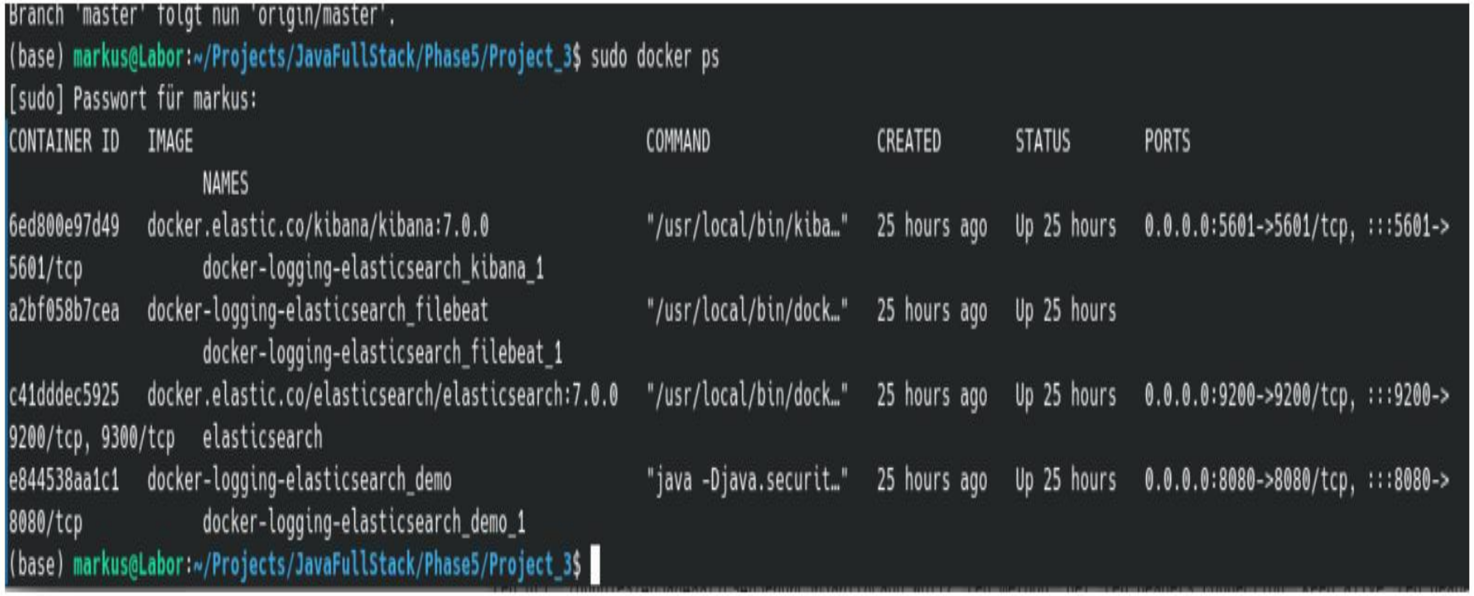
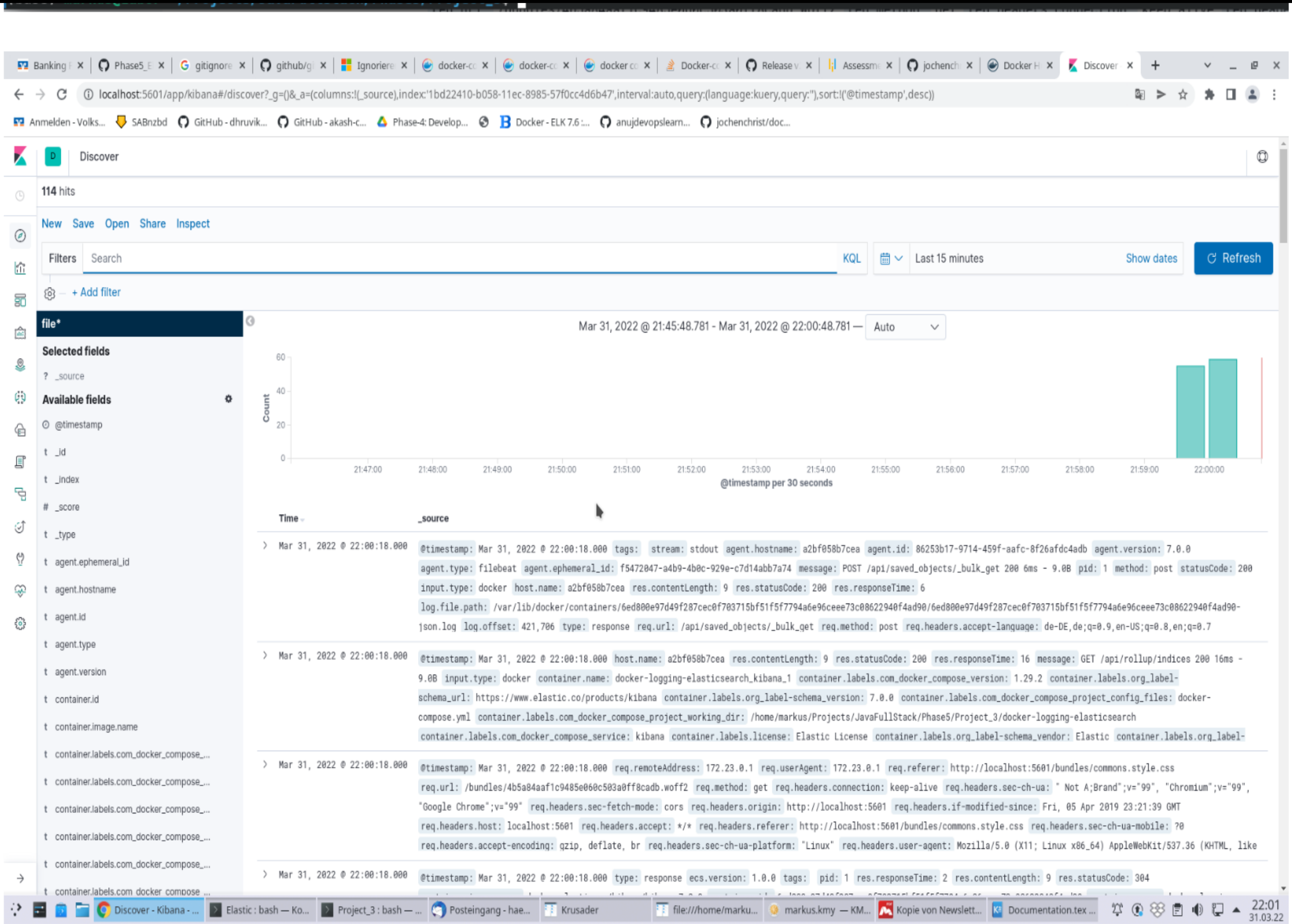
Project Output

