



МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«МИРЭА – Российский технологический университет»
РТУ МИРЭА

Институт кибербезопасности и цифровых технологий
(наименование института, филиала)

Кафедра КБ-2«Информационно-аналитические системы кибербезопасности»
(наименование кафедры)

ОТЧЕТ

по дисциплине: «Технологии хранения в системах кибербезопасности»

Задание получил:

III курс, группа БИСО-02-23

Подпись

Макаревич Сергей Витальевич

ФИО

Проверил:

«__ » 2025 г.

Дата

Подпись

Селин А. А.

ФИО

Отметка / результат

Москва 2025 г.

Оглавление

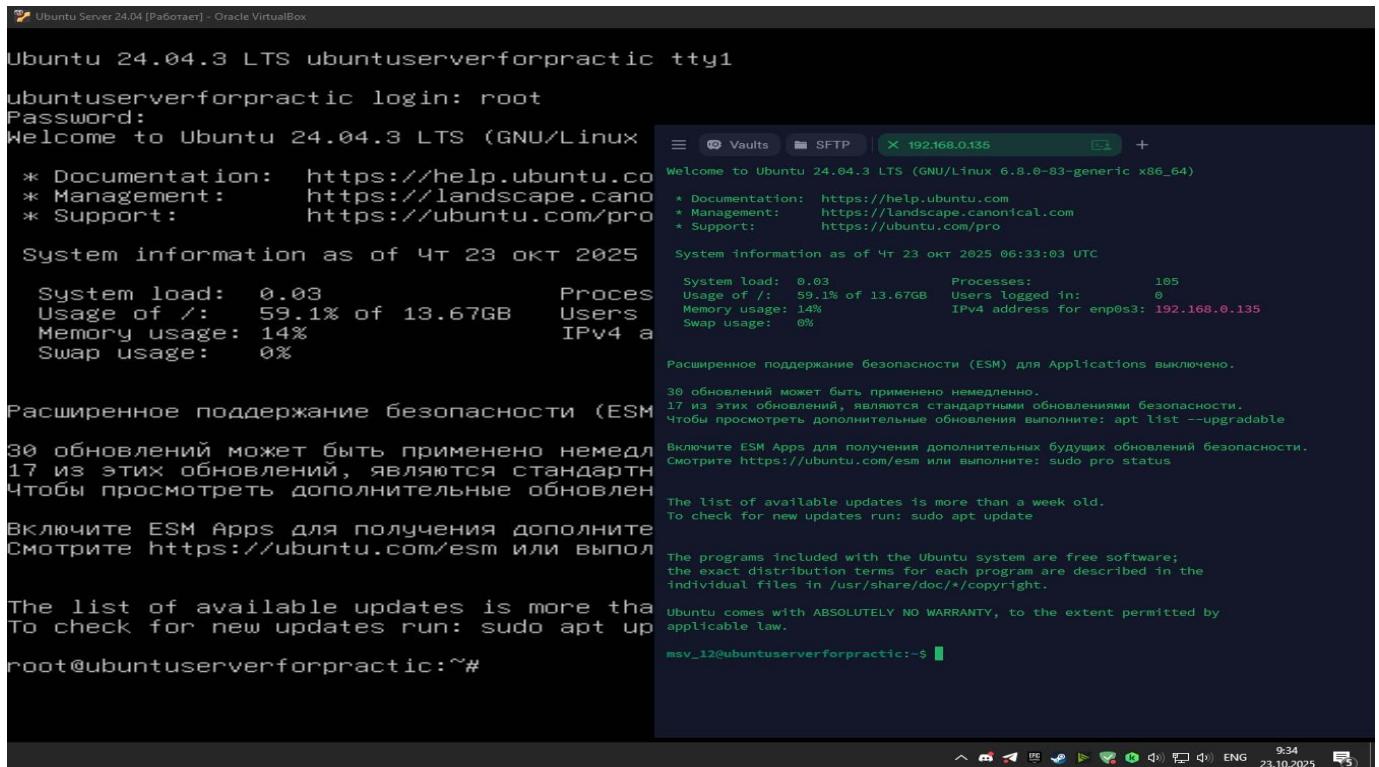
1.	Запуск виртуальной машины с Ubuntu Server 24.04, подключение к ней по ssh используя ПО Termius для удобства взаимодействия.....	3
2.	Создание пользователя и настройка окружения	3
3.	Установка Docker и Docker Compose	4
4.	Настройка параметров ядра(Постоянное изменение)	5
5.	Создание docker-compose.yml для OpenSearch	5
6.	Запуск OpenSearch	6
7.	Установка TShark.....	7
8.	Скачивание образцов трафика.....	7
9.	Обработка PCAP-файлов с помощью TShark.....	8
10.	Загрузка данных используя Python скрипт.....	10
11.	Запуск панели, подготовка OpenSearchDashboards.....	11
12.	Выполним поиск в разделе Discover.	12
13.	Создадим несколько визуализаций.	14
14.	Изучим OpenSearch Alerting.	18
15.	Изучим возможности OpenSearch Dashboards по анализу гео-данных	19
16.	Заключение.....	22

ПРАКТИЧЕСКАЯ РАБОТА № 4

«Знакомство с инструментами для работы с частично структуризованными данными на примере документо-ориентированной СУБД MongoDB»

Цель работы – получение навыков развертывания приложений с использованием Docker.

1. Запуск виртуальной машины с Ubuntu Server 24.04, подключение к ней по ssh используя ПО Termius для удобства взаимодействия.



```
Ubuntu 24.04.3 LTS ubuntuserverforpractic tty1
ubuntuserverforpractic login: root
Password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-83-generic x86_64)

 * Documentation:  https://help.ubuntu.co
 * Management:    https://landscape.canon
 * Support:       https://ubuntu.com/pro

System information as of 4т 23 окт 2025

System load:  0.03           Processes:          105
Usage of /:   59.1% of 13.67GB  Users logged in:   0
Memory usage: 14%           IPv4 address for enp0s3: 192.168.0.135
Swap usage:   0%             Swap usage:        0%

Расширенное поддержание безопасности (ESM)

30 обновлений может быть применено немедленно.
17 из этих обновлений, являются стандартными обновлениями безопасности.
Чтобы просмотреть дополнительные обновления выполните: apt list --upgradable

Включите ESM Apps для получения дополнительных будущих обновлений безопасности.
Смотрите https://ubuntu.com/esm или выполните: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

msv_12@ubuntuserverforpractic:~#
```

2. Создание пользователя и настройка окружения

```
root@ubuntuserverforpractic:~# sudo adduser msv_12
info: Adding user `msv_12' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `msv_12' (1001) ...
info: Adding new user `msv_12' (1001) with group `msv_12 (1001)' ...
info: Creating home directory `/home/msv_12' ...
info: Copying files from `/etc/skel' ...

New password:
Retype new password:
passwd: password updated successfully
Changing the user information for msv_12
Enter the new value, or press ENTER for the default
      Full Name []:
      Room Number []:
      Work Phone []:
      Home Phone []:
      Other []:
Is the information correct? [Y/n] y
info: Adding new user `msv_12' to supplemental / extra groups `users' ...
info: Adding user `msv_12' to group `users' ...
```

```

root@ubuntuserverforpractic:~# sudo usermod -aG sudo msv_12
root@ubuntuserverforpractic:~# 
root@ubuntuserverforpractic:~# su msv_12
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

msv_12@ubuntuserverforpractic:/root$ 

```

3. Установка Docker и Docker Compose

3.1. Обновление пакетов и установка зависимостей

```

individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

msv_12@ubuntuserverforpractic:~$ sudo apt update && sudo apt upgrade -y
[sudo] password for msv_12:
Пол:1 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Пол:2 https://download.docker.com/linux/ubuntu noble InRelease [48,5 kB]
Пол:3 https://download.docker.com/linux/ubuntu noble/stable amd64 Packages [33,3 kB]
Пол:4 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [1 260 kB]
Пол:5 http://security.ubuntu.com/ubuntu noble-security/main Translation-en [208 kB]
Пол:6 http://security.ubuntu.com/ubuntu noble-security/main amd64 Components [21,5 kB]
Пол:7 http://security.ubuntu.com/ubuntu noble-security/main amd64 c-n-f Metadata [8 968 B]
Пол:8 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Packages [2 069 kB]
Пол:9 http://security.ubuntu.com/ubuntu noble-security/restricted Translation-en [468 kB]
Пол:10 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Components [208 B]
Пол:11 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 c-n-f Metadata [500 B]
Пол:12 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Packages [904 kB]
Пол:13 http://security.ubuntu.com/ubuntu noble-security/universe Translation-en [202 kB]
Пол:14 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components [52,3 kB]
Пол:15 http://security.ubuntu.com/ubuntu noble-security/universe amd64 c-n-f Metadata [19,3 kB]
Пол:16 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Packages [27,4 kB]
Пол:17 http://security.ubuntu.com/ubuntu noble-security/multiverse Translation-en [5 708 B]
Пол:18 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Components [208 B]
Пол:19 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 c-n-f Metadata [384 B]
Сущ:20 http://ru.archive.ubuntu.com/ubuntu noble InRelease
Пол:21 http://ru.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Пол:22 http://ru.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Пол:23 http://ru.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [1 535 kB]
Пол:24 http://ru.archive.ubuntu.com/ubuntu noble-updates/main Translation-en [292 kB]
Пол:25 http://ru.archive.ubuntu.com/ubuntu noble-updates/main amd64 Components [175 kB]
Пол:26 http://ru.archive.ubuntu.com/ubuntu noble-updates/main amd64 c-n-f Metadata [15,3 kB]
Пол:27 http://ru.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Packages [2 164 kB]
Пол:28 http://ru.archive.ubuntu.com/ubuntu noble-updates/restricted Translation-en [488 kB]
Пол:29 http://ru.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Components [212 B]
Пол:30 http://ru.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 c-n-f Metadata [516 B]
Пол:31 http://ru.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [1 496 kB]
Пол:32 http://ru.archive.ubuntu.com/ubuntu noble-updates/universe Translation-en [301 kB]
Пол:33 http://ru.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Components [378 kB]
Пол:34 http://ru.archive.ubuntu.com/ubuntu noble-updates/universe amd64 c-n-f Metadata [31,3 kB]
Пол:35 http://ru.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Packages [30,3 kB]
Пол:36 http://ru.archive.ubuntu.com/ubuntu noble-updates/multiverse Translation-en [5 564 B]

```

9:41
ENG
23.10.2025

3.2. Установка Docker и Docker Compose через snap. Проверка установки.

```
msv_12@ubuntuserverforpractic:~$ sudo apt install snapd -y
Чтение списков пакетов... Готово
Построение дерева зависимостей... Готово
Чтение информации о состоянии... Готово
Уже установлен пакет snapd самой новой версии (2.71+ubuntu24.04).
Обновлено 0 пакетов, установлено 0 новых пакетов, для удаления отмечено 0 пакетов
msv_12@ubuntuserverforpractic:~$ sudo snap install docker
snap "docker" is already installed, see 'snap help refresh'
msv_12@ubuntuserverforpractic:~$ docker --version
Docker version 28.5.1, build e180ab8
msv_12@ubuntuserverforpractic:~$ docker-compose --version
Docker Compose version v2.33.1
msv_12@ubuntuserverforpractic:~$
```

The screenshot shows a terminal window with a dark background. At the top, there are icons for 'Vaults' and 'SFTP'. The title bar says '192.168.0.135'. Below the title bar is a scrollable text area containing the command-line session. At the bottom of the terminal window, there is a status bar with various icons and the text '9:48 23.10.2025'.

4. Настройка параметров ядра(Постоянное изменение)

```
msv_12@ubuntuserverforpractic:~$ echo "vm.max_map_count=262144" | sudo tee -a /etc/sysctl.conf
[sudo] password for msv_12:
vm.max_map_count=262144
msv_12@ubuntuserverforpractic:~$
```

The screenshot shows a terminal window with a dark background. At the bottom, there is a status bar with various icons and the text '13:37 06.11.2025'.

