

Team



Mohammad Al Zoubi
Robotics, Cognition,
Intelligence



Ali Gharaee
Computer Science



Sebastian Städler
Computer Science



Leonardo Zambrano
Computer Science

Agenda

- Technical Problems Solved
- User Interface
- Intelligent Self-Learning System

QA Mode

- Interactive chat with logfile
- Traceability of answers

Sources: Log line IDs from which the answer was generated

The screenshot shows a chat window titled "Chat with test_log1.out" in the top left corner and the "Querious" logo in the top right. The chat history includes a question: "? what is suspicious about the log?". The answer, preceded by a lightbulb icon, lists four suspicious aspects from a log file. A blue arrow points from the text "Reader friendly formulated answer" to the answer text. Another blue arrow points from the text "Sources: Log line IDs from which the answer was generated" to a box containing specific line IDs. At the bottom of the chat window is an input field labeled "? Ask Querious..." with a right-pointing arrow.

Reader friendly formulated answer

? what is suspicious about the log?

💡 There are a few suspicious aspects in the log: 1. Nov 09 14:31:45 CMX50070-101776 rsdias-daemon[887]: ed data). Nov 09 16:37:07 CMX50070-101776 rsdias-daemon[887]: ted data). These entries have incomplete messages, with "ed data)" and "ted data)" without any context. It could indicate possible data manipulation or corruption. 2. Nov 09 13:11:45 CMX50070-101776 xu_launcher[2941]: ./warning_mark.bmp Nov 09 13:12:34 CMX50070-101776 xu_launcher[9930]: ./warning_mark.bmp The repeated occurrence of the same file, "./warning_mark.bmp," in a short time span could suggest a potential issue or abnormal behavior related to this file. 3. Nov 09 16:35:07 CMX50070-101776 rsdias-daemon[887]: el normally closed (or due to unexpected data). This entry mentions an abnormal closure, possibly due to unexpected data. It indicates that have occurred during the process. 4. Nov 10 05:49:07 CMX50070- MISCUOUS dev=vethf97bf7a prom=0 old_prom=256 auid=4294967295 This audit entry indicates an anomalous promiscuous mode hf97bf7a." Promiscuous mode allows network devices to capture all and be suspicious if not expected in the given context.