Continuous Monitoring on Docker with ELK Stack.



```
Branch 'master' folgt nun 'origin/master'.
(base) markus@Labor:~/Projects/JavaFullStack/Phase5/Project_3$ sudo docker ps
[sudo] Passwort für markus:
CONTAINER ID   IMAGE                                                 COMMAND                  CREATED        STATUS        PORTS
                 NAMES
6ed800e97d49   docker.elastic.co/kibana/kibana:7.0.0                 "/usr/local/bin/kiba…"   25 hours ago   Up 25 hours   0.0.0.0:5601->5601/tcp, :::5601->
5601/tcp         docker-logging-elasticsearch_kibana_1
a2bf058b7cea   docker-logging-elasticsearch_filebeat                 "/usr/local/bin/dock…"   25 hours ago   Up 25 hours
                 docker-logging-elasticsearch_filebeat_1
c41dddec5925   docker.elastic.co/elasticsearch/elasticsearch:7.0.0   "/usr/local/bin/dock…"   25 hours ago   Up 25 hours   0.0.0.0:9200->9200/tcp, :::9200->
9200/tcp, 9300/tcp   elasticsearch
e844538aa1c1   docker-logging-elasticsearch_demo                     "java -Djava.securit…"   25 hours ago   Up 25 hours   0.0.0.0:8080->8080/tcp, :::8080->
8080/tcp         docker-logging-elasticsearch_demo_1
(base) markus@Labor:~/Projects/JavaFullStack/Phase5/Project_3$
```



