

**ДЗ 4**

## 1. Анализ логов приложения

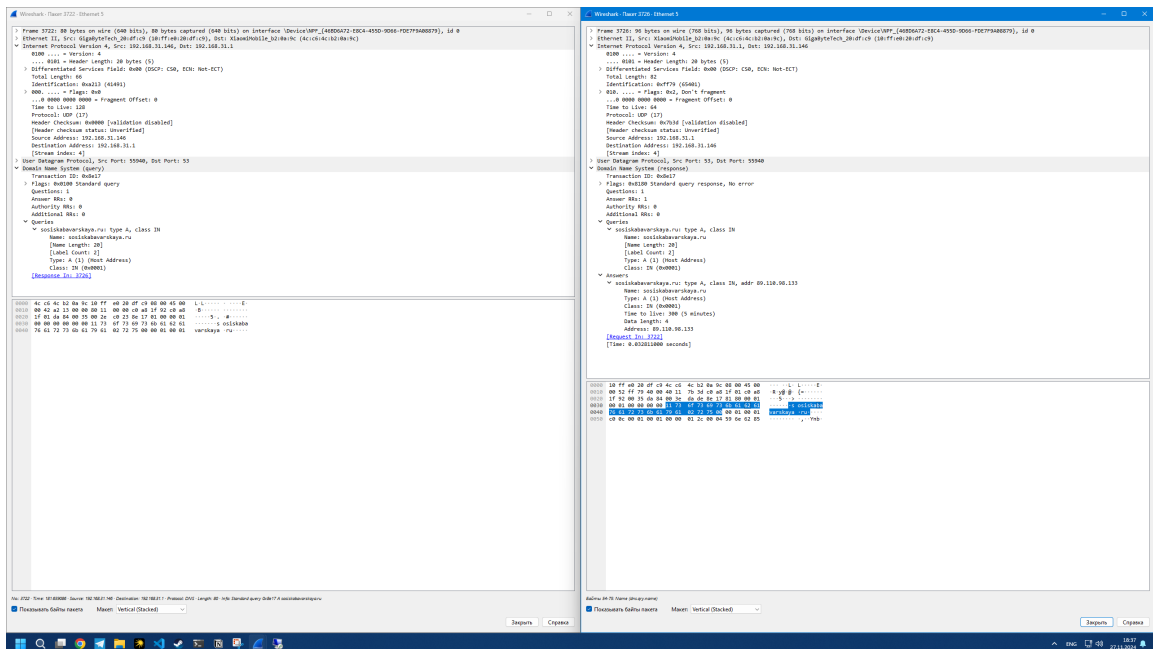
Условия: gitlab се установлен в системе контейнеризации Docker на удаленном сервере с ОС Ubuntu 24.04

[illegible]

Видно, что есть ошибки по кubernetes, это связано с ограничением SE версии гитлаба.

2. Установите Wireshark, выполните захват трафика и проанализируйте запросы DNS.

Также анализирую перехваченные пакеты при запросе к `sosiskabavarskaya.ru`



В левом окне видно, что клиент с айпи адресом 192.168.31.146 (айпи адрес машины в локальной сети) отправил dns запрос на сервер 192.168.31.1 (dns сервер в локалке) с вопросом о домене sosiskabavarskaya.ru.

запрос типа A, означающий поиск клиентом ipv4 адреса для указанного домена.