5. Создание docker-compose.yml для OpenSearch

```
msv_12@ubuntuserverforpractic:~$ echo "vm.max_map_count=262144" | sudo tee -a /etc/sysctl.conf
[sudo] password for msv_12:
vm.max_map_count=262144
msv_12@ubuntuserverforpractic:~$ mkdir opensearch-msv
cd opensearch-msv
msv_12@ubuntuserverforpractic:~/opensearch-msv$
```

The screenshot shows a terminal window with a dark background. At the bottom, there is a status bar with various icons and the text '13:42 06.11.2025'.

```

services:
  opensearch:
    image: opensearchproject/opensearch:latest
    container_name: opensearch_msv
    environment:
      - cluster.name=opensearch-cluster-msv
      - node.name=opensearch-node-msv
      - discovery.type=single-node
      # УДАЛИТЬ ЭТУ СТРОКУ: - cluster.initial_cluster_manager_nodes=opensearch-node-msv
      - bootstrap.memory_lock=true
      - "OPENSEARCH_JAVA_OPTS=-Xms512m -Xmx512m"
      - "DISABLE_INSTALL_DEMO_CONFIG=true"
      - "DISABLE_SECURITY_PLUGIN=true"
    ulimits:
      memlock:
        soft: -1
        hard: -1
      nofile:
        soft: 65536
        hard: 65536
    volumes:
      - opensearch-data-msv:/usr/share/opensearch/data
    ports:
      - "9212:9200"
      - "9600:9600"
    networks:
      - opensearch-net-msv
    restart: unless-stopped

  dashboards:
    image: opensearchproject/opensearch-dashboards:latest
    container_name: dashboards_msv
    environment:
      - 'OPENSEARCH_HOSTS=[ "http://opensearch:9200" ]'
      - "DISABLE_SECURITY_DASHBOARDS_PLUGIN=true"
    ports:
      - "5612:5601"
    networks:
      - opensearch-net-msv
    restart: unless-stopped
    depends_on:
      - opensearch

  volumes:
    opensearch-data-msv:

networks:
  opensearch-net-msv:

```

6. Запуск OpenSearch

```

msv_12@ubuntuserverforpractic:~/opensearch-msv$ sudo docker-compose up -d
[+] Running 2/2
  I dashboards      Interrupted
  X opensearch Error Get "https://registry-1.docker.io/v2/": net/http: TLS handshake timeout
Error response from daemon: Get "https://registry-1.docker.io/v2/": net/http: TLS handshake timeout
msv_12@ubuntuserverforpractic:~/opensearch-msv$ sudo docker-compose up -d
[+] Running 10/14
  :: dashboards [=====] 497.3MB / 497.6MB Pulling
    ✓ 6b8641a67e6c Pull complete
    ✓ 1ea1219adecd Pull complete
    ✓ 834cbf21ef4b Pull complete
    ✓ d7ef3b8e965e Pull complete
    ┌ 758c91650d37 Extracting      [=====] 287.4MB/417MB
    ✓ 4f4fb700ef54 Download complete
  :: opensearch [=====] 1.048GB / 1.048GB Pulling
    ✓ a6a2e926a3ac Pull complete
    ✓ 4324580a1ad5 Pull complete
    ✓ 7bb4c0e3d646 Pull complete
    :: ade63c612292 Downloading      [=====] 989.9MB/989.9MB
    ✓ d58586574fdd Download complete
    ✓ 1f4cdd2bc9bb Download complete
write /var/snap/docker/common/var-lib-docker/tmp/GetImageBlob703835994: no space left on device
msv_12@ubuntuserverforpractic:~/opensearch-msv$ 

```

7. Установка TShark

```
msv_12@ubuntuserverforpractic:~/opensearch-msv$ sudo apt install tshark --f
Чтение списков пакетов... Готово
Построение дерева зависимостей... Готово
Чтение информации о состоянии... Готово
Будут установлены следующие дополнительные пакеты:
  libb6cg729-0 libcares2 liblua5.2-0 libnghhttp3-3 libopencore-amrnb0 libopus
  libssh-gcrypt-4 libwireshark-data libwireshark17t64 libwiretap14t64 libws
Предлагаемые пакеты:
  opus-tools snmp-mibs-downloader geoipupdate geoip-database geoip-database
Следующие НОВЫЕ пакеты будут установлены:
  libb6cg729-0 libcares2 liblua5.2-0 libnghhttp3-3 libopencore-amrnb0 libopus
  libssh-gcrypt-4 libwireshark-data libwireshark17t64 libwiretap14t64 libws
Следующие пакеты будут обновлены:
  libssh-4
Обновлено 1 пакетов, установлено 18 новых пакетов, для удаления отмечено 0
Необходимо скачать 412 kB/26,8 MB архивов.
После данной операции объём занятого дискового пространства возрастёт на 13
Пол:1 http://ru.archive.ubuntu.com/ubuntu noble-updates/main amd64 libssh-4
Пол:2 http://ru.archive.ubuntu.com/ubuntu noble-updates/main amd64 libssh-g
Получено 412 kB за 1с (543 kB/s)
Предварительная настройка пакетов ...
Выбор ранее не выбранного пакета libb6cg729-0:amd64.
(Чтение базы данных ... на данный момент установлено 137659 файлов и каталогов)
Подготовка к распаковке .../00-libb6cg729-0_1.1.1-2build1_amd64.deb ...
Распаковывается libb6cg729-0:amd64 (1.1.1-2build1) ...
Выбор ранее не выбранного пакета libcares2:amd64.
Подготовка к распаковке .../01-libcares2_1.27.0-1.0ubuntu1_amd64.deb ...
Распаковывается libcares2:amd64 (1.27.0-1.0ubuntu1) ...
Выбор ранее не выбранного пакета liblua5.2-0:amd64.
Подготовка к распаковке .../02-liblua5.2-0_5.2.4-3build2_amd64.deb ...
Распаковывается liblua5.2-0:amd64 (5.2.4-3build2) ...
Выбор ранее не выбранного пакета libnghhttp3-3:amd64.
Подготовка к распаковке .../03-libnghhttp3-3_0.8.0-2_amd64.deb ...
Распаковывается libnghhttp3-3:amd64 (0.8.0-2) ...
Выбор ранее не выбранного пакета libopencore-amrnb0:amd64.
Подготовка к распаковке .../04-libopencore-amrnb0_0.1.6-1build1_amd64.deb ...
Распаковывается libopencore-amrnb0:amd64 (0.1.6-1build1) ...
Выбор ранее не выбранного пакета libopus0:amd64.
Подготовка к распаковке .../05-libopus0_1.4-1build1_amd64.deb ...
Распаковывается libopus0:amd64 (1.4-1build1) ...

13:55 06.11.2025 27
```

8. Скачивание образцов трафика

В процессе поиска файлов на сайте <https://www.malware-traffic-analysis.net> были найдены три наиболее подходящих по условию задания:

1. <https://www.malware-traffic-analysis.net/2023/02/13/2023-02-13-IcedID-traffic-carved-and-sanitized.pcap.zip>
2. <https://www.malware-traffic-analysis.net/2023/02/23/2023-02-23-example-of-IcedID-from-URL-file-with-WebDAV-traffic.pcap.zip>
3. <https://www.malware-traffic-analysis.net/2023/02/27/2023-02-27-Qakbot-infection-traffic.pcap.zip>

Скачиваем архивы используя wget:

```

msv_12@ubuntuserverforpractic:~/opensearch-msv$ wget https://www.malware-traffic-analysis.net/2023/02/13/2023-02-13-IcedID-traffic-carved-and-sanitized.pcap.zip
--2025-11-06 11:22:31-- https://www.malware-traffic-analysis.net/2023/02/13/2023-02-13-IcedID-traffic-carved-and-sanitized.pcap.zip
Resolving www.malware-traffic-analysis.net (www.malware-traffic-analysis.net)... 199.201.110.204
Connecting to www.malware-traffic-analysis.net (www.malware-traffic-analysis.net)|199.201.110.204|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4838817 (4,6M) [application/zip]
Saving to: '2023-02-13-IcedID-traffic-carved-and-sanitized.pcap.zip'

2023-02-13-IcedID-traffic-carved-and-sanitized.pcap.zip 100%[=====] 4,61M 2,82MB/s in 1,6s

2025-11-06 11:22:33 (2,82 MB/s) - '2023-02-13-IcedID-traffic-carved-and-sanitized.pcap.zip' saved [4838817/4838817]

msv_12@ubuntuserverforpractic:~/opensearch-msv$ wget https://www.malware-traffic-analysis.net/2023/02/23/2023-02-23-example-of-IcedID-from-URL-file-with-WebDAV-traffic.pcap.zip
--2025-11-06 11:22:55-- https://www.malware-traffic-analysis.net/2023/02/23/2023-02-23-example-of-IcedID-from-URL-file-with-WebDAV-traffic.pcap.zip
Resolving www.malware-traffic-analysis.net (www.malware-traffic-analysis.net)... 199.201.110.204
Connecting to www.malware-traffic-analysis.net (www.malware-traffic-analysis.net)|199.201.110.204|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2698164 (2,6M) [application/zip]
Saving to: '2023-02-23-example-of-IcedID-from-URL-file-with-WebDAV-traffic.pcap.zip'

2023-02-23-example-of-IcedID-from-URL-file-with-WebDAV-traffic.pcap.zip 100%[=====] 2,57M 1,83MB/s in 1,4s

2025-11-06 11:22:57 (1,83 MB/s) - '2023-02-23-example-of-IcedID-from-URL-file-with-WebDAV-traffic.pcap.zip' saved [2698164/2698164]

msv_12@ubuntuserverforpractic:~/opensearch-msv$ wget https://www.malware-traffic-analysis.net/2023/02/27/2023-02-27-Qakbot-infection-traffic.pcap.zip
--2025-11-06 11:23:13-- https://www.malware-traffic-analysis.net/2023/02/27/2023-02-27-Qakbot-infection-traffic.pcap.zip
Resolving www.malware-traffic-analysis.net (www.malware-traffic-analysis.net)... 199.201.110.204
Connecting to www.malware-traffic-analysis.net (www.malware-traffic-analysis.net)|199.201.110.204|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 17129439 (16M) [application/zip]
Saving to: '2023-02-27-Qakbot-infection-traffic.pcap.zip'

2023-02-27-Qakbot-infection-traffic.pcap.zip 100%[=====] 16,33M 7,35MB/s in 2,2s

2025-11-06 11:23:16 (7,35 MB/s) - '2023-02-27-Qakbot-infection-traffic.pcap.zip' saved [17129439/17129439]

msv_12@ubuntuserverforpractic:~/opensearch-msv$ █
```

14:28 06.11.2025 █

Теперь распакуем архивы:

```

msv_12@ubuntuserverforpractic:~/opensearch-msv$ unzip -P infected_20230213 2023-02-13-IcedID-traffic-carved-and-sanitized.pcap.zip
unzip -P infected_20230223 2023-02-23-example-of-IcedID-from-URL-file-with-WebDAV-traffic.pcap.zip
unzip -P infected_20230227 2023-02-27-Qakbot-infection-traffic.pcap.zip
Archive: 2023-02-13-IcedID-traffic-carved-and-sanitized.pcap.zip
  inflating: 2023-02-13-IcedID-traffic-carved-and-sanitized.pcap
Archive: 2023-02-23-example-of-IcedID-from-URL-file-with-WebDAV-traffic.pcap.zip
  inflating: 2023-02-23-example-of-IcedID-from-URL-file-with-WebDAV-traffic.pcap
Archive: 2023-02-27-Qakbot-infection-traffic.pcap.zip
  inflating: 2023-02-27-Qakbot-infection-traffic.pcap
msv_12@ubuntuserverforpractic:~/opensearch-msv$ ls -la *.pcap
-rw-r--r-- 1 msv_12 msv_12 5112540 фев 13 2023 2023-02-13-IcedID-traffic-carved-and-sanitized.pcap
-rw-r--r-- 1 msv_12 msv_12 2947526 фев 23 2023 2023-02-23-example-of-IcedID-from-URL-file-with-WebDAV-traffic.pcap
-rw-r--r-- 1 msv_12 msv_12 19141869 фев 28 2023 2023-02-27-Qakbot-infection-traffic.pcap
msv_12@ubuntuserverforpractic:~/opensearch-msv$ █
```

