SQL Murder Mystery: Solving a Crime Using Data Analysis

A data-driven investigation using SQL to uncover the truth behind a corporate murder

- Pratik Mendon

The Crime Scene

What Happened?

The CEO of TechNova Inc. has been found dead in their office on October 15, 2025, at 9:00 PM.

Our Mission

You are the lead Data Analyst to analyze corporate databases to identify the killer

The Digital Evidence Trail

Keycard Logs

Every door access timestamped

Alibis

Where suspects claim they were

Phone Records

Calls made during critical window

Crime Scene Evidence

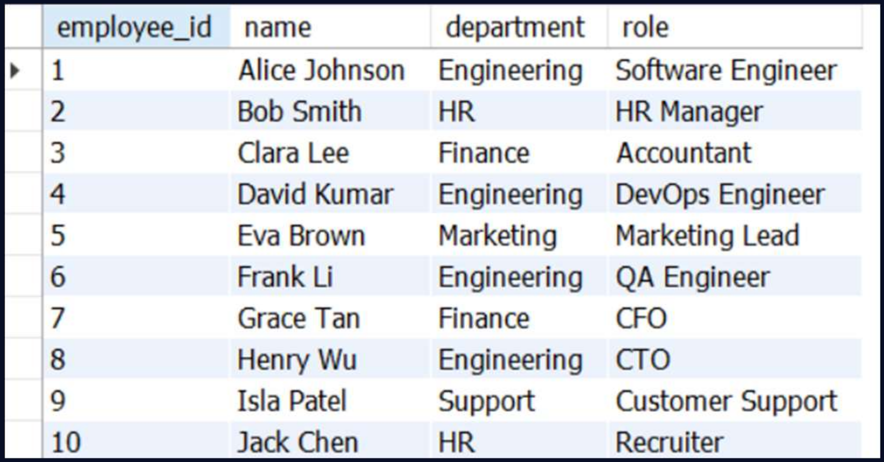
Physical traces left behind

Employee Database

Profiles - Roles and Department

Employee Database

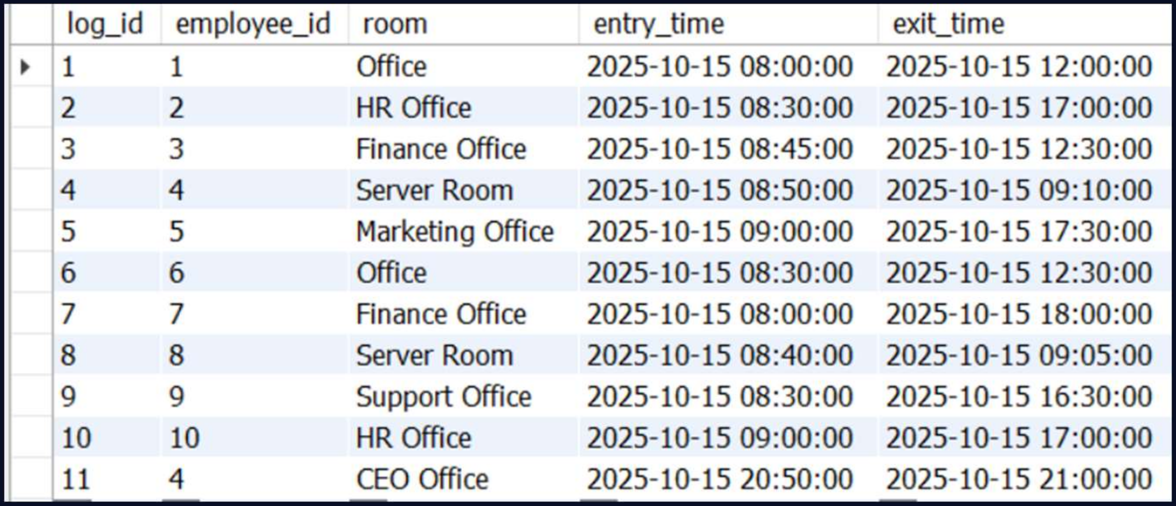
Profiles - Roles and Department



employee_id	name	department	role
1	Alice Johnson	Engineering	Software Engineer
2	Bob Smith	HR	HR Manager
3	Clara Lee	Finance	Accountant
4	David Kumar	Engineering	DevOps Engineer
5	Eva Brown	Marketing	Marketing Lead
6	Frank Li	Engineering	QA Engineer
7	Grace Tan	Finance	CFO
8	Henry Wu	Engineering	CTO