localhost:5601/app/kibana#/discover?_g=()&_a=(columns:!(_source),index:'1bd22410-b058-11ec-8985-57f0cc4d6b47',interval:auto,query:(language:kuery,query:''),sort:!('@timestamp',desc))

114 hits

Mar 31, 2022 @ 21:45:48.781 - Mar 31, 2022 @ 22:00:48.781 —

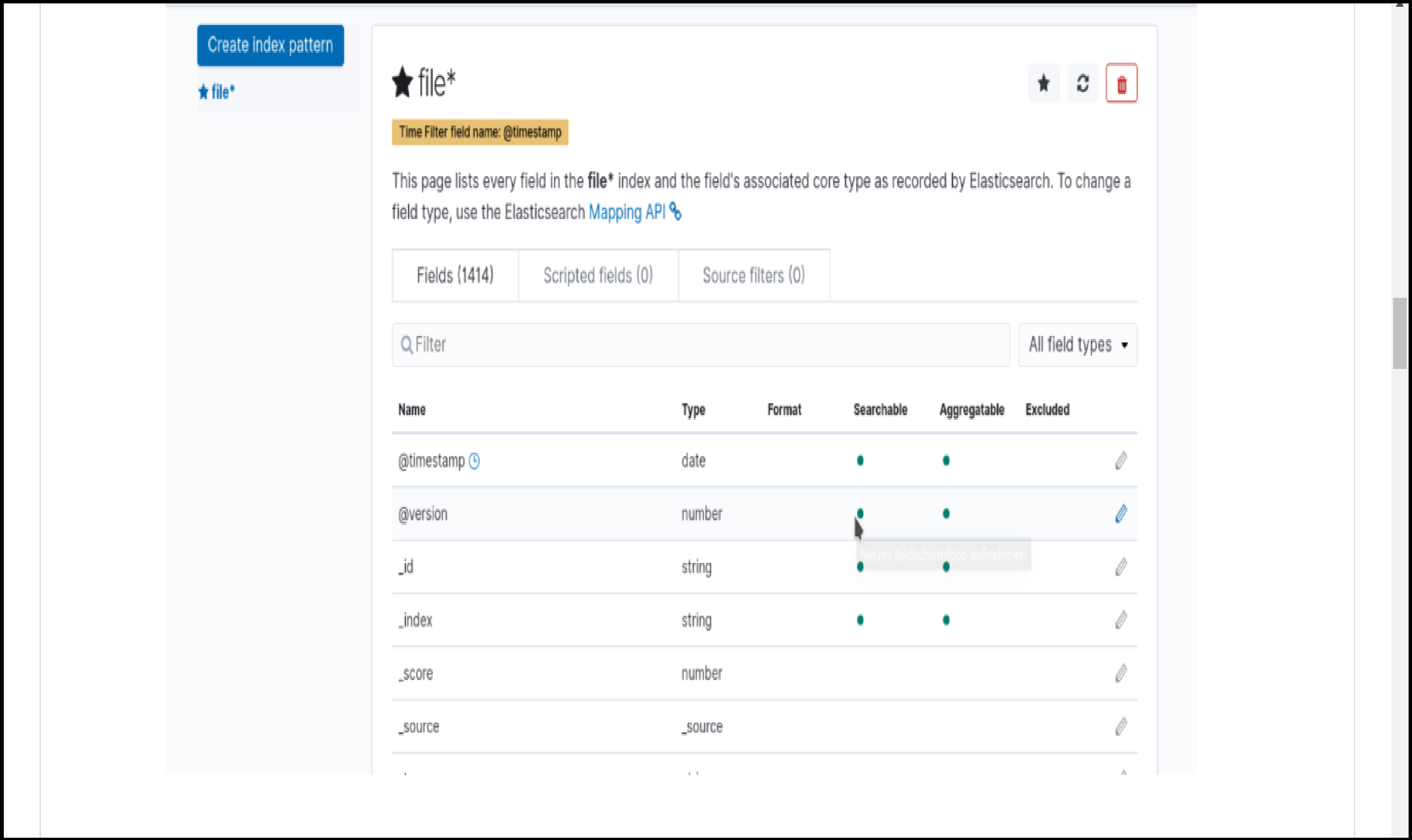
Selected fields

```
? _source
```

Available fields

```
@timestamp
t _id
t _index
# _score
t _type
t agent.ephemeral_id
t agent.hostname
t agent.id
t agent.type
t agent.version
t container.id
t container.image.name
t container.labels.com_docker_compose_...
t container.labels.com_docker_compose_...
t container.labels.com_docker_compose_...
t container.labels.com_docker_compose_...
t container.labels.com_docker_compose_...
t container.labels.com_docker_compose_...
```

