**Шаги выполнения ТЗ:**

1. В рамках тестового задания выбран датасет Web Log Access Dataset

Файл логов: `access\_log.txt`.

<https://www.kaggle.com/datasets/sanjeevsahu/web-log-access-dataset>

1. Скачал файл логов. Создал папку проекта, в ней подпапку dataset. Переместил в нее файл access\_log\_Jul95.txt
2. Создал папку logstash в проекте. Разместил в ней файл конфига, включающий себя пайплайн для сбора и отправки данных.
3. Создал в корне проекта файл docker-compose.yml для развёртывания всех компонентов проекта в Docker-контейнерах.
4. Установил Docker Desktop на Windows.
5. Открыл терминал в корне проекта и выполнил команду docker-compose up.
6. Перешёл в браузере по адресу http://localhost:5601 — открылся интерфейс OpenSearch Dashboards.
7. В меню Dashboards Management создал новый index pattern “weblogs”, указав поле времени @timestamp
8. Убедился, что в Discover отображаются события из логов.
9. В разделе Visualize создал 5 различных визуализаций. На основе них создал дашборд. Настроил цвета. Положительная статистика – зелёный, нейтральная – синий, предупреждение – жёлтый, критическая – красный.

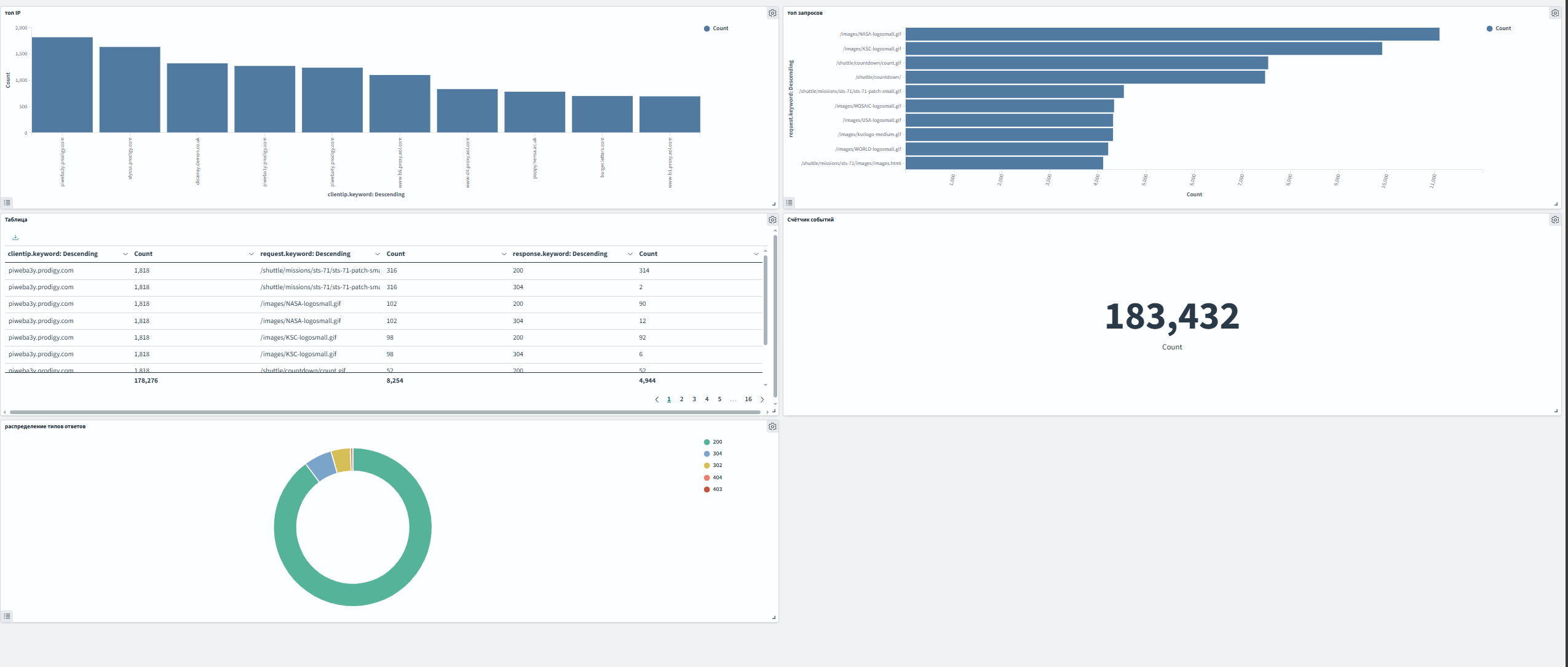
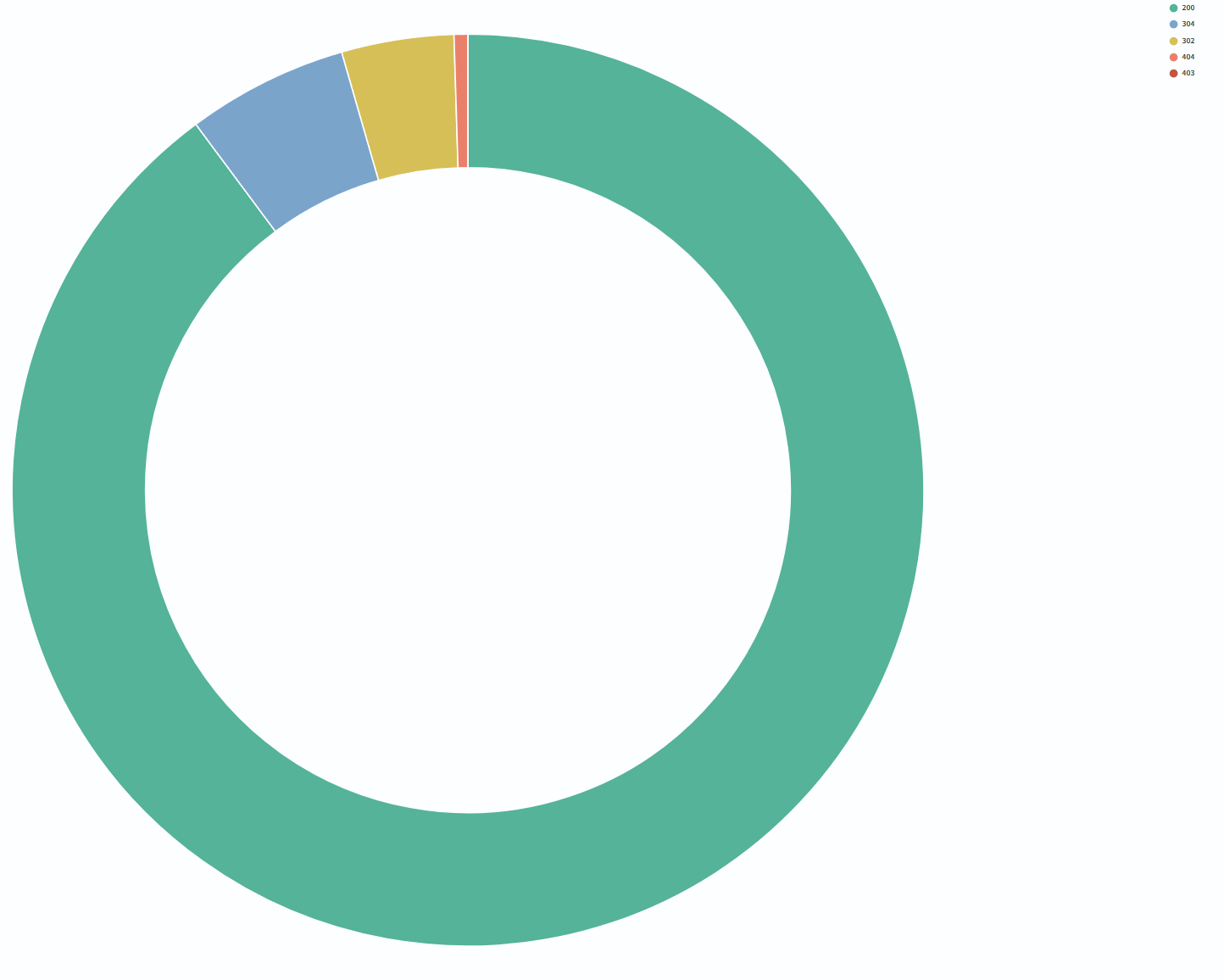
**Сложности и их решения**

