





GOOGLE GGLING

STRUCTURED LOGS

- ▶ Easy to read by humans & log aggregation systems
- ▶ Provides contextual information using labels
- ▶ Easy to filter by only selecting relevant labels



cedi@mae:~



cedi@mae ~

zsh cedi-dev-admin@cedi-dev : observability

```
> kubectl logs -n observability loki-backend-0 | grep "error" | grep -v "403" | tail -n 1
```

```
level=error ts=2023-05-22T14:01:24.044644417Z caller=table.go:342 table-name=loki_index_19498 org_id=fake msg="index set fake has some problem, cleaning it up" err="open /var/loki/boltdb-shipper-cache/loki_index_19498/fake: no such file or directory"
```

cedi@mae ~

zsh 2.779s cedi-dev-admin@cedi-dev : observability







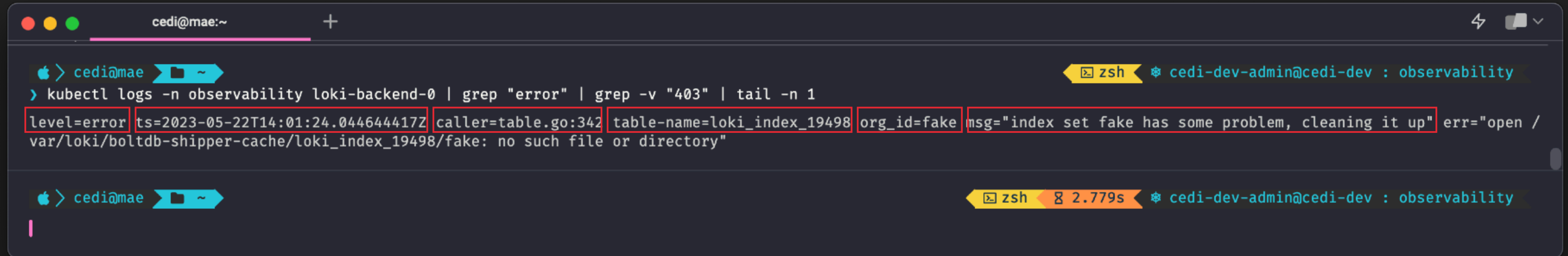








# STRUCTURED LOGS

A terminal window titled 'cedi@mae:~' with a '+' icon and window controls. It shows a command to filter logs for errors with a 403 status. The output is a single log line with various labels highlighted by red boxes. A second terminal window is partially visible below, showing a shell prompt and a timer.

```
cedi@mae:~  
> kubectl logs -n observability loki-backend-0 | grep "error" | grep -v "403" | tail -n 1  
level=error ts=2023-05-22T14:01:24.044644417Z caller=table.go:342 table-name=loki_index_19498 org_id=fake msg="index set fake has some problem, cleaning it up" err="open /  
var/loki/boltdb-shipper-cache/loki_index_19498/fake: no such file or directory"  
  
cedi@mae:~  
|
```

- ▶ Easy to read by humans & log aggregation systems
- ▶ Provides contextual information using labels
- ▶ Easy to filter by only selecting relevant labels

## STRUCTURED LOGGING FORMATS

- ▶ logfmt
- ▶ JSON
- ▶ Common Event Format (CEF)
- ▶ W3C Extended Log File Format