14:32 06.11.2025 █

9. Обработка PCAP-файлов с помощью TShark

9.1. Первый файл

```
msv_12@ubuntuserverforpractic:~/opensearch-msv$ sudo tshark -r 2023-02-13-IcedID-traffic-carved-and-sanitized.pcap \
-Y "http.host or tls.handshake.extensions_server_name or dnsqry.name" \
-T fields \
-e frame.time_epoch \
-e ip.src \
-e ip.dst \
-e tcp.srcport \
-e tcp.dstport \
-e udp.srcport \
-e udp.dstport \
-e http.host \
-e tls.handshake.extensions_server_name \
-e frame.protocols \
-e frame.len \
-e http.request.method \
-e http.response.code \
-e dnsqry.name \
-e tcp.flags \
-E header=n -E separator=; -E aggregator=, > result_msv.csv
Running as user "root" and group "root". This could be dangerous.
msv_12@ubuntuserverforpractic:~/opensearch-msv$
```

14:37 06.11.2025 [27]

9.2. Второй файл

```
msv_12@ubuntuserverforpractic:~/opensearch-msv$ sudo tshark -r 2023-02-23-example-of-IcedID-from-URL-file-with-WebDAV-traffic.pcap \
-Y "http.host or tls.handshake.extensions_server_name or dnsqry.name" \
-T fields \
-e frame.time_epoch \
-e ip.src \
-e ip.dst \
-e tcp.srcport \
-e tcp.dstport \
-e udp.srcport \
-e udp.dstport \
-e http.host \
-e tls.handshake.extensions_server_name \
-e frame.protocols \
-e frame.len \
-e http.request.method \
-e http.response.code \
-e dnsqry.name \
-e tcp.flags \
-E header=n -E separator=; -E aggregator=, >> result_msv.csv
Running as user "root" and group "root". This could be dangerous.
msv_12@ubuntuserverforpractic:~/opensearch-msv$
```

14:38 06.11.2025 [27]

9.3. Третий файл

```
msv_12@ubuntuserverforpractic:~/opensearch-msv$ sudo tshark -r 2023-02-27-Qakbot-infection-traffic.pcap \
-Y "http.host or tls.handshake.extensions_server_name or dnsqry.name" \
-T fields \
-e frame.time_epoch \
-e ip.src \
-e ip.dst \
-e tcp.srcport \
-e tcp.dstport \
-e udp.srcport \
-e udp.dstport \
-e http.host \
-e tls.handshake.extensions_server_name \
-e frame.protocols \
-e frame.len \
-e http.request.method \
-e http.response.code \
-e dnsqry.name \
-e tcp.flags \
-E header=n -E separator=; -E aggregator=, >> result_msv.csv
Running as user "root" and group "root". This could be dangerous.
** (tshark:10924) 11:38:45.606694 [Epan WARNING] -- Dissector bug, protocol CLDAP, in packet 2289: ./epan/dissectors/packet-ldap.c:2180: failed assertion "recursion_depth <= 100"
** (tshark:10924) 11:38:45.607356 [Epan WARNING] -- Dissector bug, protocol CLDAP, in packet 2293: ./epan/dissectors/packet-ldap.c:2180: failed assertion "recursion_depth <= 100"
** (tshark:10924) 11:38:45.624502 [Epan WARNING] -- Dissector bug, protocol CLDAP, in packet 2865: ./epan/dissectors/packet-ldap.c:2180: failed assertion "recursion_depth <= 100"
```

Обоснование по каждому дополнительно выбранному полю:

1. http.request.method:

Позволяет определить тип выполняемого HTTP-запроса (GET, POST, PROPFIND и др.). Помогает выявить подозрительную активность, например, использование методов WebDAV (PROPFIND, PUT) или массовые автоматизированные GET-запросы, характерные для сканирования и C2-трафика.

2. http.response.code:

Отражает результат обработки запроса сервером (200, 404, 500 и др.). Позволяет оценить успешность выполнения операций и обнаружить ошибки, связанные с атаками или сканированием. Анализ сочетания с методом запроса помогает понять контекст действий (например, POST + 200 — возможная передача данных).

3. dnsqry.name:

Показывает доменные имена, к которым выполняются обращения. Используется для выявления вредоносных доменов, DGA-активности и аномальных запросов. Помогает сопоставить IP-адреса с доменами и анализировать сетевое взаимодействие на уровне имён.

4. ssh.protocol:

Содержит информацию о версии и типе SSH-протокола. Позволяет отслеживать активность удалённого доступа, выявлять несанкционированные подключения или попытки подбора паролей, а также использование устаревших версий SSH.

5. ftp.request.command:

Отражает команды FTP (USER, PASS, STOR, RETR и др.). Полезно для анализа передачи файлов, обнаружения попыток эксфильтрации данных или брутфорса. Позволяет отследить загрузку или выгрузку подозрительных файлов.

10. Загрузка данных используя Python скрипт.

Используемый Python скрипт:

https://github.com/l1ratch/WC_BISO/blob/main/5_sem/TXbCK/practic/pr_5/uto.py

```
(venv) msv_12@ubuntuserverforpractic:~/opensearch-msv$ python uto.py
2025-11-07 07:54:28,003 - INFO - HEAD http://localhost:9212/ [status:200 request:0.076s]
2025-11-07 07:54:28,003 - INFO - Успешное подключение к OpenSearch
2025-11-07 07:54:28,356 - INFO - PUT http://localhost:9212/_template/packets_msv [status:200 request:0.353s]
2025-11-07 07:54:28,357 - INFO - Шаблон индекса 'packets_msv' успешно создан
2025-11-07 07:54:28,357 - INFO - Чтение файла result_msv.csv
2025-11-07 07:54:29,340 - INFO - POST http://localhost:9212/_bulk?refresh=true [status:200 request:0.942s]
2025-11-07 07:54:29,343 - INFO - Всего загружено 761 документов в индекс packets-msv
2025-11-07 07:54:29,343 - INFO - Данные успешно загружены в OpenSearch
2025-11-07 07:54:29,383 - INFO - POST http://localhost:9212/packets-msv/_count [status:200 request:0.038s]
2025-11-07 07:54:29,384 - INFO - В индексе packets-msv теперь 761 документов
(venv) msv_12@ubuntuserverforpractic:~/opensearch-msv$ █
```

11. Запуск панели, подготовка OpenSearchDashboards.

The screenshot shows the 'Index patterns' section of the OpenSearch Dashboards interface. The top navigation bar includes 'Dashboards Ma...', 'Index patterns' (which is highlighted in green), and a user icon. On the left, there's a sidebar with 'Dashboards Management' and a collapsed menu showing 'patterns', 'sources', 'objects', and 'seed settings'. The main content area has a title 'Index patterns' and a sub-instruction 'Create and manage the index patterns that help you retrieve your data from OpenSearch.' Below this is a search bar with a magnifying glass icon and the placeholder 'Search...'. A table lists an index pattern named 'packets-msv*' under the 'Pattern' column, with 'Default' under 'Data Source Connection'. At the bottom, there's a 'Rows per page: 10' dropdown and a navigation bar with icons for back, forward, and search.

OpenSearch Dashboards

Discover

Selected fields

Available fields

Selected fields

Search

Filter by type 0

DQL Refresh

Results (500/761) Download as CSV

_source

> _frame_time_epoch: 1,676,385,992,536 _ip_src: 10.2.13.181 _ip_dst: 10.2.13.1 _tcp_srcport: - _tcp_dstport: - _udp_srcport: 61,841 _udp_dstport: 53 _http_host: - _tls_handshake_extensions_server_name: - _frame_protocols: eth:ethertype:ip:udp:dns _frame_len: 79 _http_request_method: - _http_response_code: - _dns_qry_name: microsoftteamus.top _tcp_flags: - _timestamp: 2023-02-13 16:33:12.536934107 _id: XMBPZoBb_53JuwSTWd _type: - _index: packets-msv _score: 0

> _frame_time_epoch: 1,676,385,992,887 _ip_src: 10.2.13.1 _ip_dst: 10.2.13.101 _tcp_srcport: - _tcp_dstport: - _udp_srcport: 53 _udp_dstport: 61,841 _http_host: - _tls_handshake_extensions_server_name: - _frame_protocols: eth:ethertype:ip:udp:dns _frame_len: 249 _http_request_method: - _http_response_code: - _dns_qry_name: microsoftteamus.top _tcp_flags: - _timestamp: 2023-02-13 16:33:12.887197018 _id: XMBPZoBb_53JuwSTWd _type: - _index: packets-msv _score: 0

> _frame_time_epoch: 1,676,385,993,094 _ip_src: 10.2.13.181 _ip_dst: 85.193.93.125 _tcp_srcport: 49,812 _tcp_dstport: 88 _udp_srcport: - _udp_dstport: - _http_host: microsoftteamus.top _tls_handshake_extensions_server_name: - _frame_protocols: eth:ethertype:ip:tcp:http _frame_len: 828 _http_request_method: GET _http_response_code: - _dns_qry_name: - _tcp_flags: @x0818 _timestamp: 2023-02-13 16:33:13.088339293 _id: YGBPZoBb_53JuwSTWd _type: - _index: packets-msv _score: 0

> _frame_time_epoch: 1,676,385,996,826 _ip_src: 10.2.13.101 _ip_dst: 85.193.93.125 _tcp_srcport: 49,814 _tcp_dstport: 88 _udp_srcport: - _udp_dstport: - _http_host: microsoftteamus.top _tls_handshake_extensions_server_name: - _frame_protocols: eth:ethertype:ip:tcp:http _frame_len: 813 _http_request_method: GET _http_response_code: - _dns_qry_name: - _tcp_flags: @x0818 _timestamp: 2023-02-13 16:33:16.826119008 _id: YM8PZoBb_53JuwSTWd _type: - _index: packets-msv _score: 0

> _frame_time_epoch: 1,676,385,996,832 _ip_src: 10.2.13.101 _ip_dst: 85.193.93.125 _tcp_srcport: 49,815 _tcp_dstport: 88 _udp_srcport: - _udp_dstport: - _http_host: microsoftteamus.top _tls_handshake_extensions_server_name: - _frame_protocols: eth:ethertype:ip:tcp:http _frame_len: 828 _http_request_method: GET _http_response_code: - _dns_qry_name: - _tcp_flags: @x0818 _timestamp: 2023-02-13 16:33:16.831859951 _id: YM8PZoBb_53JuwSTWd _type: - _index: packets-msv _score: 0

> _frame_time_epoch: 1,676,385,996,833 _ip_src: 10.2.13.181 _ip_dst: 85.193.93.125 _tcp_srcport: 49,816 _tcp_dstport: 88 _udp_srcport: - _udp_dstport: - _http_host: microsoftteamus.top _tls_handshake_extensions_server_name: - _frame_protocols: eth:ethertype:ip:tcp:http _frame_len: 767 _http_request_method: GET _http_response_code: - _dns_qry_name: - _tcp_flags: @x0818 _timestamp: 2023-02-13 16:33:16.832787837 _id: YGBPZoBb_53JuwSTWd _type: - _index: packets-msv _score: 0

> _frame_time_epoch: 1,676,385,997,336 _ip_src: 10.2.13.181 _ip_dst: 85.193.93.125 _tcp_srcport: 49,821 _tcp_dstport: 88 _udp_srcport: - _udp_dstport: - _http_host: microsoftteamus.top _tls_handshake_extensions_server_name: - _frame_protocols: eth:ethertype:ip:tcp:http _frame_len: 812 _http_request_method: GET _http_response_code: - _dns_qry_name: - _tcp_flags: @x0818 _timestamp: 2023-02-13 16:33:17.335551923 _id: ZGBPZoBb_53JuwSTWd _type: - _index: packets-msv _score: 0

> _frame_time_epoch: 1,676,385,997,894 _ip_src: 10.2.13.181 _ip_dst: 85.193.93.125 _tcp_srcport: 49,822 _tcp_dstport: 88 _udp_srcport: - _udp_dstport: - _http_host: microsoftteamus.top _tls_handshake_extensions_server_name: - _frame_protocols: eth:ethertype:ip:tcp:http _frame_len: 812 _http_request_method: GET _http_response_code: - _dns_qry_name: - _tcp_flags: @x0818 _timestamp: 2023-02-13 16:33:17.897797884 _id: 7MBPZoBb_53JuwSTWd _type: - _index: packets-msv _score: 0

12. Выполним поиск в разделе Discover.

