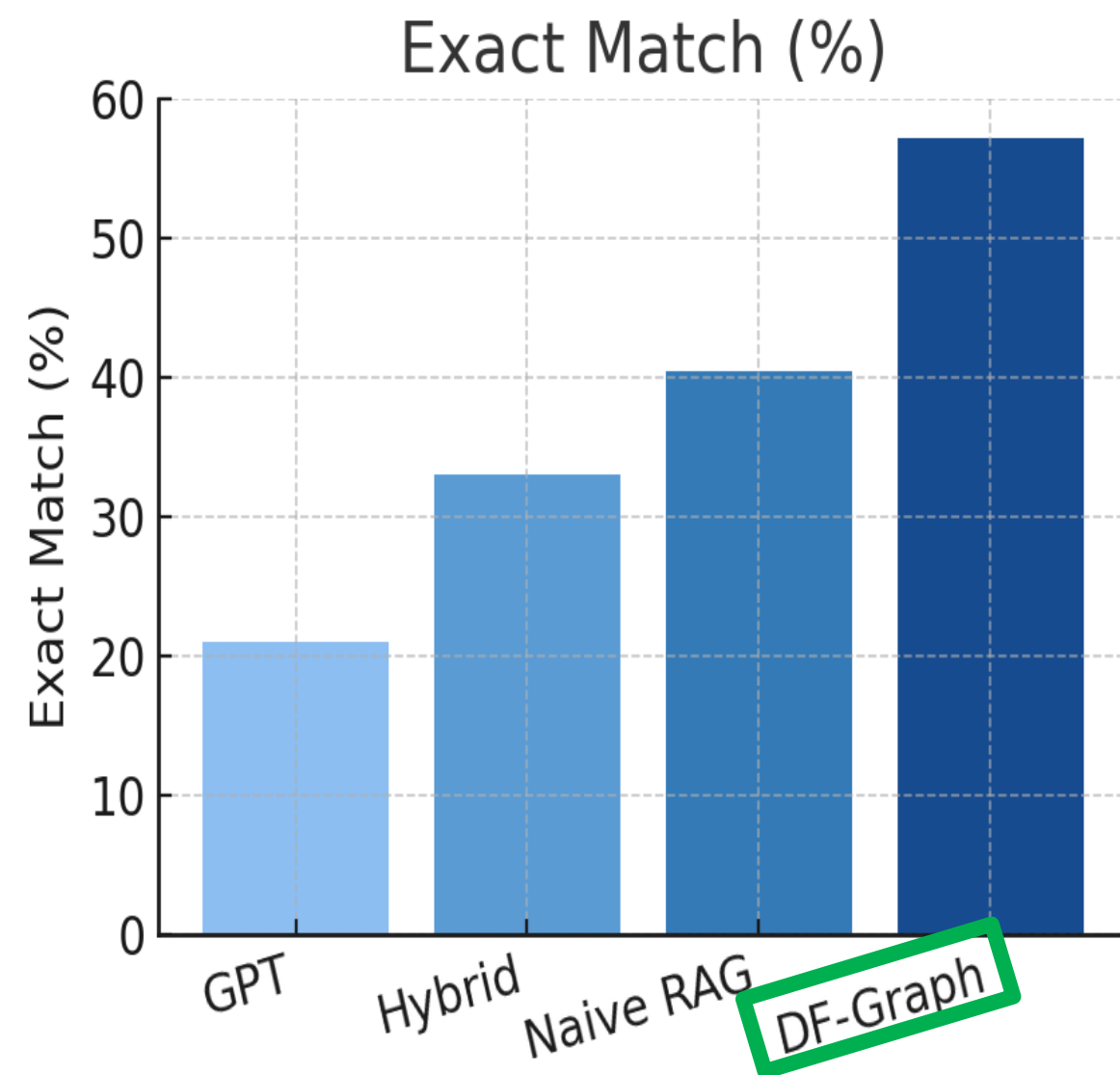


DF-Graph

Graph-structured,
contextually grounded

Evaluation1 : Quantitative results

Evaluation Metrics & Key Findings



Evaluation2: User study

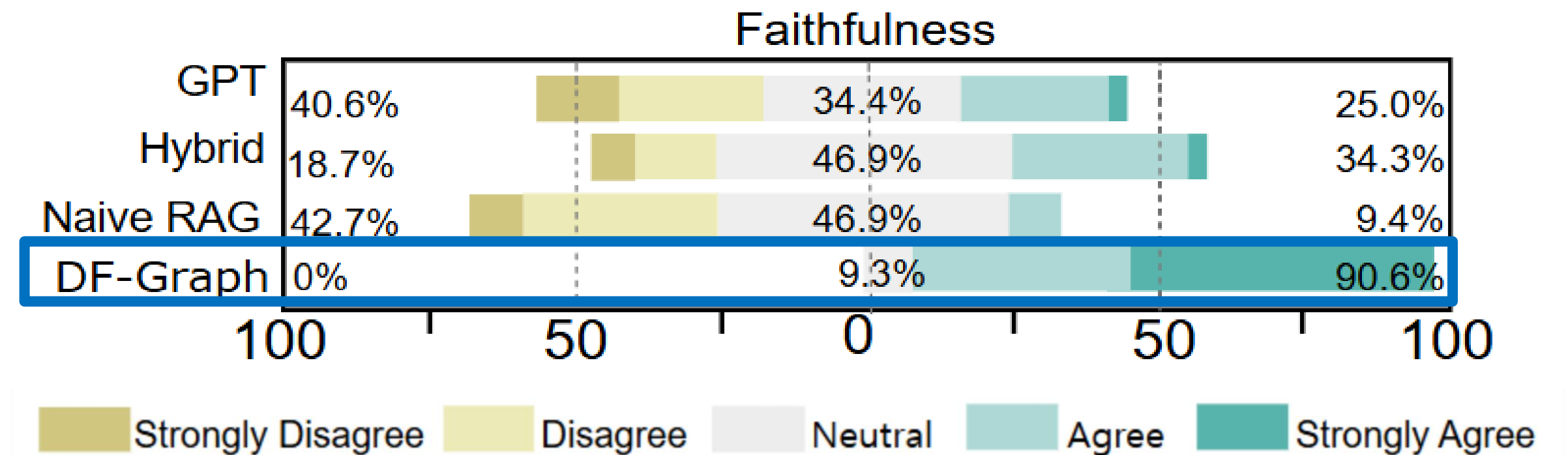
- **Participants** : 8 digital forensic professionals

ID	Experience(yrs)	Frequency	ID	Experience(yrs)	Frequency
P1	9	daily	P5	8	daily
P2	16	weakly	P6	13	weakly
P3	5	daily	P7	7	daily
P4	5	daily	P8	7	daily

- **Study Design and Evaluation Protocol** : Latin square method

Evaluation2: User study

- Accuracy(Q1) : **DF-Graph (78.1%)** , Naive RAG (56.2%), Hybrid (43.8%), GPT (40.6%)
- **5-point Likert scales** for each task
 - Faithfulness (Q2): Grounded in message content?
: **DF-Graph (90.6%)**



Participants' feedback

Practical implementation potential



“DF–Graph helps resolve major concerns in AI–based digital forensics, particularly source traceability. I look forward to seeing it used in practice soon.”

Potential for legal admissibility

“DF–Graph works just like real forensic workflows, and its structure helps me understand the logic instantly.”



Conclusion

“DF-Graph uses graph structures to help LLMs capture context and generate traceable, reliable forensic results.”

- Quantitative results**

Metric	DF-Graph Score
Exact Match (%)	57.23 $\pm$ 1.95
BERTScore-F1	0.859 $\pm$ 0.005
Faithfulness	0.561 $\pm$ 0.005

- Qualitative evaluation**

Evaluation Metrics	DF-Graph
Faithfulness (Q2)	9.3%
Explainability (Q3)	12.6%
Clarity (Q4)	15.6%
Interpretability (Q5)	9.4%

Thank You

If you're interested in our work,
please check out our paper for more details



The paper can be accessed via the QR code below

`munich1984@skku.edu`