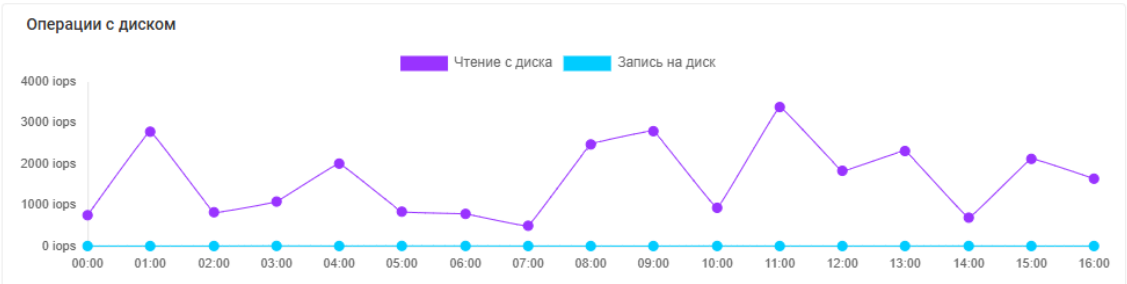
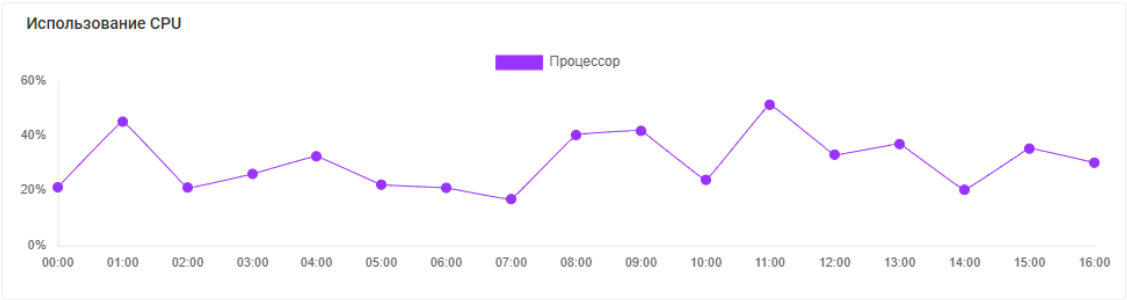
В правом окне видно, что ответ dns сервера такой: домен sosiskabavarskaya соответствует ip адресу 89.110.90.133, что подтверждается у провайдера vds и ns записями у провайдера ns записей

89.110.98.133   АКТИВНО   Ubuntu 24.04   Процессор: 2 core   Память: 4 Gb   Хранилище: 100 Gb   Трафик: 32 Tb

Управление   Доступ   Тариф   Переустановка   IP   Локальная сеть   Резервные копии   Внешние диски   **Статистика**

### Мониторинг

Период  
Сегодня



DNS management for **sosiskabavarskaya.ru**

Review, add, and edit DNS records. Edits will go into effect once saved.

DNS Setup: Full ⓘ   Import and Export ▾   ⚙ Dashboard Display Settings

Search DNS Records

<input type="checkbox"/>	Type ⓘ	Name ⓘ	Content ⓘ	Proxy status ⓘ	TTL ⓘ	Actions
<input type="checkbox"/>				☁ DNS only	Auto	<a href="#">Edit ▶</a>
<input type="checkbox"/>				☁ DNS only	Auto	<a href="#">Edit ▶</a>
<input type="checkbox"/>				☁ DNS only	Auto	<a href="#">Edit ▶</a>
<input type="checkbox"/>	A	sosiskabavarskaya.ru	89.110.98.133	☁ DNS only	Auto	<a href="#">Edit ▶</a>

**Cloudflare Nameservers**

Every DNS zone on Cloudflare is assigned a set of Cloudflare-branded nameservers.

Type	Value
NS	bella.ns.cloudflare.com
NS	kareem.ns.cloudflare.com

а также выполнением команды dig (NS записи совпадают)

```

gitlab@v2681068:~$ dig NS sosiskabavarskaya.ru

; <<>> DiG 9.18.28-0ubuntu0.24.04.1-Ubuntu <<>> NS sosiskabavarskaya.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42735
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;sosiskabavarskaya.ru.          IN      NS

;; ANSWER SECTION:
sosiskabavarskaya.ru.  21600   IN      NS      bella.ns.cloudflare.com.
sosiskabavarskaya.ru.  21600   IN      NS      kareem.ns.cloudflare.com.

;; Query time: 55 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Wed Nov 27 16:41:51 MSK 2024
;; MSG SIZE rcvd: 107

gitlab@v2681068:~$ █

```

Так как ответ корректен, то dns-сервер успешно разрешил имя домена в ip-адрес. Т.е. домен активен и зарегистрирован.

Также отдельно видно, что айпи вдски доступен, сервер принимает соединения и все в целом хорошо

```

sosiskabavarskaya@sosiskabavarska:~$ nmap -Pn sosiskabavarskaya.ru
Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-27 18:46 +05
Nmap scan report for sosiskabavarskaya.ru (89.110.98.133)
Host is up (0.025s latency).
rDNS record for 89.110.98.133: v2681068.hosted-by-vdsina.ru
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 5.02 seconds
sosiskabavarskaya@sosiskabavarska:~$ █

```