Results (10/10) Download as CSV

`_source`

```
> [frame_time_epoch] 1,676,305,992.536 [ip_src] 10.2.13.101 [ip_dst] 10.2.13.1 [tcp_srcport] - [tcp_dstport] - [udp_srcport] 61,841 [udp_dstport] 53 [http_host] - [tls_handshake_extensions_server_name] - [frame_protocols] eth:ether type:ip:udp:dns [frame_len: 79 http.request.method: - http.response.code: - dnsqry.name: microsoftteamsus.top [tcp_flags: - timestamp: 2023-02-13 16:33:12.536634107 _id: XMBPXZoBb_53JuwfSTMc _type: - _index: packets-msv _score: 0]
```

`Expanded document`

Table JSON

```
{
  "_id": "XMBPXZoBb_53JuwfSTMc",
  "_index": "packets-msv",
  "_score": 0,
  "_type": "-",
  "dnsqry.name": "microsoftteamsus.top",
  "frame_len": 79,
  "frame_protocols": "eth:ether type:ip:udp:dns",
  "frame_time_epoch": 1,676,305,992.536,
  "http.host": "-",
  "http.request.method": "-",
  "http.response.code": "-",
  "ip.dst": "10.2.13.101",
  "ip.src": "10.2.13.101",
  "tcp.dstport": "-",
  "tcp.flags": "-",
  "tcp.srcport": "-",
  "timestamp": "2023-02-13 16:33:12.536634107",
  "tls.handshake_extensions_server_name": "-",
  "udp.dstport": "53",
  "udp.srcport": "61,841",
  "http.host": "-",
  "tls.handshake_extensions_server_name": "-",
  "frame_protocols": "eth:ether type:ip:udp:dns"
}
```

View single document

Попробовал функцию поиска, выполнил поисковый запрос по одному из найденных доменов microsoftteamsus.top. Запросы используют метод GET.

Results (16/16) Download as CSV

`_source`

```
> [frame_time_epoch] 1,676,305,993.094 [ip_src] 10.2.13.101 [ip_dst] 85.193.93.125 [tcp_srcport] 49,812 [tcp_dstport] 88 [udp_srcport] - [udp_dstport] - [http_host] microsoftteamsus.top [tls_handshake_extensions_server_name] - [frame_protocols] eth:ether type:ip:tcp:http [frame_len: 828 http.request.method: GET http.response.code: - dnsqry.name: - tcp_flag: #x0018 [timestamp: 2023-02-13 16:33:13.093633293 _id: YGPXZoBb_53JuwfSTMc _type: - _index: packets-msv _score: 0]
```

```
> [frame_time_epoch] 1,676,305,996.026 [ip_src] 10.2.13.101 [ip_dst] 85.193.93.125 [tcp_srcport] 49,814 [tcp_dstport] 88 [udp_srcport] - [udp_dstport] - [http_host] microsoftteamsus.top [tls_handshake_extensions_server_name] - [frame_protocols] eth:ether type:ip:tcp:http [frame_len: 813 http.request.method: GET http.response.code: - dnsqry.name: - tcp_flag: #x0018 [timestamp: 2023-02-13 16:33:16.826115998 _id: YGPXZoBb_53JuwfSTMc _type: - _index: packets-msv _score: 0]
```

```
> [frame_time_epoch] 1,676,305,996.032 [ip_src] 10.2.13.101 [ip_dst] 85.193.93.125 [tcp_srcport] 49,815 [tcp_dstport] 88 [udp_srcport] - [udp_dstport] - [http_host] microsoftteamsus.top [tls_handshake_extensions_server_name] - [frame_protocols] eth:ether type:ip:tcp:http [frame_len: 820 http.request.method: GET http.response.code: - dnsqry.name: - tcp_flag: #x0018 [timestamp: 2023-02-13 16:33:16.83199951 _id: YGPXZoBb_53JuwfSTMc _type: - _index: packets-msv _score: 0]
```

```
> [frame_time_epoch] 1,676,305,996.033 [ip_src] 10.2.13.101 [ip_dst] 85.193.93.125 [tcp_srcport] 49,816 [tcp_dstport] 88 [udp_srcport] - [udp_dstport] - [http_host] microsoftteamsus.top [tls_handshake_extensions_server_name] - [frame_protocols] eth:ether type:ip:tcp:http [frame_len: 767 http.request.method: GET http.response.code: - dnsqry.name: - tcp_flag: #x0018 [timestamp: 2023-02-13 16:33:16.832787037 _id: YGPXZoBb_53JuwfSTMc _type: - _index: packets-msv _score: 0]
```

```
> [frame_time_epoch] 1,676,305,997.316 [ip_src] 10.2.13.101 [ip_dst] 85.193.93.125 [tcp_srcport] 49,821 [tcp_dstport] 88 [udp_srcport] - [udp_dstport] - [http_host] microsoftteamsus.top [tls_handshake_extensions_server_name] - [frame_protocols] eth:ether type:ip:tcp:http [frame_len: 812 http.request.method: GET http.response.code: - dnsqry.name: - tcp_flag: #x0018 [timestamp: 2023-02-13 16:33:17.33551023 _id: ZGPXZoBb_53JuwfSTMc _type: - _index: packets-msv _score: 0]
```

```
> [frame_time_epoch] 1,676,305,997.894 [ip_src] 10.2.13.101 [ip_dst] 85.193.93.125 [tcp_srcport] 49,822 [tcp_dstport] 88 [udp_srcport] - [udp_dstport] - [http_host] microsoftteamsus.top [tls.handshake_extensions_server_name] - [frame_protocols] eth:ether type:ip:tcp:http [frame_len: 812 http.request.method: GET http.response.code: - dnsqry.name: - tcp_flag: #x0018 [timestamp: 2023-02-13 16:33:17.83782384 _id: ZGPXZoBb_53JuwfSTMc _type: - _index: packets-msv _score: 0]
```

```
> [frame_time_epoch] 1,676,306,006.4 [ip_src] 10.2.13.101 [ip_dst] 85.193.93.125 [tcp_srcport] 49,823 [tcp_dstport] 88 [udp_srcport] - [udp_dstport] - [http_host] microsoftteamsus.top [tls.handshake_extensions_server_name] - [frame_protocols] eth:ether type:ip:tcp:http [frame_len: 778 http.request.method: GET http.response.code: - dnsqry.name: - tcp_flag: #x0018 [timestamp: 2023-02-13 16:33:26.409116968 _id: ZGPXZoBb_53JuwfSTMc _type: - _index: packets-msv _score: 0]
```

```
> [frame_time_epoch] 1,676,306,006.4 [ip_src] 10.2.13.101 [ip_dst] 85.193.93.125 [tcp_srcport] 49,824 [tcp_dstport] 88 [udp_srcport] - [udp_dstport] - [http_host] microsoftteamsus.top [tls.handshake_extensions_server_name] - [frame_protocols] eth:ether type:ip:tcp:http [frame_len: 774 http.request.method: GET http.response.code: - dnsqry.name: - tcp_flag: #x0018 [timestamp: 2023-02-13 16:33:26.409232184 _id: ZGPXZoBb_53JuwfSTMc _type: - _index: packets-msv _score: 0]
```

```
> [frame_time_epoch] 1,676,306,008.781 [ip_src] 10.2.13.101 [ip_dst] 45.61.139.138 [tcp_srcport] 49,863 [tcp_dstport] 88 [udp_srcport] - [udp_dstport] - [http_host] alishabreindeer.com [tls.handshake_extensions_server_name] - [frame_protocols] eth:ether type:ip:tcp:http [frame_len: 368 http.request.method: GET http.response.code: - dnsqry.name: - tcp_flag: #x0018 [timestamp: 2023-02-13 16:38:28.798733026 _id: 3GPXZoBb_53JuwfSTMc _type: - _index: packets-msv _score: 0]
```

```
> [frame_time_epoch] 1,677,169,248.552 [ip_src] 10.24.8.189 [ip_dst] 104.156.149.6 [tcp_srcport] 58,655 [tcp_dstport] 88 [udp_srcport] - [udp_dstport] - [http_host] 104.156.149.6 [tls.handshake_extensions_server_name] - [frame_protocols] eth:ether type:ip:tcp:http [frame_len: 244 http.request.method: GET http.response.code: - dnsqry.name: - tcp_flag: #x0018 [timestamp: 2023-02-23 16:26:48.551176952 _id: 4GPXZoBb_53JuwfSTMc _type: - _index: packets-msv _score: 0]
```

`Expanded document`

Table JSON

```
{
  "_id": "4GPXZoBb_53JuwfSTMc",
  "_index": "packets-msv",
  "_score": 0,
  "_type": "-",
  "dnsqry.name": "-",
  "frame_len": 244,
  "frame_protocols": "eth:ether type:ip:tcp:http",
  "frame_time_epoch": 1,677,169,248.552,
  "http.host": "104.156.149.6",
  "http.request.method": "GET",
  "http.response.code": "-",
  "ip.dst": "104.156.149.6"
}
```