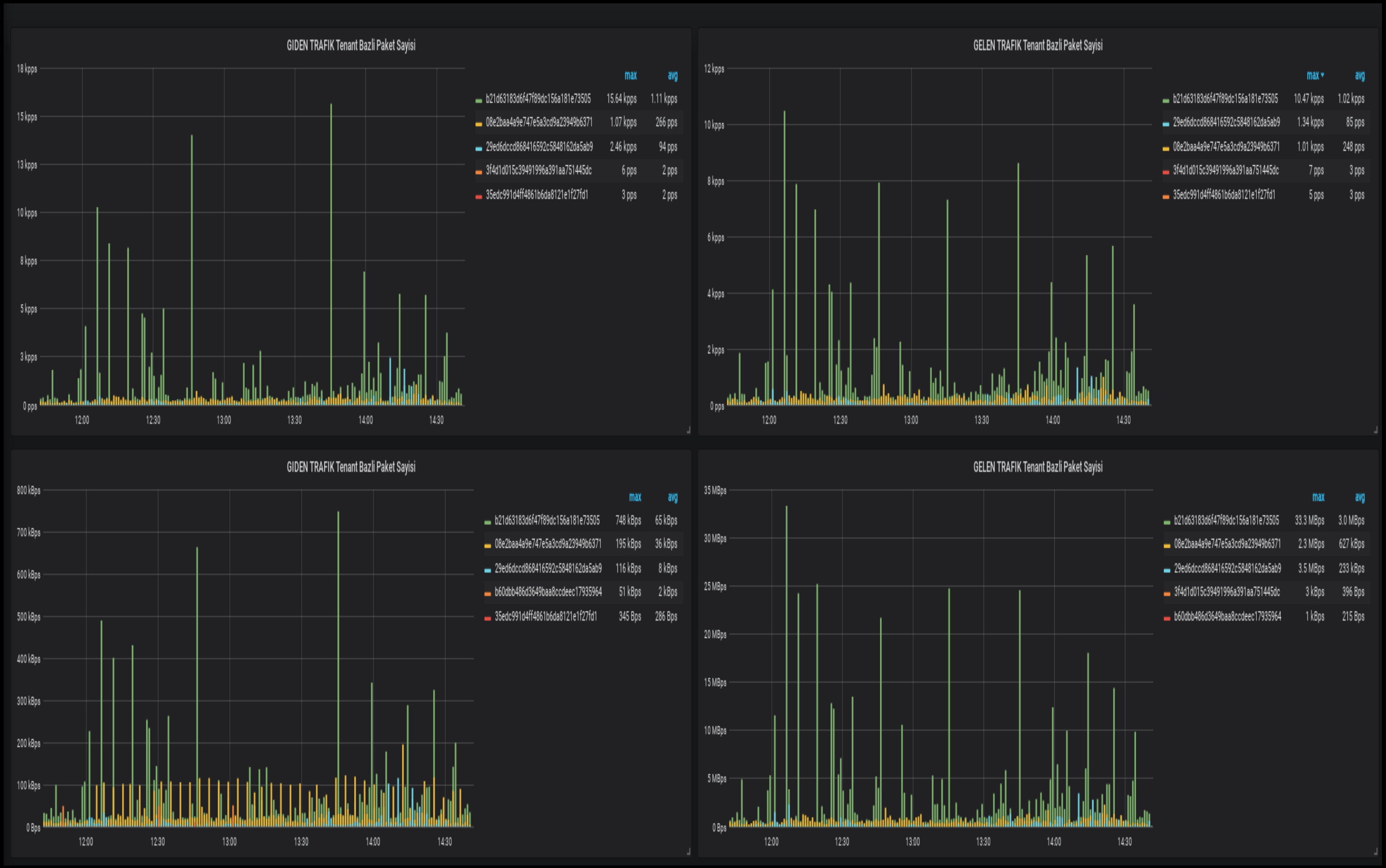
```
Time                       _source
> Mar 31, 2022 @ 22:00:18.000  @timestamp: Mar 31, 2022 @ 22:00:18.000 tags:  stream: stdout agent.hostname: a2bf058b7cea agent.id: 86253b17-9714-459f-aafc-8f26afdc4adb agent.version: 7.0.0
                             agent.type: filebeat agent.ephemeral_id: f5472047-a4b9-4b0c-929e-c7d14abb7a74 message: POST /api/saved_objects/_bulk_get 200 6ms - 9.0B pid: 1 method: post statusCode: 200
                             input.type: docker host.name: a2bf058b7cea res.contentLength: 9 res.statusCode: 200 res.responseTime: 6
                             log.file.path: /var/lib/docker/containers/6ed800e97d49f287cec0f703715bf51f5f7794a6e96ceee73c08622940f4ad90/6ed800e97d49f287cec0f703715bf51f5f7794a6e96ceee73c08622940f4ad90-
                             json.log log.offset: 421,706 type: response req.url: /api/saved_objects/_bulk_get req.method: post req.headers.accept-language: de-DE,de;q=0.9,en-US;q=0.8,en;q=0.7
> Mar 31, 2022 @ 22:00:18.000  @timestamp: Mar 31, 2022 @ 22:00:18.000 host.name: a2bf058b7cea res.contentLength: 9 res.statusCode: 200 res.responseTime: 16 message: GET /api/rollup/indices 200 16ms -
                             9.0B input.type: docker container.name: docker-logging-elasticsearch_kibana_1 container.labels.com_docker_compose_version: 1.29.2 container.labels.org_label-
                             schema_url: https://www.elastic.co/products/kibana container.labels.org_label-schema_version: 7.0.0 container.labels.com_docker_compose_project_config_files: docker-