9	Isla Patel	Support	Customer Support
10	Jack Chen	HR	Recruiter

Keycard Logs

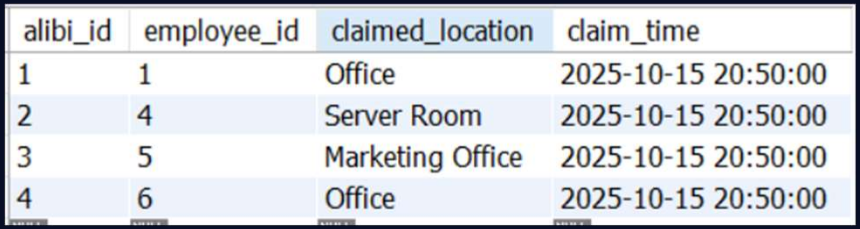
Every door access timestamped



log_id	employee_id	room	entry_time	exit_time
1	1	Office	2025-10-15 08:00:00	2025-10-15 12:00:00
2	2	HR Office	2025-10-15 08:30:00	2025-10-15 17:00:00
3	3	Finance Office	2025-10-15 08:45:00	2025-10-15 12:30:00
4	4	Server Room	2025-10-15 08:50:00	2025-10-15 09:10:00
5	5	Marketing Office	2025-10-15 09:00:00	2025-10-15 17:30:00
6	6	Office	2025-10-15 08:30:00	2025-10-15 12:30:00
7	7	Finance Office	2025-10-15 08:00:00	2025-10-15 18:00:00
8	8	Server Room	2025-10-15 08:40:00	2025-10-15 09:05:00
9	9	Support Office	2025-10-15 08:30:00	2025-10-15 16:30:00
10	10	HR Office	2025-10-15 09:00:00	2025-10-15 17:00:00
11	4	CEO Office	2025-10-15 20:50:00	2025-10-15 21:00:00

Alibis

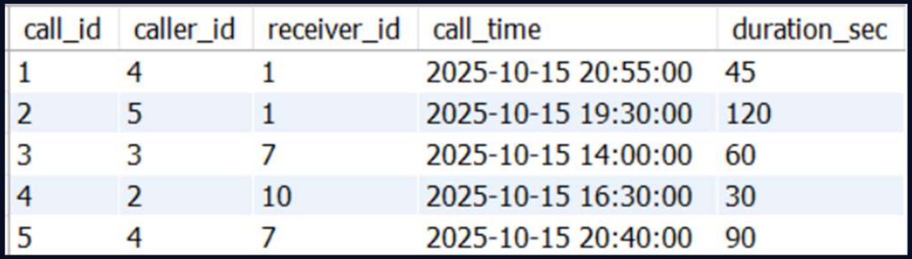
Where suspects claim they were



alibi_id	employee_id	claimed_location	claim_time
1	1	Office	2025-10-15 20:50:00
2	4	Server Room	2025-10-15 20:50:00
3	5	Marketing Office	2025-10-15 20:50:00
4	6	Office	2025-10-15 20:50:00