Results (11/11) Download as CSV										
Source		Destination								
Frame	Time	Epoch	IP Src	Port Src	IP Dst	Port Dst	Protocol	Length	Method	Score
> [frame_time_epoch]_1,677,169,246,074 [ip_src]_18.24.8.189 [ip_dst]_184.156.149.6 [tcp_srcport]_50,052 [tcp_dstport]_88 [udp_srcport] - [udp_dstport] - [http_host]_184.156.149.6 [tls_handshake_extensions_server_name] - [frame_protocols]_eth:ethertype:ip:tcp:http [frame_len]_222 [http_request_method]_PR	[http_response_code] - [dns_qry_name] - [tcp_flags]_0x0010 [timestamp]_2023-02-23 16:20:46.874182893 [id]_4WPXZ0Bz_533wFtMw [type] - [index]_packets-mv [score]_0									
> [frame_time_epoch]_1,677,169,246,076 [ip_src]_18.24.8.189 [ip_dst]_184.156.149.6 [tcp_srcport]_50,052 [tcp_dstport]_88 [udp_srcport] - [udp_dstport] - [http_host]_184.156.149.6 [tls_handshake_extensions_server_name] - [frame_protocols]_eth:ethertype:ip:tcp:http [frame_len]_223 [http_request_method]_PR	[http_response_code] - [dns_qry_name] - [tcp_flags]_0x0010 [timestamp]_2023-02-23 16:20:46.896111963 [id]_4WPXZ0Bz_533wFtMw [type] - [index]_packets-mv [score]_0									
> [frame_time_epoch]_1,677,169,246,939 [ip_src]_18.24.8.189 [ip_dst]_184.156.149.6 [tcp_srcport]_50,052 [tcp_dstport]_88 [udp_srcport] - [udp_dstport] - [http_host]_184.156.149.6 [tls_handshake_extensions_server_name] - [frame_protocols]_eth:ethertype:ip:tcp:http [frame_len]_225 [http_request_method]_PR	[http_response_code] - [dns_qry_name] - [tcp_flags]_0x0010 [timestamp]_2023-02-23 16:20:46.938873053 [id]_4WPXZ0Bz_533wFtMw [type] - [index]_packets-mv [score]_0									
> [frame_time_epoch]_1,677,169,246,943 [ip_src]_18.24.8.189 [ip_dst]_184.156.149.6 [tcp_srcport]_50,054 [tcp_dstport]_88 [udp_srcport] - [udp_dstport] - [http_host]_184.156.149.6 [tls_handshake_extensions_server_name] - [frame_protocols]_eth:ethertype:ip:tcp:http [frame_len]_225 [http_request_method]_PR	[http_response_code] - [dns_qry_name] - [tcp_flags]_0x0010 [timestamp]_2023-02-23 16:20:46.942679114 [id]_4WPXZ0Bz_533wFtMw [type] - [index]_packets-mv [score]_0									
> [frame_time_epoch]_1,677,169,246,952 [ip_src]_18.24.8.189 [ip_dst]_184.156.149.6 [tcp_srcport]_50,053 [tcp_dstport]_88 [udp_srcport] - [udp_dstport] - [http_host]_184.156.149.6 [tls_handshake_extensions_server_name] - [frame_protocols]_eth:ethertype:ip:tcp:http [frame_len]_244 [http_request_method]_GE	[http_response_code] - [dns_qry_name] - [tcp_flags]_0x0010 [timestamp]_2023-02-23 16:20:46.951785934 [id]_4WPXZ0Bz_533wFtMw [type] - [index]_packets-mv [score]_0									
> [frame_time_epoch]_1,677,169,250,332 [ip_src]_18.24.8.189 [ip_dst]_184.156.149.6 [tcp_srcport]_50,055 [tcp_dstport]_88 [udp_srcport] - [udp_dstport] - [http_host]_184.156.149.6 [tls_handshake_extensions_server_name] - [frame_protocols]_eth:ethertype:ip:tcp:http [frame_len]_248 [http_request_method]_PR	[http_response_code] - [dns_qry_name] - [tcp_flags]_0x0010 [timestamp]_2023-02-23 16:20:46.953199904 [id]_4WPXZ0Bz_533wFtMw [type] - [index]_packets-mv [score]_0									
> [frame_time_epoch]_1,677,169,250,432 [ip_src]_18.24.8.189 [ip_dst]_184.156.149.6 [tcp_srcport]_50,057 [tcp_dstport]_88 [udp_srcport] - [udp_dstport] - [http_host]_184.156.149.6 [tls_handshake_extensions_server_name] - [frame_protocols]_eth:ethertype:ip:tcp:http [frame_len]_231 [http_request_method]_PR	[http_response_code] - [dns_qry_name] - [tcp_flags]_0x0010 [timestamp]_2023-02-23 16:20:46.95423263997 [id]_4WPXZ0Bz_533wFtMw [type] - [index]_packets-mv [score]_0									
> [frame_time_epoch]_1,677,169,250,442 [ip_src]_18.24.8.189 [ip_dst]_184.156.149.6 [tcp_srcport]_50,057 [tcp_dstport]_88 [udp_srcport] - [udp_dstport] - [http_host]_184.156.149.6 [tls_handshake_extensions_server_name] - [frame_protocols]_eth:ethertype:ip:tcp:http [frame_len]_248 [http_request_method]_GE	[http_response_code] - [dns_qry_name] - [tcp_flags]_0x0010 [timestamp]_2023-02-23 16:20:46.954477685 [id]_4WPXZ0Bz_533wFtMw [type] - [index]_packets-mv [score]_0									
> [frame_time_epoch]_1,677,169,250,509 [ip_src]_18.24.8.189 [ip_dst]_184.156.149.6 [tcp_srcport]_50,060 [tcp_dstport]_88 [udp_srcport] - [udp_dstport] - [http_host]_184.156.149.6 [tls_handshake_extensions_server_name] - [frame_protocols]_eth:ethertype:ip:tcp:http [frame_len]_244 [http_request_method]_PR	[http_response_code] - [dns_qry_name] - [tcp_flags]_0x0010 [timestamp]_2023-02-23 16:20:46.956944854 [id]_4WPXZ0Bz_533wFtMw [type] - [index]_packets-mv [score]_0									
> [frame_time_epoch]_1,677,169,250,613 [ip_src]_18.24.8.189 [ip_dst]_184.156.149.6 [tcp_srcport]_50,061 [tcp_dstport]_88 [udp_srcport] - [udp_dstport] - [http_host]_184.156.149.6 [tls_handshake_extensions_server_name] - [frame_protocols]_eth:ethertype:ip:tcp:http [frame_len]_244 [http_request_method]_PR	[http_response_code] - [dns_qry_name] - [tcp_flags]_0x0010 [timestamp]_2023-02-23 16:20:46.956115668 [id]_4WPXZ0Bz_533wFtMw [type] - [index]_packets-mv [score]_0									
> [frame_time_epoch]_1,677,169,250,655 [ip_src]_18.24.8.189 [ip_dst]_184.156.149.6 [tcp_srcport]_50,063 [tcp_dstport]_88 [udp_srcport] - [udp_dstport] - [http_host]_184.156.149.6 [tls_handshake_extensions_server_name] - [frame_protocols]_eth:ethertype:ip:tcp:http [frame_len]_246 [http_request_method]_PR	[http_response_code] - [dns_qry_name] - [tcp_flags]_0x0010 [timestamp]_2023-02-23 16:20:46.956503118 [id]_4WPXZ0Bz_533wFtMw [type] - [index]_packets-mv [score]_0									

Решил изучить все GET запросы. Нашел запросы от http хоста 104.156.149.6. Изучив вывод поиска по хосту заметил, что все выполненные им запросы практически идентичны и используют метод GET, предполагаю, что это скрипт. Выполню поиск по ip-источнику этих запросов(10.24.8.189) исключив GET запросы:

Здесь в основном запросы на порты 443 и 53. Предполагаю, что это хаб или другое устройство организующее устройства в сети, возможно устройства на котором расположен dns сервер.

renomesolar.com

Add filter

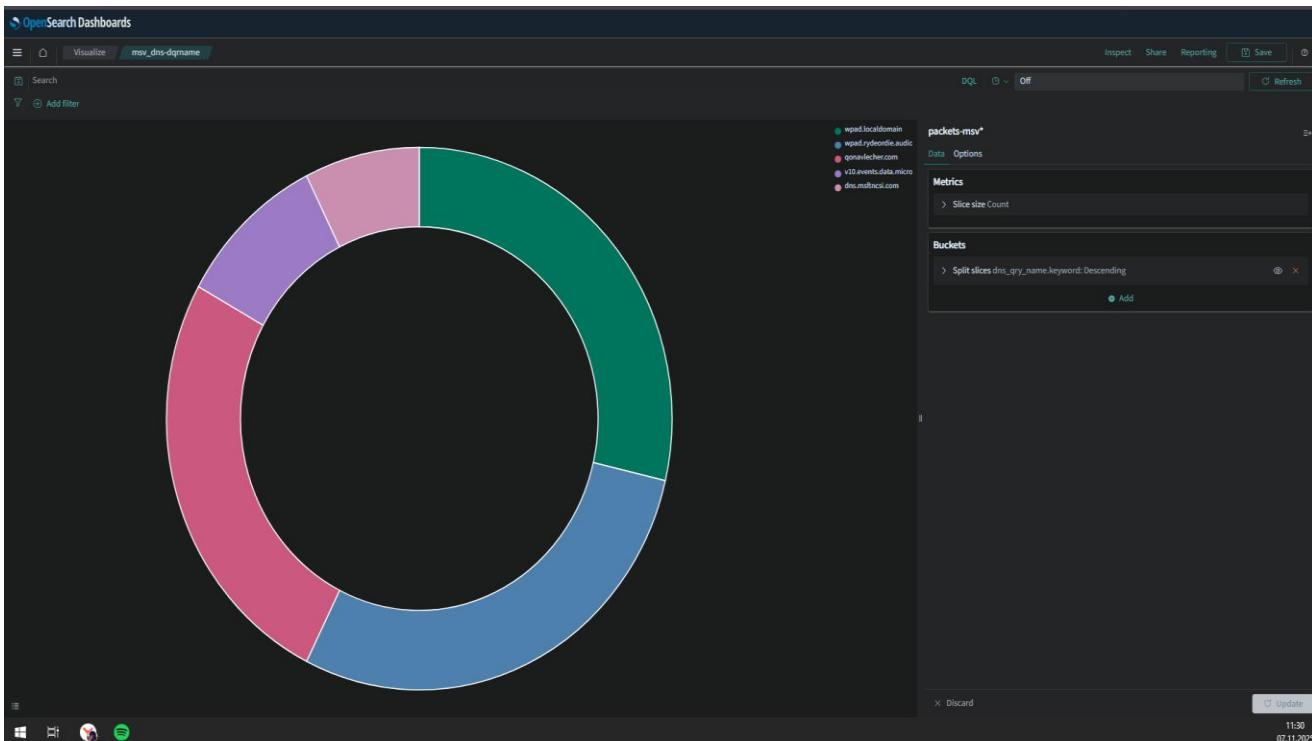
Results (8/8) Download as CSV

```
_source
> [frame_time_epoch]:1,677,169,314,231 [ip_src]:10.24.8.189 [ip_dst]:10.24.8.8 [tcp_srcport]:53 [tcp_dstport]:53 [udp_srcport]:53 [udp_dstport]:53 [http_host]: - [tls_handshake_extensions_server_name]: - [frame_protocol]:eth:ethertype:ip:udp:dns [frame_len]:28 [http_request_method]: - [http_response_code]: - [dnsqryname]:renomesolar.com [tcp_flags]: - [timestamp]:2023-02-23 16:21:54.13116898 [_id]:728PZobB_53uwsfMe [_type]: - [index]:packets-msv [_score]:0
> [frame_time_epoch]:1,677,169,314,245 [ip_src]:10.24.8.189 [ip_dst]:10.24.8.8 [tcp_srcport]:53 [tcp_dstport]:53 [udp_srcport]:53 [udp_dstport]:53 [http_host]: - [tls_handshake_extensions_server_name]: - [frame_protocol]:eth:ethertype:ip:udp:dns [frame_len]:28 [http_request_method]: - [http_response_code]: - [dnsqryname]:renomesolar.com [tcp_flags]: - [timestamp]:2023-02-23 16:21:54.16253998 [_id]:728PZobB_53uwsfMe [_type]: - [index]:packets-msv [_score]:0
> [frame_time_epoch]:1,677,169,314,292 [ip_src]:10.24.8.189 [ip_dst]:38.180.0.89 [tcp_srcport]:53 [tcp_dstport]:443 [udp_srcport]: - [udp_dstport]: - [http_host]: - [tls_handshake_extensions_server_name]:renomesolar.com [frame_protocol]:eth:ethertype:ip:tcp:tls [frame_len]:236 [http_request_method]: - [http_response_code]: - [dnsqryname]: - [tcp_flags]:w+0x18 [timestamp]:2023-02-23 16:21:54.39158018 [_id]:728PZobB_53uwsfMe [_type]: - [index]:packets-msv [_score]:0
> [frame_time_epoch]:1,677,169,315,533 [ip_src]:10.24.8.189 [ip_dst]:38.180.0.89 [tcp_srcport]:53 [tcp_dstport]:443 [udp_srcport]:53 [udp_dstport]:53 [http_host]: - [tls_handshake_extensions_server_name]:renomesolar.com [frame_protocol]:eth:ethertype:ip:tcp:tls [frame_len]:236 [http_request_method]: - [http_response_code]: - [dnsqryname]: - [tcp_flags]:w+0x18 [timestamp]:2023-02-23 16:21:55.92188682 [_id]:728PZobB_53uwsfMe [_type]: - [index]:packets-msv [_score]:0
> [frame_time_epoch]:1,677,169,315,532 [ip_src]:10.24.8.189 [ip_dst]:38.180.0.89 [tcp_srcport]:53 [tcp_dstport]:443 [udp_srcport]:53 [udp_dstport]:53 [http_host]: - [tls_handshake_extensions_server_name]:renomesolar.com [frame_protocol]:eth:ethertype:ip:tcp:tls [frame_len]:236 [http_request_method]: - [http_response_code]: - [dnsqryname]: - [tcp_flags]:w+0x18 [timestamp]:2023-02-23 16:21:55.93387483 [_id]:728PZobB_53uwsfMe [_type]: - [index]:packets-msv [_score]:0
> [frame_time_epoch]:1,677,169,616,189 [ip_src]:10.24.8.189 [ip_dst]:38.180.0.89 [tcp_srcport]:53 [tcp_dstport]:443 [udp_srcport]:53 [udp_dstport]:53 [http_host]: - [tls_handshake_extensions_server_name]:renomesolar.com [frame_protocol]:eth:ethertype:ip:tcp:tls [frame_len]:236 [http_request_method]: - [http_response_code]: - [dnsqryname]: - [tcp_flags]:w+0x18 [timestamp]:2023-02-23 16:21:56.168749894 [_id]:728PZobB_53uwsfMe [_type]: - [index]:packets-msv [_score]:0
> [frame_time_epoch]:1,677,169,917,647 [ip_src]:10.24.8.189 [ip_dst]:38.180.0.89 [tcp_srcport]:53 [tcp_dstport]:443 [udp_srcport]:53 [udp_dstport]:53 [http_host]: - [tls_handshake_extensions_server_name]:renomesolar.com [frame_protocol]:eth:ethertype:ip:tcp:tls [frame_len]:236 [http_request_method]: - [http_response_code]: - [dnsqryname]: - [tcp_flags]:w+0x18 [timestamp]:2023-02-23 16:31:57.646892071 [_id]:728PZobB_53uwsfMe [_type]: - [index]:packets-msv [_score]:0
> [frame_time_epoch]:1,677,178,219,237 [ip_src]:10.24.8.189 [ip_dst]:38.180.0.89 [tcp_srcport]:53 [tcp_dstport]:443 [udp_srcport]:53 [udp_dstport]:53 [http_host]: - [tls_handshake_extensions_server_name]:renomesolar.com [frame_protocol]:eth:ethertype:ip:tcp:tls [frame_len]:236 [http_request_method]: - [http_response_code]: - [dnsqryname]: - [tcp_flags]:w+0x18 [timestamp]:2023-02-23 16:36:59.237163939 [_id]:728PZobB_53uwsfMe [_type]: - [index]:packets-msv [_score]:0
```