                             compose.yml container.labels.com_docker_compose_project_working_dir: /home/markus/Projects/JavaFullStack/Phase5/Project_3/docker-logging-elasticsearch
                             container.labels.com_docker_compose_service: kibana container.labels.license: Elastic License container.labels.org_label-schema_vendor: Elastic container.labels.org_label-
> Mar 31, 2022 @ 22:00:18.000  @timestamp: Mar 31, 2022 @ 22:00:18.000 req.remoteAddress: 172.23.0.1 req.userAgent: 172.23.0.1 req.referer: http://localhost:5601/bundles/commons.style.css
                             req.url: /bundles/4b5a84aaf1c9485e060c503a0ff8cadb.woff2 req.method: get req.headers.connection: keep-alive req.headers.sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="99",
                             "Google Chrome";v="99" req.headers.sec-fetch-mode: cors req.headers.origin: http://localhost:5601 req.headers.if-modified-since: Fri, 05 Apr 2019 23:21:39 GMT
                             req.headers.host: localhost:5601 req.headers.accept: */* req.headers.referer: http://localhost:5601/bundles/commons.style.css req.headers.sec-ch-ua-mobile: ?0
                             req.headers.accept-encoding: gzip, deflate, br req.headers.sec-ch-ua-platform: "Linux" req.headers.user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
> Mar 31, 2022 @ 22:00:18.000  @timestamp: Mar 31, 2022 @ 22:00:18.000 type: response ecs.version: 1.0.0 tags:  pid: 1 res.responseTime: 2 res.contentLength: 9 res.statusCode: 304
```