Phone Records

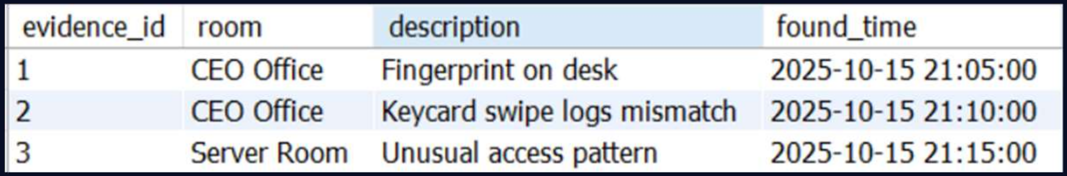
Calls made during critical window



call_id	caller_id	receiver_id	call_time	duration_sec
1	4	1	2025-10-15 20:55:00	45
2	5	1	2025-10-15 19:30:00	120
3	3	7	2025-10-15 14:00:00	60
4	2	10	2025-10-15 16:30:00	30
5	4	7	2025-10-15 20:40:00	90

Crime Scene Evidence

Physical traces left behind



evidence_id	room	description	found_time
1	CEO Office	Fingerprint on desk	2025-10-15 21:05:00
2	CEO Office	Keycard swipe logs mismatch	2025-10-15 21:10:00
3	Server Room	Unusual access pattern	2025-10-15 21:15:00

Made with GAMMA

The Investigation Framework

01

Identify Access

Who entered the CEO's office near 21:00?

02

Verify Alibis

Cross-check claimed locations with logs

03

Analyze Communications

Examine calls between 20:50–21:00

04

Match Evidence

Connect physical traces to suspects

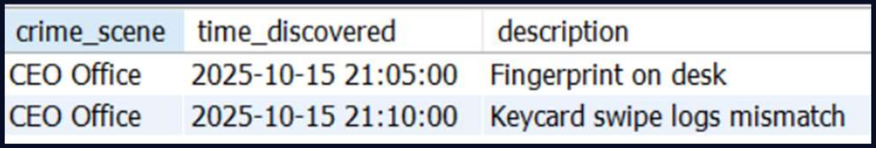
05

Converge Data

Identify the suspect who can't be cleared

Query #1: Where and When the Crime happened?

```
SELECT  room AS crime_scene,
found_time AS time_discovered,
`description`
FROM evidence WHERE room = 'CEO Office’
ORDER BY found_time;
```

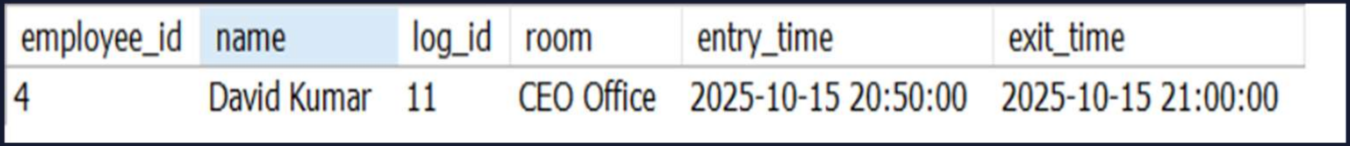


crime_scene	time_discovered	description
CEO Office	2025-10-15 21:05:00	Fingerprint on desk
CEO Office	2025-10-15 21:10:00	Keycard swipe logs mismatch

Made with GAMMA

Query #2: Analyze who accessed critical areas at the time

```
SELECT e.employee_id, e.`name`,  k.log_id, k.room, k.entry_time,  k.exit_time
FROM employees e JOIN keycard_logs k ON e.employee_id = k.employee_id
WHERE room = "CEO Office" AND entry_time BETWEEN "2025-10-15 20:30:00" AND "2025-10-15 21:10:00";
```



employee_id	name	log_id	room	entry_time	exit_time
4	David Kumar	11	CEO Office	2025-10-15 20:50:00	2025-10-15 21:00:00