Нашел запросы к 38.180.0.89 по 443, связанные с renomesolar.com. Первые два запроса являются dns запросами. Сначала 10.24.8.189 отправил запрос 10.24.8.8 на 53 порт, затем получил ответ от 10.24.8.8 и начал отправлять запросы 38.180.0.89 на 443 порт. Хороший пример того как работает dns сервер. Можем сделать вывод, что 10.24.8.189 является одним из устройств в сети, а 10.24.8.8 является локальным dns сервером этой сети.

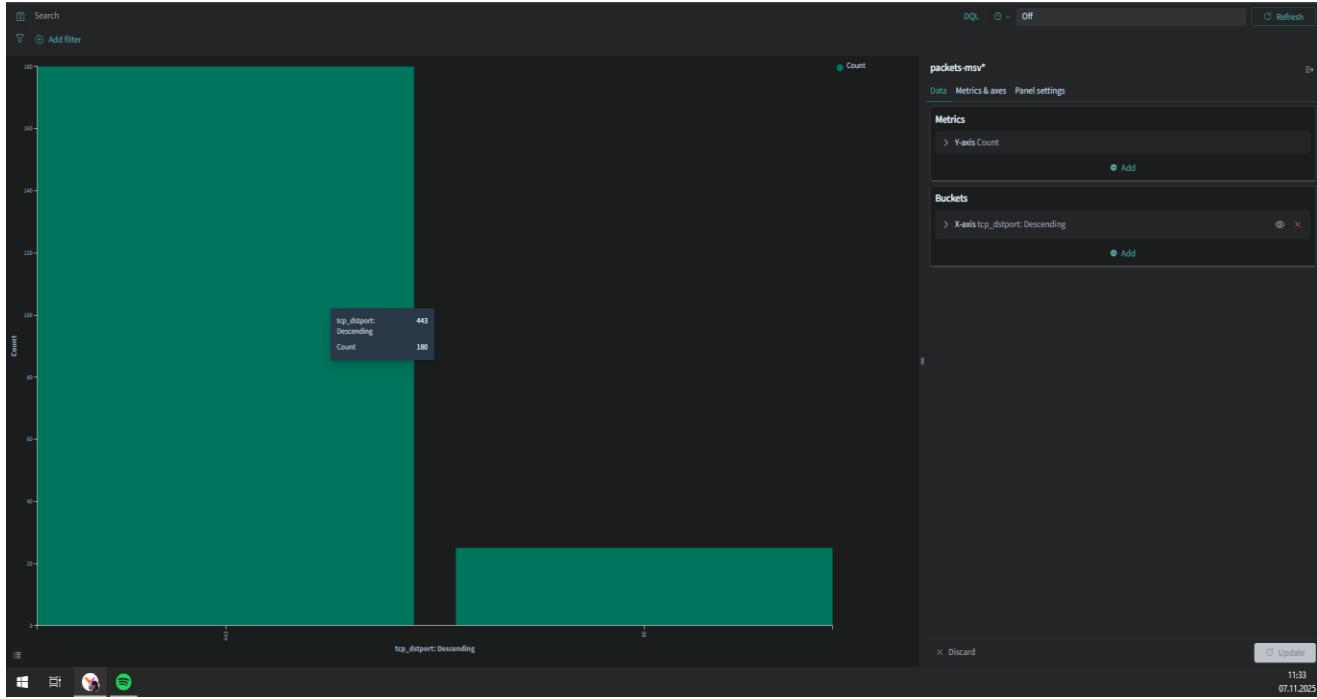
13. Создадим несколько визуализаций.

13.1. По полю dns_qry_name.keyword



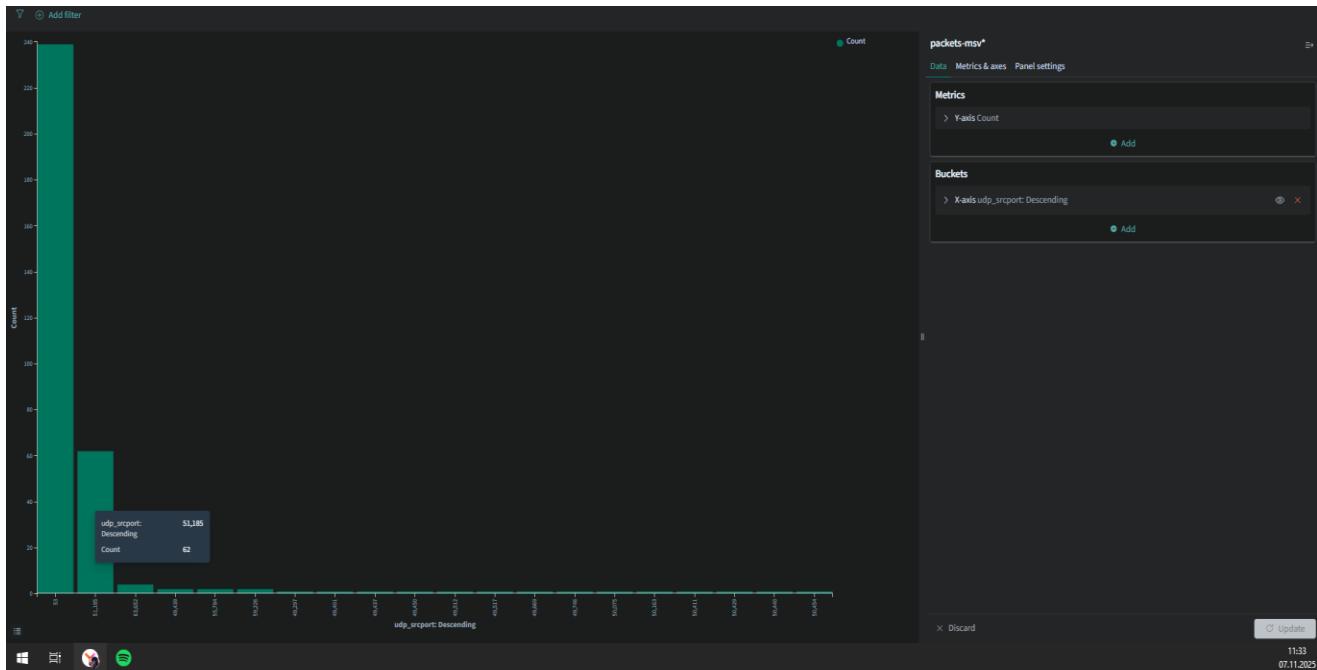
Чаще всего запросы шли к dns wpad.localdomain и wpab.rydeordie.audio – по 78 запросов. Чуть чаще к qonavlecher.com – по 70, и совсем редко к двум от компании Microsoft.

13.2. По полю tcp_dstport



На данной диаграмме видно, что наиболее часто используемым dst портом является 443(180 запросов) из чего можно сделать вывод что в основном все запросы были по защищенному протоколу, лишь 25 запросов относятся к 80 порту.

13.3. По полю udp_srcport

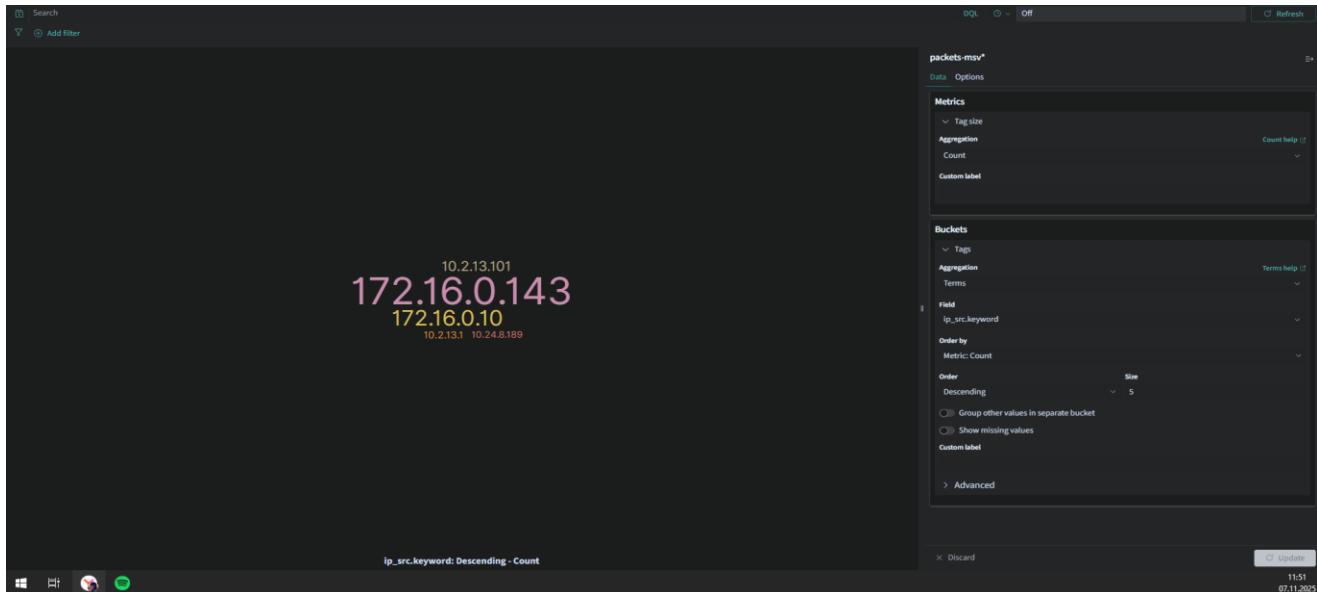


На данной диаграмме можно заметить, что самым часто используемым портом является

53 - порт который чаще всего используется для dns серверов(239 запросов), на втором месте 51185 порт у которого всего 62 запроса. Следом уже идут другие по 4, 2 и 1 запросам.