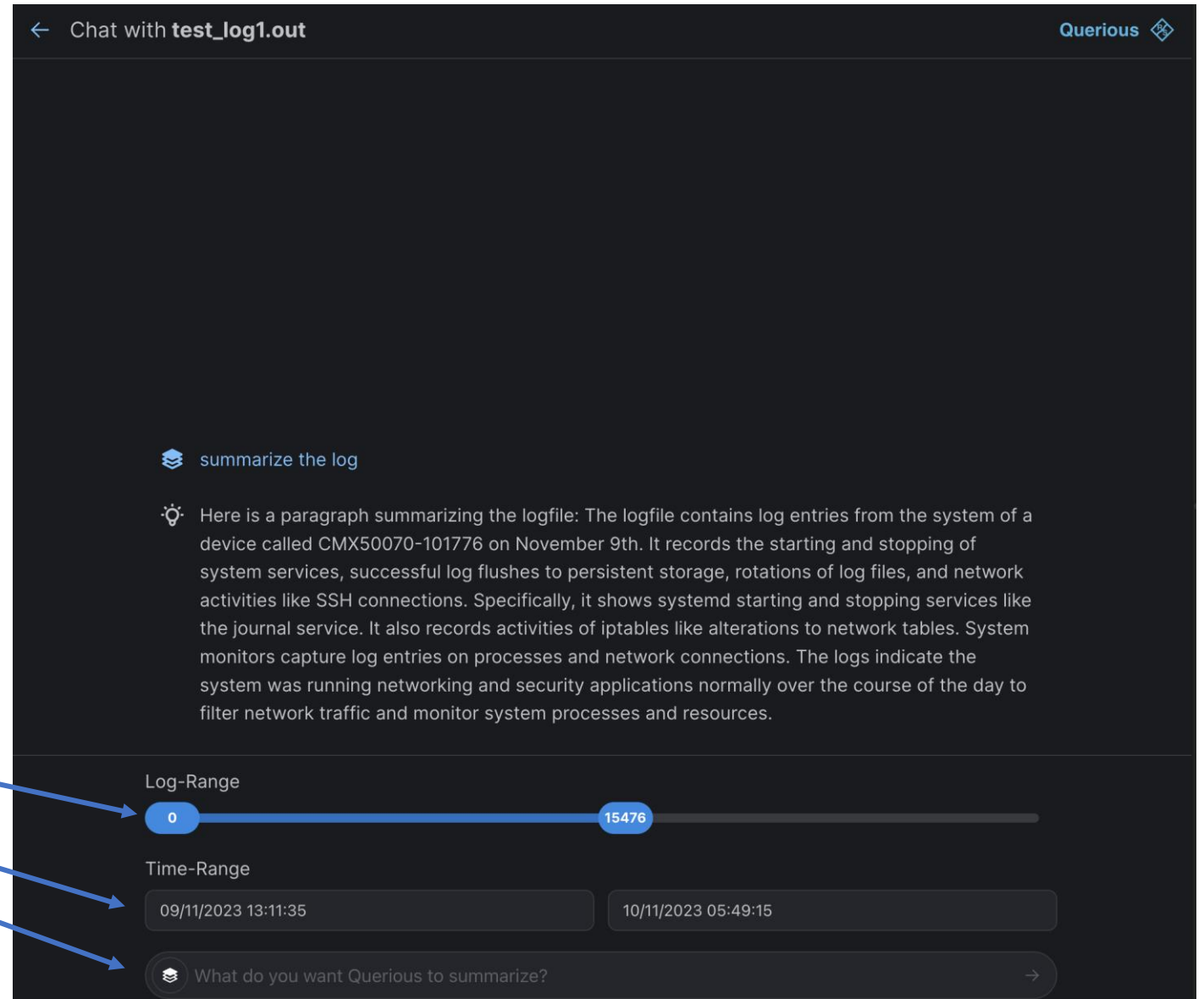
line: 828, line: 1886, line: 1974, line: 2603, line: 4901, line: 18243, line: 18438, line: 19473, line: 19746, line: 28843

[view source](#)

? Ask Querious...

Summary Mode

- Static summary (experimental) based on
 - Topic clustering
 - Uniform logs sampling
- Strong dynamic summary with four parameters:
 - Line range
 - Time range
 - Relevant Topics
 - Irrelevant Topics (experimental)



Log Search Mode


- Display most relevant loglines


← Chat with **test_log1.out**

Querious

something unusual might have occurred during the process. 4. Nov 10 05:49:07 CMX50070-101776 audit: ANOM_PROMISCUOUS dev=vethf97bf7a prom=0 old_prom=256 auid=4294967295 uid=0 gid=0 ses=4294967295 This audit entry indicates an anomalous promiscuous mode change for the device "vethf97bf7a." Promiscuous mode allows network devices to capture all network traffic, which could be suspicious if not expected in the given context.

[view source](#)

 What multicast group did the avahi-daemon join on the interface 'eth_external.IPv4'?



2087 | Nov 09 13:11:42 CMX50070-101776 avahi-daemon[379]: Joining mDNS multicast group on interface eth_external.IPv4 with address 10.102.37.173.

1722 | Nov 09 13:11:39 CMX50070-101776 avahi-daemon[379]: Joining mDNS multicast group on interface eth_internal.IPv4 with address 172.22.254.245.

28250 | Nov 10 05:49:04 CMX50070-101776 avahi-daemon[379]: Leaving mDNS multicast group on interface eth_external.IPv4 with address 10.102.37.173.

2652 | Nov 09 13:11:45 CMX50070-101776 avahi-daemon[379]: Joining mDNS multicast group on interface docker0.IPv4 with address 100.82.64.1.

2377 | Nov 09 13:11:45 CMX50070-101776 avahi-daemon[379]: Joining mDNS multicast group on interface docker0.IPv4 with address 100.82.64.1.