**Docker Compose не работал** -требовал обновления в десктопном приложении, но не обновлялся. В результате был обновлен через консоль wsl --update.

**Logstash запускался некорректно (индекс `weblogs` не создавался автоматически)** — проблема была в невнимательности (сохранял изменения в VS в другой папке), при запуске не читался правильный файл конфига.

**Не отображался response –** при использовании маски %{COMBINEDAPACHELOG} не отображались некоторые поля. Заменил на: "message" => "%{IPORHOST:clientip} %{USER:ident} %{USER:auth} \[%{HTTPDATE:timestamp}\] \"%{WORD:verb} %{URIPATHPARAM:request}(?: HTTP/%{NUMBER:httpversion})?\" %{NUMBER:response} (?:%{NUMBER:bytes}|-)"

**Скриншоты**

**Используемые команды:**

перезапуск - docker restart logstash

- docker-compose restart logstash

логи - docker logs logstash

удаление старого индекса - curl -X DELETE <http://localhost:9200/weblogs>

проверка индексов - curl -X GET <http://localhost:9200/_cat/indices?v>

вкл\выкл - docker-compose down -v docker-compose up -d

проверки:

- docker exec -it logstash head -n 5 /usr/share/logstash/dataset/access\_log\_Jul95.txt

- docker exec -it logstash ls -l /usr/share/logstash/dataset