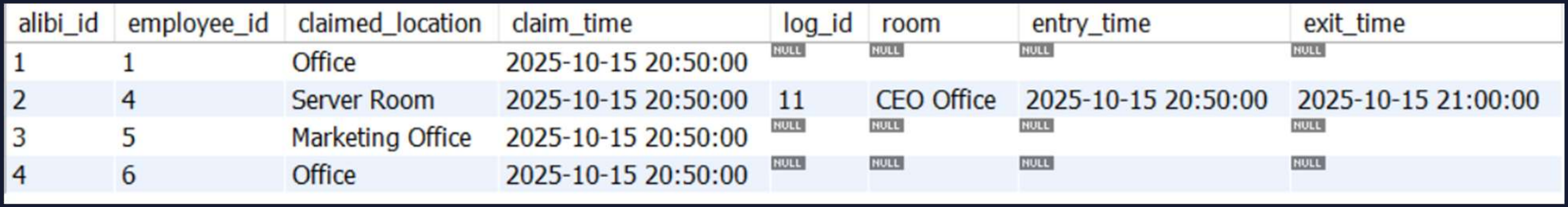
Why It Matters

Who entered the CEO's Office close to the time of the murder?

Made with GAMMA

Query #3: Cross check Alibis with Actual logs

```
SELECT a.*, k.log_id, k.room, k.entry_time, k.exit_time
FROM alibis a LEFT JOIN keycard_logs k ON a.employee_id = k.employee_id
AND a.claim_time BETWEEN k.entry_time and k.exit_time ORDER BY alibi_id;
```



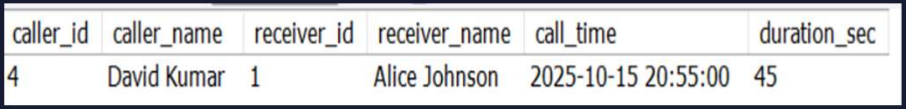
alibi_id	employee_id	claimed_location	claim_time	log_id	room	entry_time	exit_time
1	1	Office	2025-10-15 20:50:00	NULL	NULL	NULL	NULL
2	4	Server Room	2025-10-15 20:50:00	11	CEO Office	2025-10-15 20:50:00	2025-10-15 21:00:00
3	5	Marketing Office	2025-10-15 20:50:00	NULL	NULL	NULL	NULL
4	6	Office	2025-10-15 20:50:00	NULL	NULL	NULL	NULL

Why It Matters

Who claimed to be somewhere else but was not?

Query #4: Investigate Suspicious Phone Activity between 20:50 and 21:00

```
SELECT c.caller_id, e1.`name` AS caller_name, c.receiver_id,
e2.`name` AS receiver_name,    c.call_time,   c.duration_sec
FROM employees e1 LEFT JOIN calls c ON e1.employee_id = c.caller_id
LEFT JOIN employees e2 on e2.employee_id = c.receiver_id
WHERE c.call_time BETWEEN "2025-10-15 20:50:00" AND "2025-10-15 21:00:00";
```



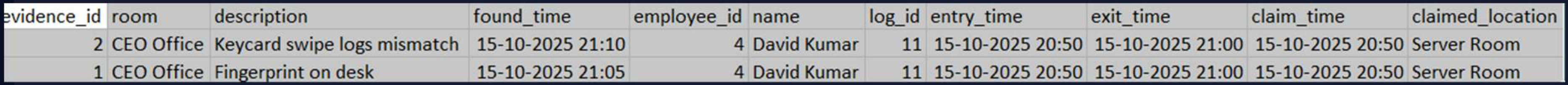
caller_id	caller_name	receiver_id	receiver_name	call_time	duration_sec
4	David Kumar	1	Alice Johnson	2025-10-15 20:55:00	45

Pattern Analysis

Query #5: Crime Scene Evidence Match with Movements and claims

1. 20:50 – Entry time
   Suspect enters CEO Office
2. 21:00 – Time of Death
   CEO found deceased
3. 21:05 – Physical Evidence
   Fingerprint on Desk
4. 21:10 – Logs evidence
   Keycard swipe logs mismatch

```
SELECT e.*, k.employee_id, es.`name`,  k.log_id,  k.entry_time,  k.exit_time,  a.claim_time, a.claimed_location FROM evidence e
LEFT JOIN keycard_logs k ON e.room = k.room LEFT JOIN employees es ON k.employee_id = es.employee_id LEFT JOIN alibis a
ON k.employee_id = a.employee_id WHERE e.found_time BETWEEN k.entry_time and date_add(k.exit_time, interval 15 minute);
```