2083 | Nov 09 13:11:42 CMX50070-101776 avahi-daemon[379]: Joining mDNS multicast group on interface eth_external.IPv6 with address fe80::8e8b:9f0:b893:1176.

1489 | Nov 09 13:11:37 CMX50070-101776 avahi-daemon[379]: Joining mDNS multicast group on interface lo.IPv4 with address 127.0.0.1.

28248 | Nov 10 05:49:04 CMX50070-101776 avahi-daemon[379]: Leaving mDNS multicast group on interface eth_internal.IPv4 with address 172.22.254.245.

3116 | Nov 09 13:11:51 CMX50070-101776 avahi-daemon[379]: Joining mDNS multicast group on interface br-e97410f82a59.IPv4 with address 100.82.64.129.

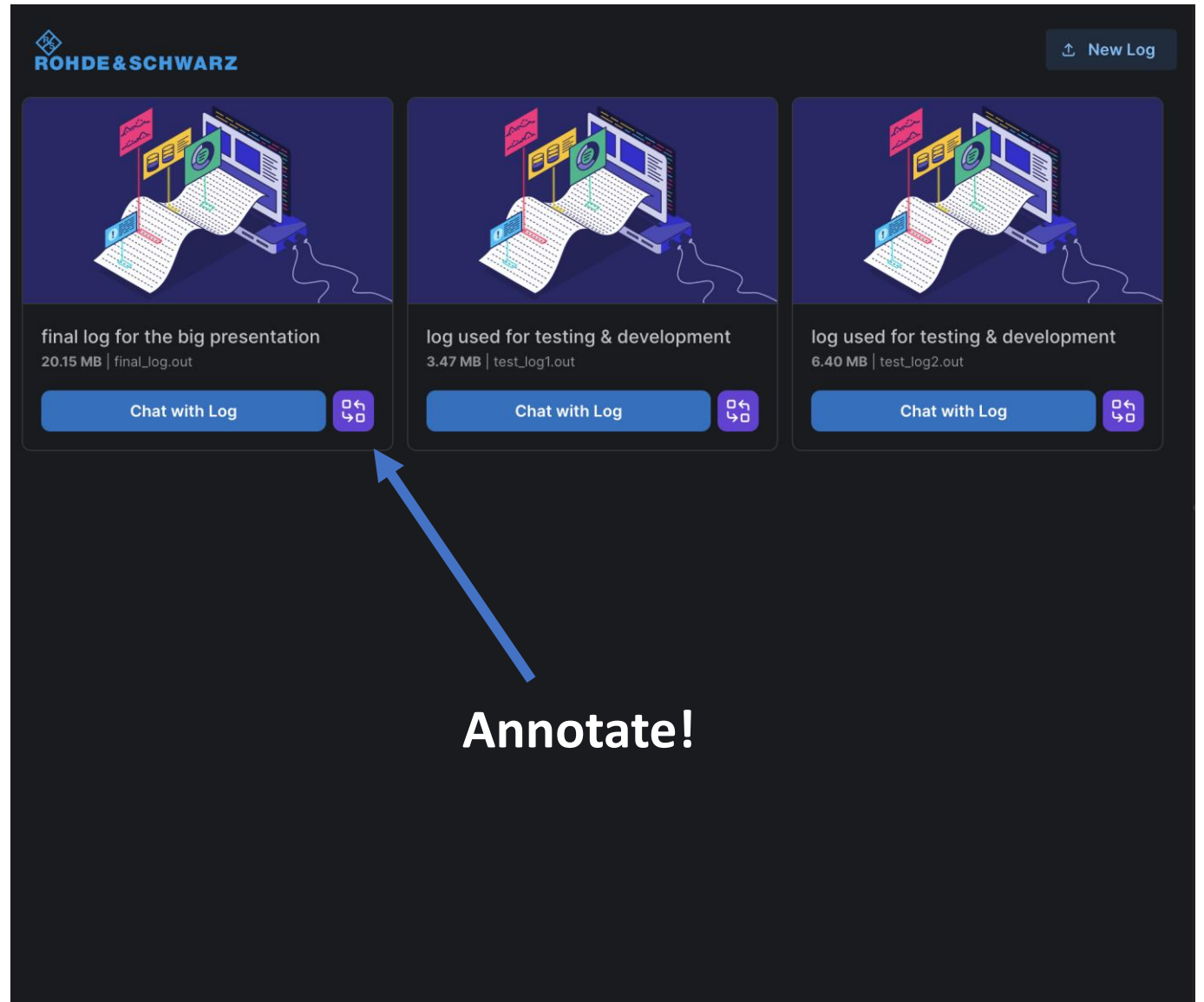
1732 | Nov 09 13:11:39 CMX50070-101776 avahi-daemon[379]: Joining mDNS multicast group on interface eth_internal.IPv6 with address fe80::290:b8ff:fe24:d36a.