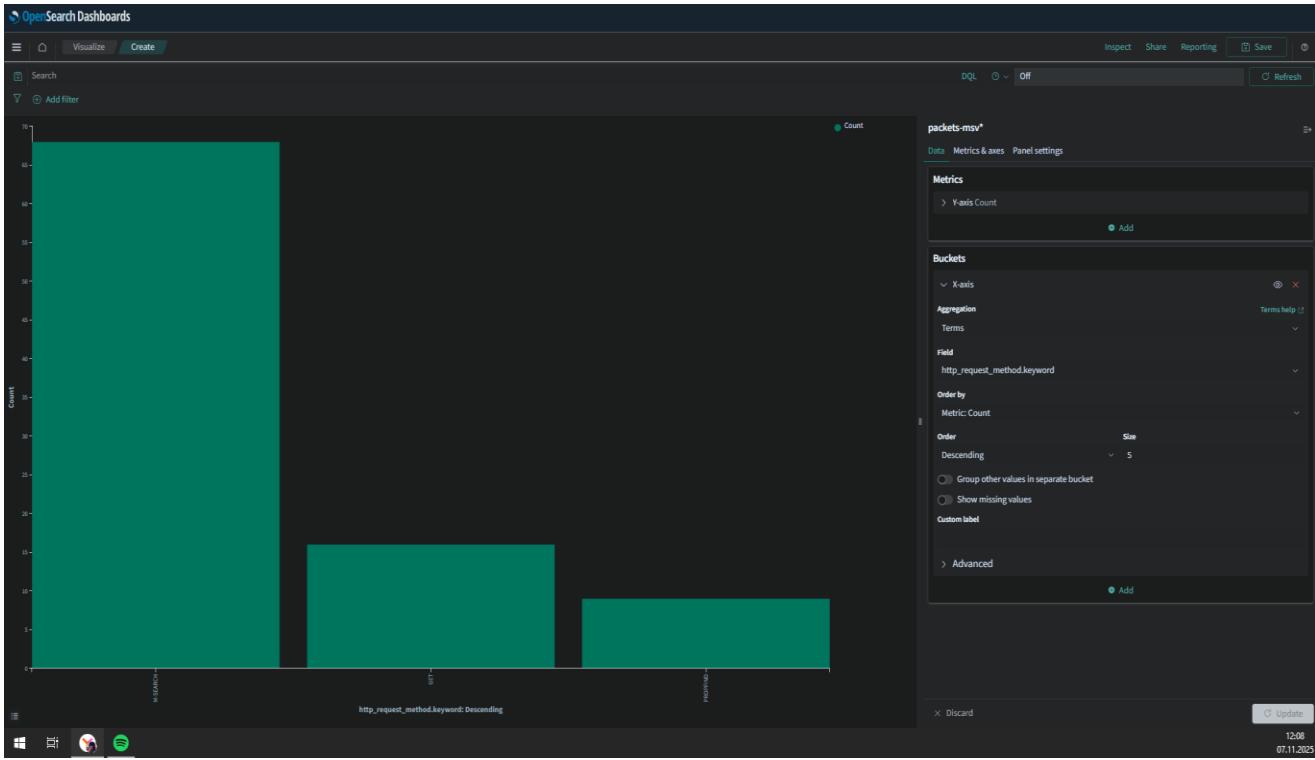
(По исследованным диаграммам можно сделать предположение, что на устройстве или в локальной сети устройства был запущен локальный DNS-сервер. Вероятно для отслеживания запросов.)

13.4. По полю ip_src



На это диаграмме мы видим вывод с сортировкой по частоте использования ip адреса источников запросов – локальные адреса с которых выполняются запросы. Наиболее часто используемым является 172.16.0.143 – который вероятно является одним из основных адресов устройства в его локальной сети.

13.5. По полю http_rewuest_method

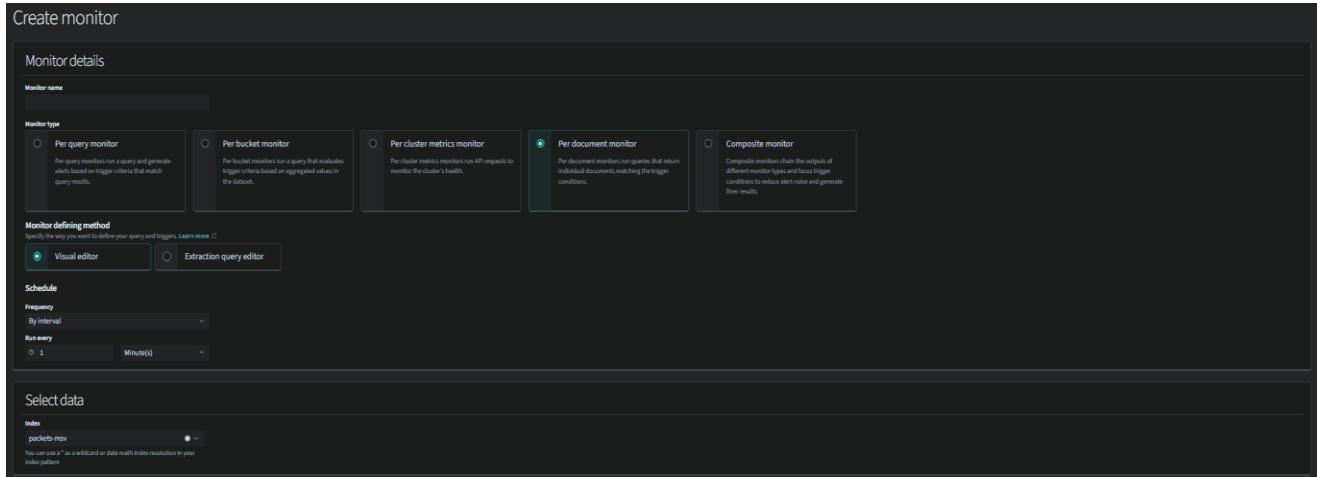


Здесь мы видим диаграмму по используемым методам http запросов. Наиболее часто используемым является метод M-SEARCH , который используется устройствами (например, Smart TV, медиаплеерами) для поиска других сервисов по сети – 68 запросов, Значительно меньшее количество стандартных запросов GET и совсем немного запросов PROPFIND (метод для работы с веб-ресурсами, как WebDAV) говорят о том, что обычный веб-трафик и управление файлами являются вторичной активностью в данном срезе данных. Следовательно можно сделать вывод, что в основном сетевая активность связана с автоматическим поиском и объявлением сетевых устройств.

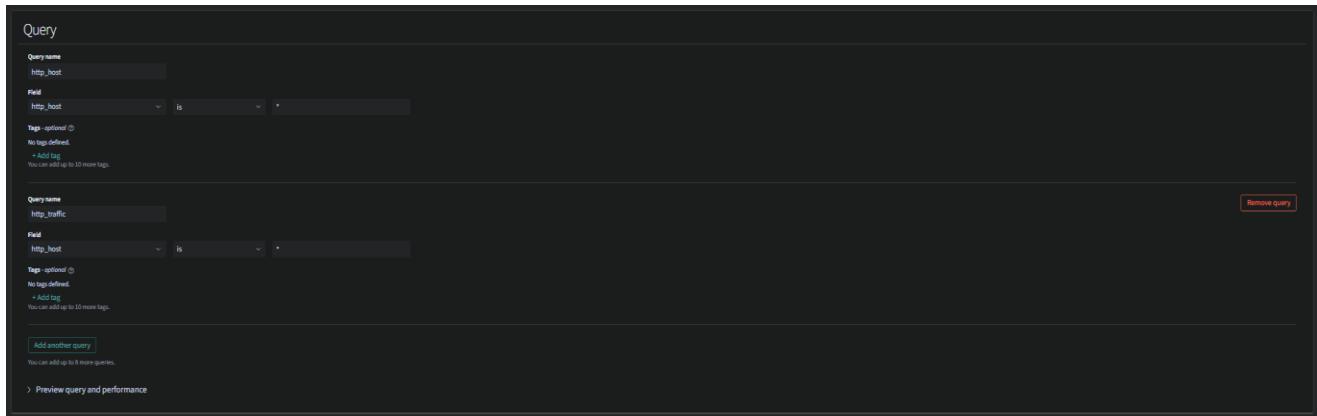
14. Изучим OpenSearch Alerting.

Из-за некоторых ограничений нашей версии контейнера, я попытался настроить простой монитор который будет срабатывать если есть ЛЮБОЕ количество документов

Начальная настройка:



Создаем Query. Из-за ограничений платформы для нашего сценария создадим два Query с одинаковыми условиями:



Создаем тригер:

AND http_traffic = условие "ЕСЛИ есть документы, соответствующие запросу http_traffic", что эквивалентно "Сработать, если обнаружен HTTP трафик".

The screenshot shows the AWS CloudWatch Triggers interface. A single trigger named 'test' is listed. The trigger conditions are set to 'http_host' AND 'http_traffic'. The actions section is currently empty. There is a note indicating that no channels have been added yet.

Таким образом наш тригер будет срабатывать когда какой-либо http трафик появится. Однако из-за ограничений арі в нашей реализации контейнера большинство функционала недоступно, и по большей части из-за выключенной безопасности.

15. Изучим возможности OpenSearch Dashboards по анализу геоданных

В наших данных нет геометрической информации, поэтому для работы с гео-данными потребуется обогащение исходных данных. Для этого обычно используются сервисы по типу MaxMind GeoIP2 и IP2Location. Однако в целях изучения мы обогатим наши исходные данные вручную “выдуманными” данными, для чего будем использовать Python скрипт:

https://github.com/l1ratch/WC_BISO/blob/main/5_sem/TXbCK/practic/pr_5/ewgd.py

Для обогащения данных был разработан Python-скрипт, который выполняет следующие операции:

1. Добавление полей в маппинг индекса OpenSearch для хранения геоданных:
geo_location (тип geo_point) - координаты широты/долготы;
country - страна расположения;
city – город;
region - географический регион.
2. Генерация демонстрационных данных на основе предопределенного списка городов мира, включая:
Столицы и крупные города (Нью-Йорк, Лондон, Токио и др.);
Различные географические регионы (Северная Америка, Европа, Азия и т.д.);
Реалистичные координаты для каждого местоположения.
3. Обновление документов в индексе packets-msv с присвоением случайных географических меток существующим записям сетевого трафика.