evidence_id	room	description	found_time	employee_id	name	log_id	entry_time	exit_time	claim_time	claimed_location
2	CEO Office	Keycard swipe logs mismatch	15-10-2025 21:10	4	David Kumar	11	15-10-2025 20:50	15-10-2025 21:00	15-10-2025 20:50	Server Room
1	CEO Office	Fingerprint on desk	15-10-2025 21:05	4	David Kumar	11	15-10-2025 20:50	15-10-2025 21:00	15-10-2025 20:50	Server Room

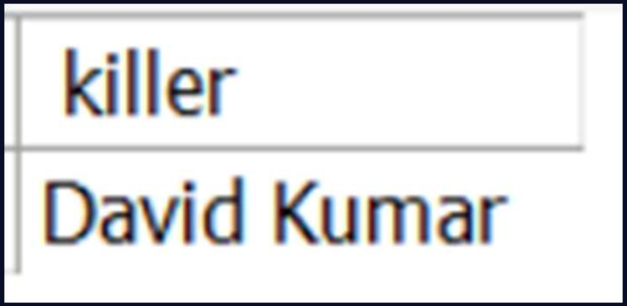
Made with GAMMA

The Final Query: Convergence of Evidence

```
-- Findings from keylogs
WITH cte_key AS (SELECT e.employee_id,  e.`name`, "Keylogs" AS Match_Found_in FROM employees e LEFT JOIN keycard_logs k ON e.employee_id = k.employee_id WHERE k.room = "CEO Office"),
-- Findings from calls
cte_calls AS (SELECT e.employee_id,  e.`name`, "Call logs" AS Match_Found_in FROM employees e LEFT JOIN calls c ON e.employee_id = c.caller_id WHERE c.call_time BETWEEN "2025-10-15 20:30:00" AND "2025-10-15 21:10:00"),
-- Findings from alibis
cte_alibis AS (SELECT e.employee_id, e.`name`, "Alibis" AS Match_Found_in FROM employees e LEFT JOIN alibis a ON e.employee_id = a.employee_id
LEFT JOIN keycard_logs k ON a.employee_id = k.employee_id WHERE a.claim_time BETWEEN "2025-10-15 20:30:00" AND "2025-10-15 21:10:00"AND k.room <> a.claimed_location),
-- Findings from evidence
cte_evidence AS (SELECT  e.employee_id,   e.`name`,  "Evidence" AS Match_Found_in FROM employees e LEFT JOIN keycard_logs k ON e.employee_id = k.employee_id LEFT JOIN evidence ec ON k.room = ec.room WHERE ec.found_time BETWEEN k.entry_time and date_add(k.exit_time, interval 15 minute))
SELECT `name` AS killer FROM cte_key UNION SELECT `name` AS killer FROM cte_calls UNION SELECT `name` AS killer FROM  cte_alibis UNION SELECT `name` AS killer FROM cte_evidence;
```

Made with GAMMA

The Culprit



killer
David Kumar

Case Closed

All evidence points to one individual: access logs place them at the scene, alibi contradicts keycard data, phone records show suspicious activity, and physical evidence confirms presence

Why This Project Matters

Complex Joins

Connecting 5 tables to build complete picture from fragmented data sources

Precise Filtering

Time-based queries, location matching, threshold conditions to isolate relevant records

Data Validation

Cross-referencing claims against reality, identifying inconsistencies and contradictions

Critical Thinking

Asking right questions, building logical investigation flow, connecting disparate clues

Timeline Reconstruction

Ordering events chronologically to establish sequence and causation

Insight Generation

Transforming raw database records into actionable intelligence and clear conclusions

Special Thanks

DPD zero

INDIAN DATA CLUB

Let's Connect

Pratik Mendon

Github - 21 Days SQL