 Search relevant logs with Querious...

→

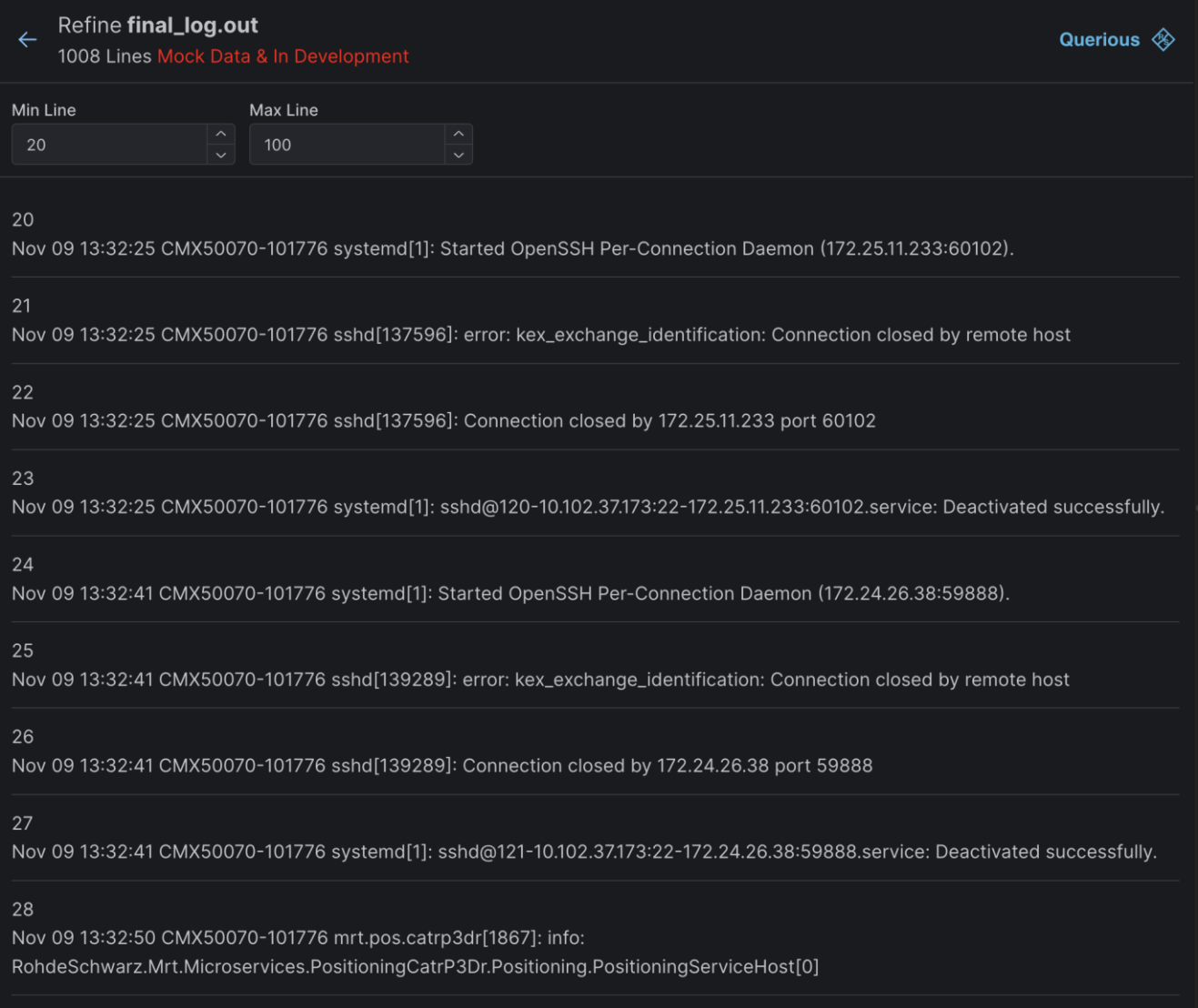
Learning From Human Feedback

- Possibility to improve the ranking algorithm through user annotations.



Learning From Human Feedback

- Click on a line/lines and submit a question to which the line/lines are the answer.
- Question-answer pairs can be used for training the ranking model.



The screenshot shows a log viewer interface with a dark theme. At the top, there's a header bar with a back arrow, the text "Refine final_log.out", and "1008 Lines Mock Data & In Development". On the right of the header is the "Querious" logo. Below the header, there are two input fields for "Min Line" (set to 20) and "Max Line" (set to 100). The main area displays a list of log entries, each preceded by a line number from 20 to 28. The log entries are as follows:

- 20: Nov 09 13:32:25 CMX50070-101776 systemd[1]: Started OpenSSH Per-Connection Daemon (172.25.11.233:60102).