Time Filter field name: @timestamp

This page lists every field in the **file*** index and the field's associated core type as recorded by Elasticsearch. To change a field type, use the Elasticsearch Mapping API

Name	Type	Format	Searchable	Aggregatable	Excluded
@timestamp	date		●	●	
@version	number		●	●	
_id	string		●	●	
_index	string		●	●	
_score	number				
_source	_source				



GIDEN TRAFIK Tenant Bazli Paket Sayisi

	max	avg
🟩 b21d63183d6f47f89dc156a181e73505	15.64 kpps	1.11 kpps
🟨 08e2baa4a9e747e5a3cd9a23949b6371	1.07 kpps	266 pps
🟦 29ed6dccd868416592c5848162da5ab9	2.46 kpps	94 pps
🟧 3f4d1d015c39491996a391aa751445dc	6 pps	2 pps
🟥 35edc991d4ff4861b6da8121e1f27fd1	3 pps	2 pps

GELEN TRAFIK Tenant Bazli Paket Sayisi

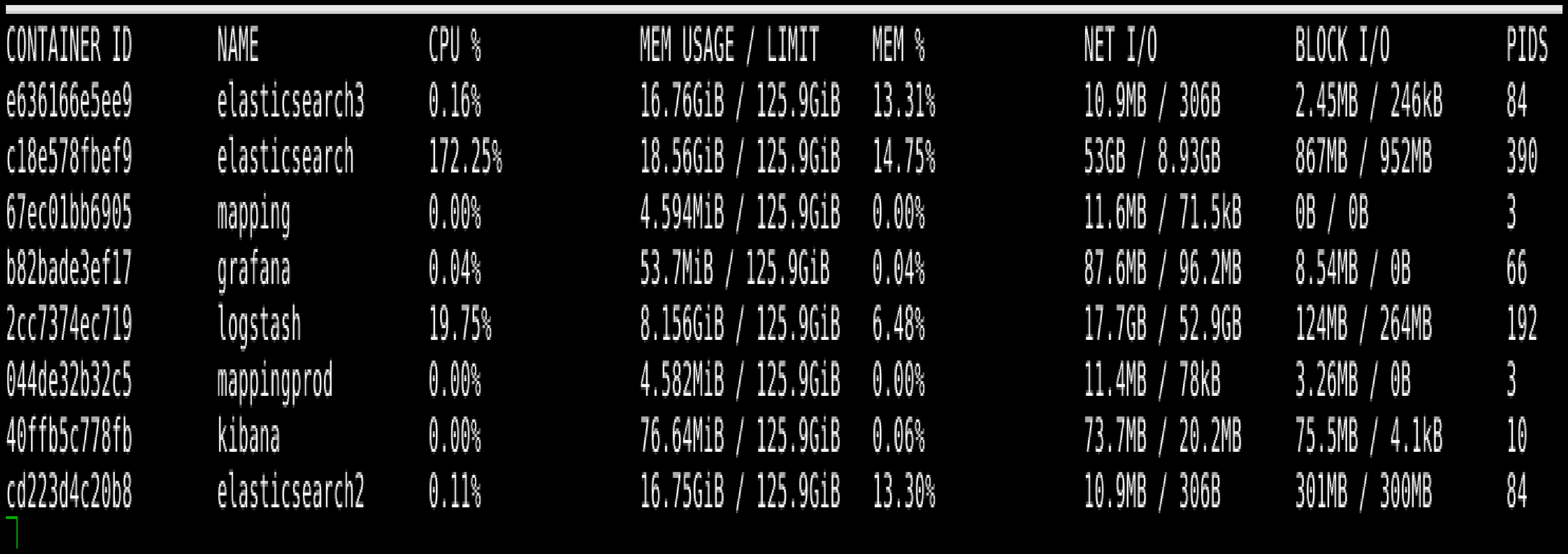
	max ▾	avg
🟩 b21d63183d6f47f89dc156a181e73505	10.47 kpps	1.02 kpps
🟦 29ed6dccd868416592c5848162da5ab9	1.34 kpps	85 pps
🟨 08e2baa4a9e747e5a3cd9a23949b6371	1.01 kpps	248 pps
🟥 3f4d1d015c39491996a391aa751445dc	7 pps	3 pps
🟧 35edc991d4ff4861b6da8121e1f27fd1	5 pps	3 pps