Приступим к обогащению:

```

INFO[opensearch]:POST http://localhost:9212/packets-msv/_update/xGBPXZoBb_53JuwfSTWe?refresh=false [status:200 request:0.008s]
INFO[opensearch]:POST http://localhost:9212/packets-msv/_update/G2BPXZoBb_53JuwfSTWe?refresh=false [status:200 request:0.009s]
INFO[opensearch]:POST http://localhost:9212/packets-msv/_update/IwBPXZoBb_53JuwfSTWe?refresh=false [status:200 request:0.01s]
INFO[opensearch]:POST http://localhost:9212/packets-msv/_update/lmBPXZoBb_53JuwfSTWe?refresh=false [status:200 request:0.012s]
INFO[opensearch]:POST http://localhost:9212/packets-msv/_update/H2BPXZoBb_53JuwfSTWe?refresh=false [status:200 request:0.013s]
INFO[opensearch]:POST http://localhost:9212/packets-msv/_update/0wBPXZoBb_53JuwfSTWe?refresh=false [status:200 request:0.013s]
INFO[opensearch]:POST http://localhost:9212/packets-msv/_update/zwBPXZoBb_53JuwfSTWe?refresh=false [status:200 request:0.009s]
INFO[opensearch]:POST http://localhost:9212/packets-msv/_update/lzBPXZoBb_53JuwfSTWe?refresh=false [status:200 request:0.009s]
INFO[opensearch]:POST http://localhost:9212/packets-msv/_update/JwBPXZoBb_53JuwfSTWe?refresh=false [status:200 request:0.009s]
INFO[opensearch]:POST http://localhost:9212/packets-msv/_update/JwBPXZoBb_53JuwfSTWe?refresh=false [status:200 request:0.007s]
INFO[main] :Добавлено 200 документов
INFO[main] :Обогащение завершено. Всего обновлено 200 документов
INFO[opensearch]:POST http://localhost:9212/packets-msv/_search [status:200 request:0.009s]
INFO[main] :Проверка индекса завершена
INFO[main] :IP: 10.2.13.101 -> São Paulo, Brazil
INFO[main] :IP: 10.2.13.1 -> New York, USA
INFO[main] :IP: 10.2.13.101 -> Paris, France
INFO[main] :IP: 10.2.13.101 -> Berlin, Germany
INFO[opensearch]:POST http://localhost:9212/packets-msv/_doc?refresh=true [status:201 request:0.248s]
INFO[main] :Добавлен демо-документ: 93.184.216.34 -> Frankfurt
INFO[opensearch]:POST http://localhost:9212/packets-msv/_doc?refresh=true [status:201 request:0.034s]
INFO[main] :Добавлен демо-документ: 8.8.8.8 -> Mountain View
INFO[opensearch]:POST http://localhost:9212/packets-msv/_doc?refresh=true [status:201 request:0.032s]
INFO[main] :Добавлен демо-документ: 77.88.55.60 -> Moscow
INFO[main] :Обогащение данных завершено успешно!
(venv) msv_12@ubuntuserverforpractic:~/opensearch-msv$ 

```

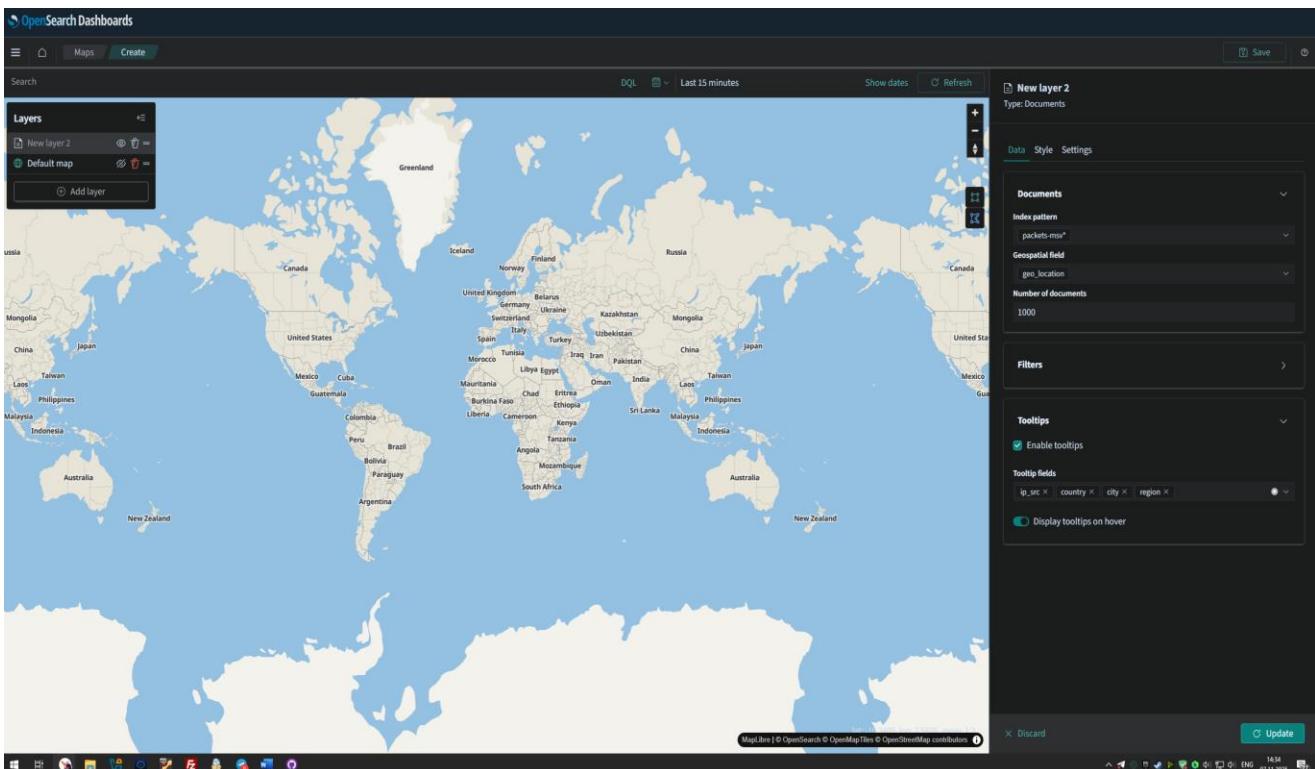
Проверим добавление данных:

```

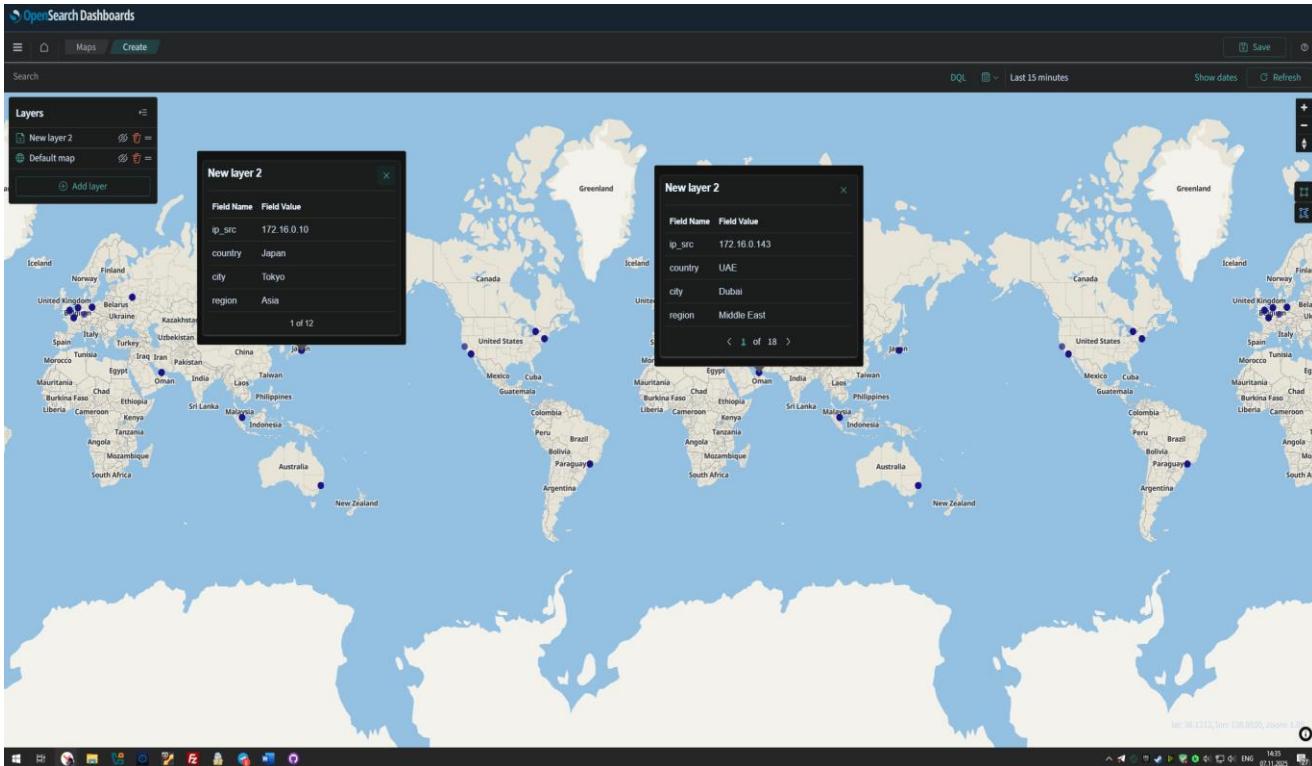
(venv) msv_12@ubuntuserverforpractic:~/opensearch-msv$ curl -X GET "http://localhost:9212/packets-msv/_search" -H 'Content-Type: application/json' -d '{
  "size": 3,
  "query": {
    "exists": {
      "field": "geo_location"
    }
  },
  "_source": ["ip_src", "country", "city", "geo_location"]
}'
{"took":2,"timed_out":false,"shards":[{"total":1,"successful":1,"skipped":0,"failed":0}],"hits":{"total":{"value":203,"relation":"eq"},"max_score":1.0,"hits": [{"_index":"packets-msv","_id":"w2BPXZoBb_53JuwfSTWe","_score":1.0,"_source":{"country":"China","geo_location":{"lon":116.4074,"lat":39.9042}, "city":"Beijing","ip_src":"10.2.13.101"}, {"_index":"packets-msv","_id":"xGBPXZoBb_53JuwfSTWe","_score":1.0,"_source":{"country":"UAE","geo_location":{"lon":55.2708,"lat":25.2048}, "city":"Dubai","ip_src":"10.2.13.101"}, {"_index":"packets-msv","_id":"xwBPXZoBb_53JuwfSTWe","_score":1.0,"_source":{"country":"UAE","geo_location":{"lon":55.2708,"lat":25.2048}, "city":"Dubai","ip_src":"10.2.13.1"}]}]}}
(venv) msv_12@ubuntuserverforpractic:~/opensearch-msv$ 

```

Открываем в визуализациях карту и добавляем новый слой:



Получаем карту с точками отображающие географические локации добавленные нами и связанные с данными из исходных файлов:



В этом пункте мы обновили документы сетевого трафика путем добавления географических меток. Для обогащения данных использовался Python-скрипт, который присвоил случайные географические локации из предопределенного списка, включающего 14 городов из различных регионов мира.

16. Заключение

В ходе выполнения практической работы были получены навыки развертывания и администрирования контейнеризированных приложений с использованием Docker и Docker Compose. Успешно развернута система OpenSearch и панель OpenSearch Dashboards, произведена загрузка и анализ сетевого трафика, а также визуализация результатов.

С помощью инструмента TShark выполнена предварительная обработка PCAP-файлов, после чего данные были загружены в OpenSearch для дальнейшего анализа. Исследование логов показало характерные особенности сетевой активности, включая использование протоколов HTTP, DNS и защищённых соединений HTTPS. Были выявлены возможные признаки автоматизированных запросов и работы локального DNS-сервера.

Кроме того, реализовано обогащение данных географическими метками, что позволило расширить возможности аналитики и визуализации. Также изучены базовые принципы настройки мониторинга и оповещений (Alerting) в OpenSearch, что является важным элементом систем информационной безопасности.

Таким образом, в результате проделанной работы достигнута цель — освоены инструменты для работы с частично структуризованными данными и получения аналитической информации на основе сетевого трафика с использованием современных технологий контейнеризации и анализа данных.