- 21: Nov 09 13:32:25 CMX50070-101776 sshd[137596]: error: kex_exchange_identification: Connection closed by remote host
- 22: Nov 09 13:32:25 CMX50070-101776 sshd[137596]: Connection closed by 172.25.11.233 port 60102
- 23: Nov 09 13:32:25 CMX50070-101776 systemd[1]: sshd@120-10.102.37.173:22-172.25.11.233:60102.service: Deactivated successfully.
- 24: Nov 09 13:32:41 CMX50070-101776 systemd[1]: Started OpenSSH Per-Connection Daemon (172.24.26.38:59888).
- 25: Nov 09 13:32:41 CMX50070-101776 sshd[139289]: error: kex_exchange_identification: Connection closed by remote host
- 26: Nov 09 13:32:41 CMX50070-101776 sshd[139289]: Connection closed by 172.24.26.38 port 59888
- 27: Nov 09 13:32:41 CMX50070-101776 systemd[1]: sshd@121-10.102.37.173:22-172.24.26.38:59888.service: Deactivated successfully.
- 28: Nov 09 13:32:50 CMX50070-101776 mrt.pos.catrp3dr[1867]: info: RohdeSchwarz.Mrt.Microservices.PositioningCatrp3Dr.Positioning.PositioningServiceHost[0]

Questions?