GIDEN TRAFIK Tenant Bazli Paket Sayisi

	max	avg
🟩 b21d63183d6f47f89dc156a181e73505	748 kBps	65 kBps
🟨 08e2baa4a9e747e5a3cd9a23949b6371	195 kBps	36 kBps
🟦 29ed6dccd868416592c5848162da5ab9	116 kBps	8 kBps
🟧 b60dbb486d3649baa8ccdeec17935964	51 kBps	2 kBps
🟥 35edc991d4ff4861b6da8121e1f27fd1	345 Bps	286 Bps

GELEN TRAFIK Tenant Bazli Paket Sayisi

	max	avg
🟩 b21d63183d6f47f89dc156a181e73505	33.3 MBps	3.0 MBps
🟨 08e2baa4a9e747e5a3cd9a23949b6371	2.3 MBps	627 kBps
🟦 29ed6dccd868416592c5848162da5ab9	3.5 MBps	233 kBps
🟧 3f4d1d015c39491996a391aa751445dc	3 kBps	396 Bps
🟥 b60dbb486d3649baa8ccdeec17935964	1 kBps	215 Bps



```
CONTAINER ID   NAME             CPU %     MEM USAGE / LIMIT     MEM %    NET I/O           BLOCK I/O         PIDS
e636166e5ee9   elasticsearch3   0.16%     16.76GiB / 125.9GiB   13.31%   10.9MB / 306B     2.45MB / 246kB    84
c18e578fbef9   elasticsearch    172.25%   18.56GiB / 125.9GiB   14.75%   53GB / 8.93GB     867MB / 952MB     390
67ec01bb6905   mapping          0.00%     4.594MiB / 125.9GiB   0.00%    11.6MB / 71.5kB   0B / 0B           3
b82bade3ef17   grafana          0.04%     53.7MiB / 125.9GiB    0.04%    87.6MB / 96.2MB   8.54MB / 0B       66
2cc7374ec719   logstash         19.75%    8.156GiB / 125.9GiB   6.48%    17.7GB / 52.9GB   124MB / 264MB     192
044de32b32c5   mappingprod      0.00%     4.582MiB / 125.9GiB   0.00%    11.4MB / 78kB     3.26MB / 0B       3
40ffb5c778fb   kibana           0.00%     76.64MiB / 125.9GiB   0.06%    73.7MB / 20.2MB   75.5MB / 4.1kB    10
cd223d4c20b8   elasticsearch2   0.11%     16.75GiB / 125.9GiB   13.30%   10.9MB / 306B     301MB / 300MB     84
```

=================== **THE END** ===================