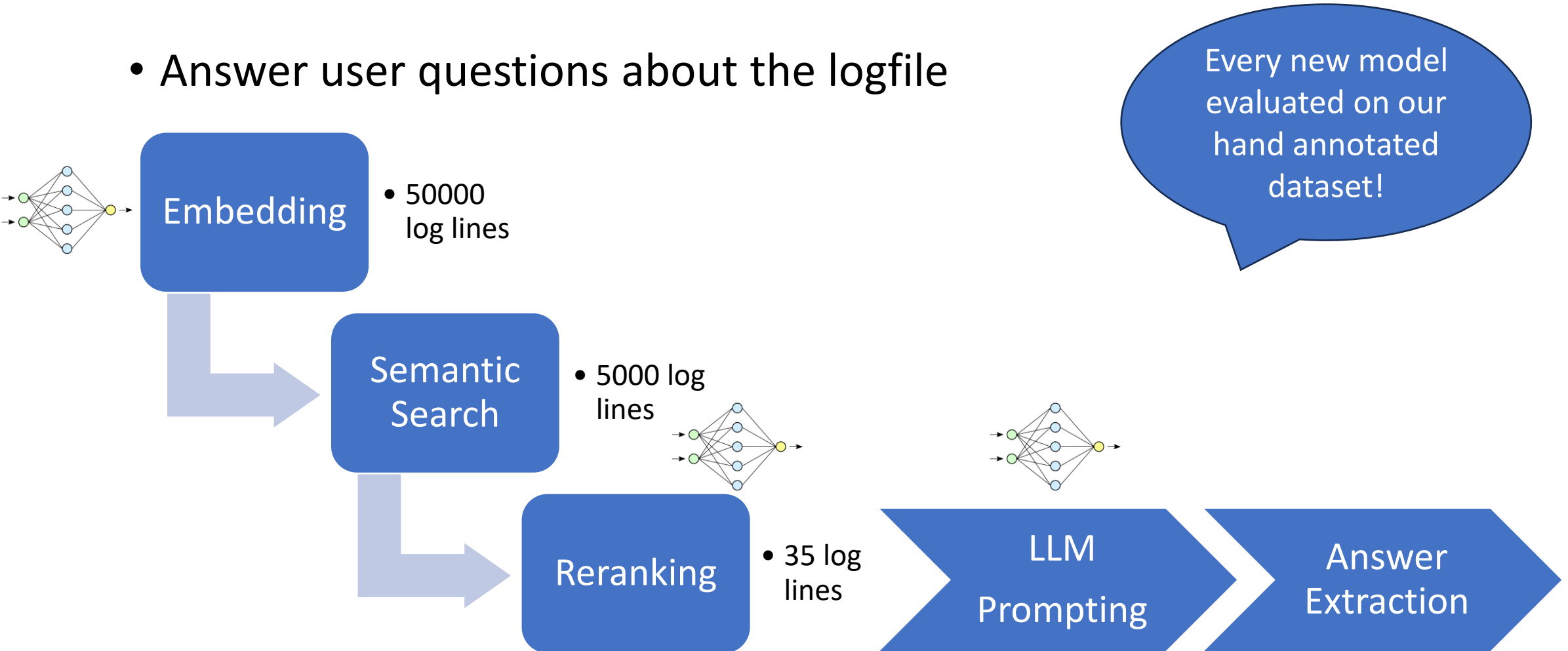
. . .

Appendix

- Pipelines for solving different problems
- Dataset and testing method

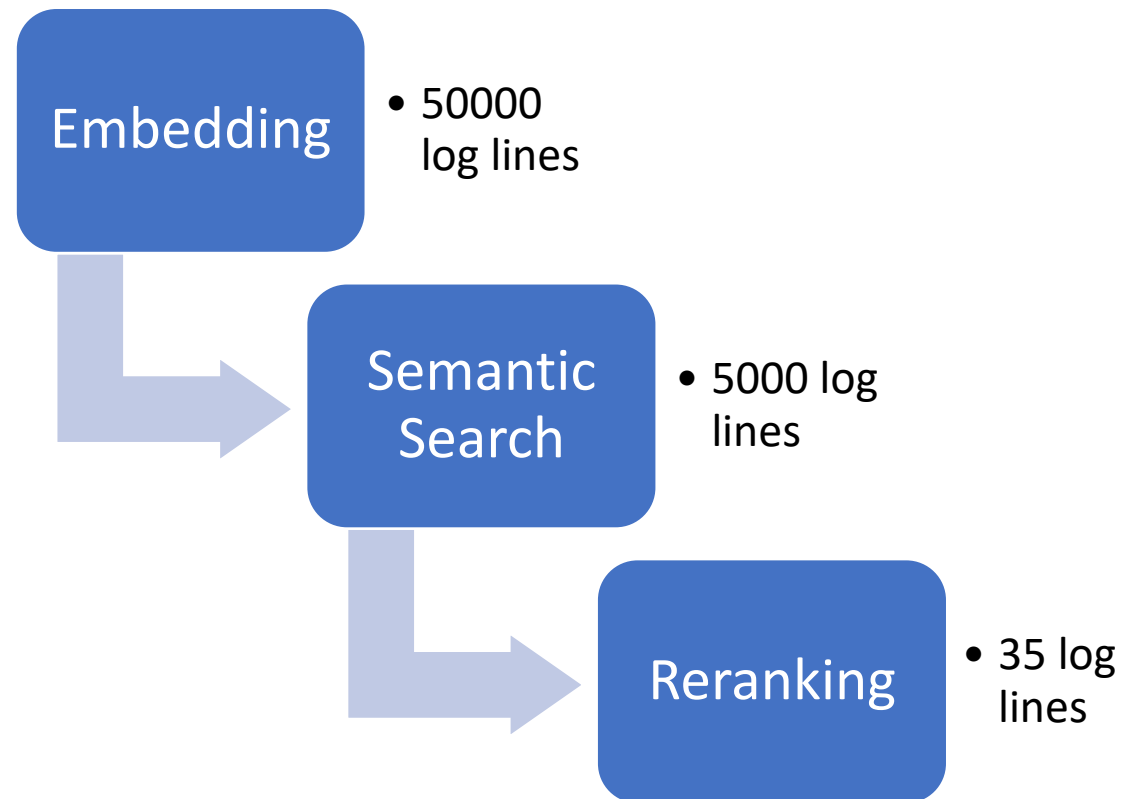
QA Mode

- Answer user questions about the logfile



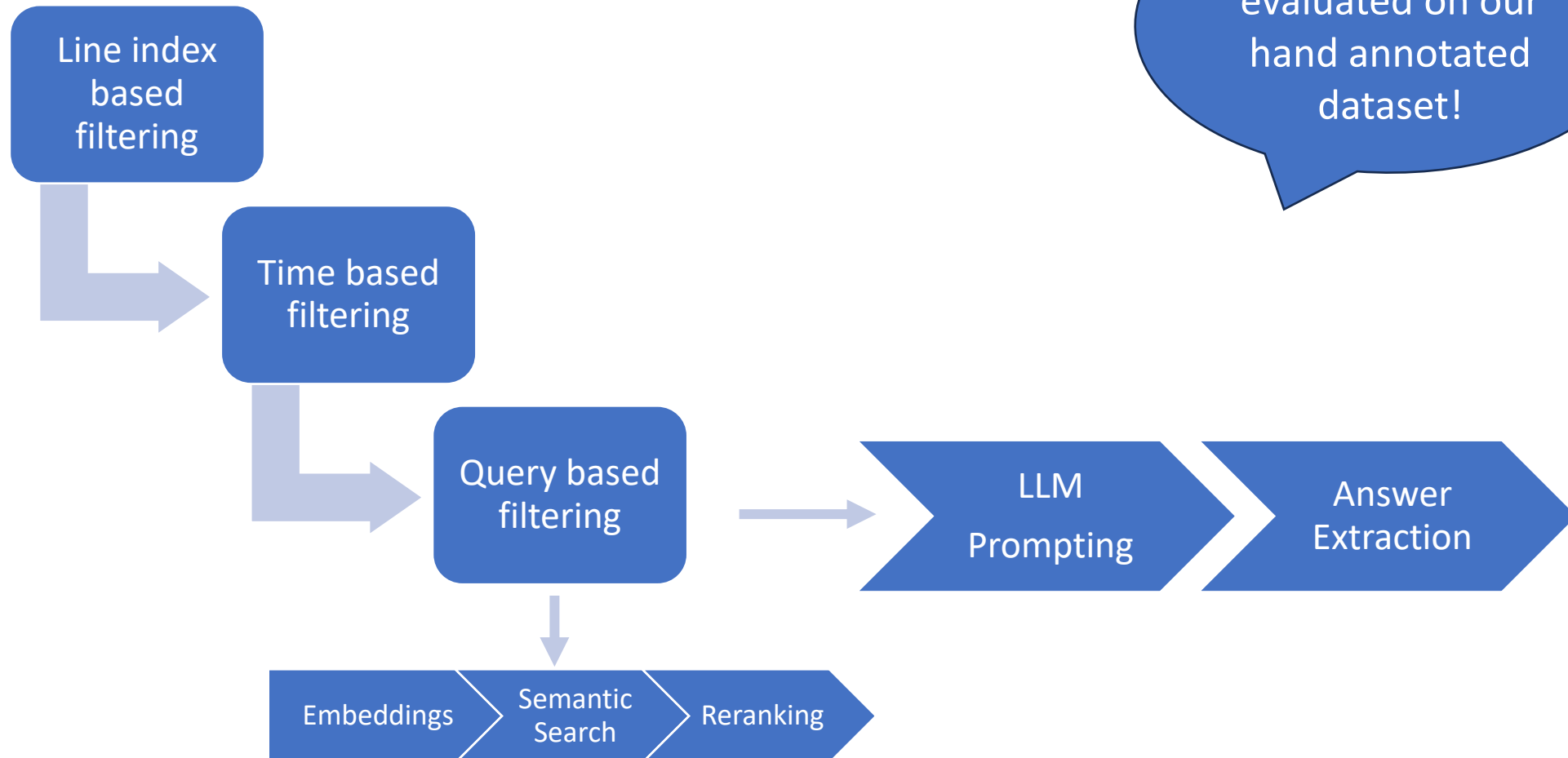
Log Search Mode

- Display most relevant loglines

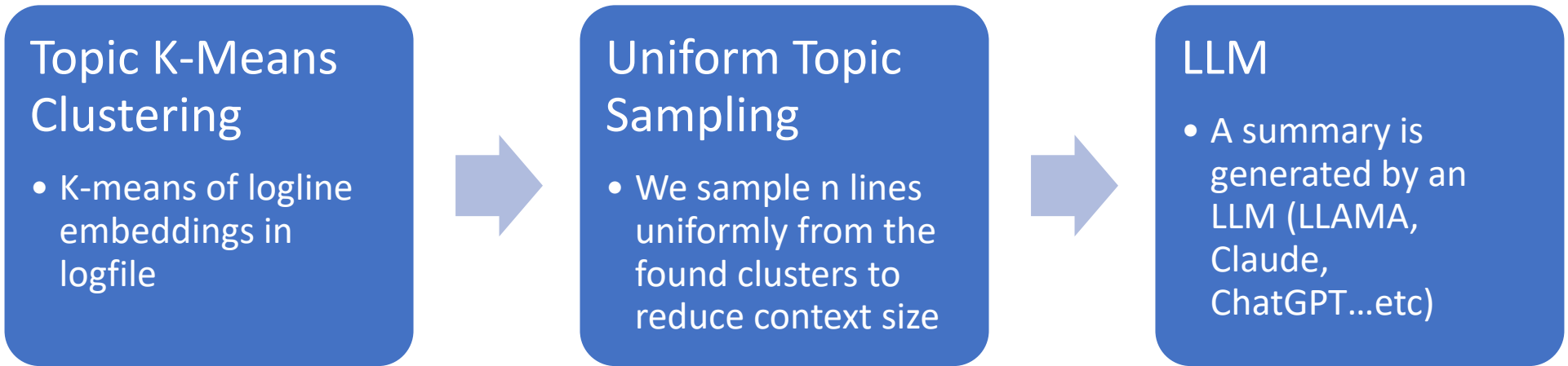


Summary Mode: Dynamic Summary

- Parametrizable Summerizatoin



Summary Mode: Static (experimental)



Dataset and Testing Method

- We create and annotate a testset of 20 examples per hand from the file „test_log1.out“
- We use this testset to evaluate the performance of different, rerank algorithms, distance measures, embeddings models...etc.
- Example:
 - Question: *“When were the root privileges removed for user avahi?”*
 - Label: *“Log Line: 1451”*

Dataset and Testing Method

- As an evaluation metric we use the mean reciprocal rank:

$$\text{MRR} = \frac{1}{|Q|} \sum_{i=1}^{|Q|} \frac{1}{\text{rank}_i}$$