



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

Отметка / результат

Селин А. А.

ФИО

Москва 2025 г.

Оглавление

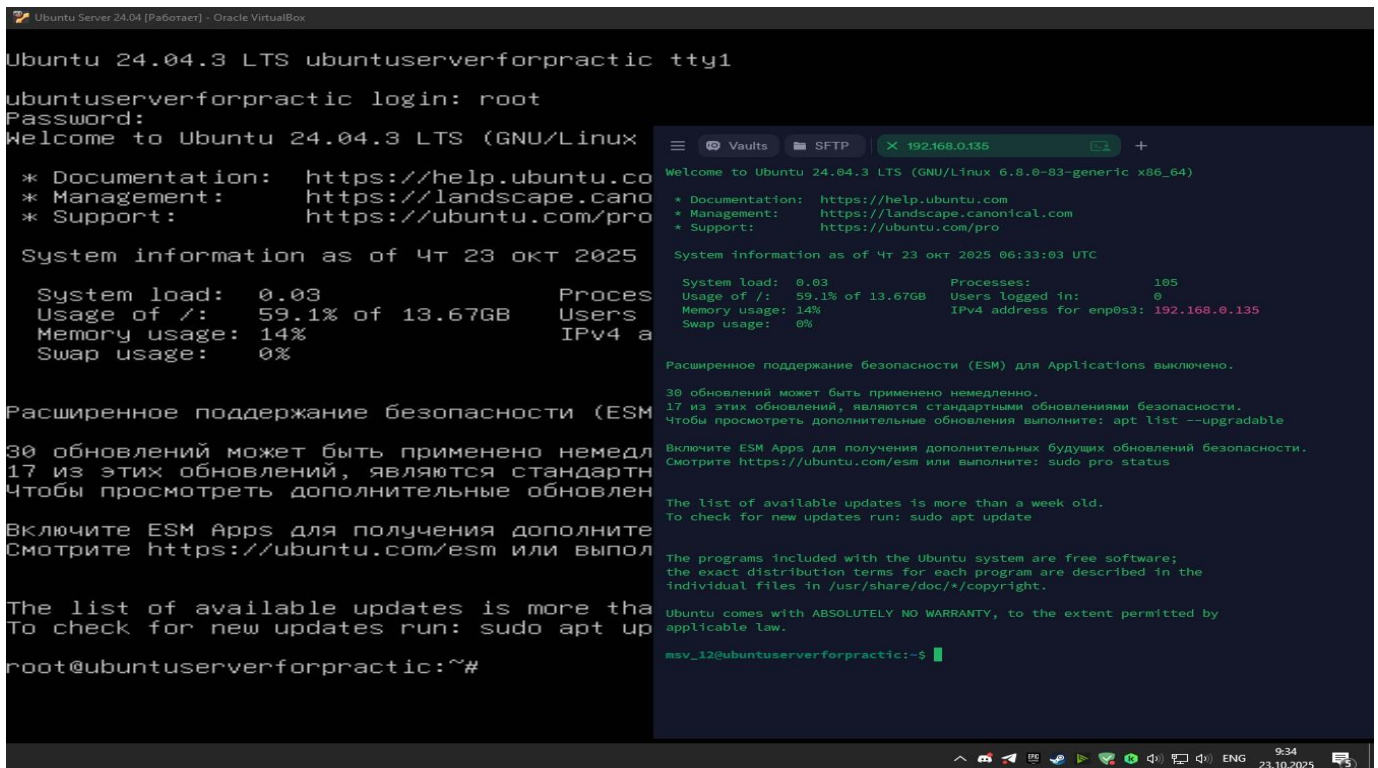
- 1. Запуск виртуальной машины с Ubuntu Server 24.04, подключение к ней по ssh используя ПО Termius для удобства взаимодействия.....3
- 2. Создание пользователя и настройка окружения3
- 3. Установка Docker и Docker Compose4
- 4. Настройка параметров ядра(Постоянное изменение)5
- 5. Создание docker-compose.yml для OpenSearch5
- 6. Запуск OpenSearch6
- 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..... 10
- 12. Выполним поиск в разделе Discover. 11
- 14. Изучим OpenSearch Alerting. 16
- 15. Изучим возможности OpenSearch Dashboards по анализу гео-данных 18
- 16. Заключение.....20

ПРАКТИЧЕСКАЯ РАБОТА № 4

«Знакомство с инструментами для работы с частично структурированными 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 Server 24.04 (Pa60raet) - Oracle VirtualBox
Ubuntu 24.04.3 LTS ubuntuerverforpractic tty1
ubuntuerverforpractic login: root
Password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-26-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * 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%

Расширенное поддержание безопасности (ESM) для Applications выключено.
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

root@ubuntuerverforpractic:~#
```

2. Создание пользователя и настройка окружения

```
root@ubuntuerverforpractic:~# 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

```

Vaults SFTP 192.168.0.135
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]

```

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 -v
Docker version 28.5.1, build e180ab8
msv_12@ubuntuserverforpractic:~$ docker-compose --version
Docker Compose version v2.33.1
msv_12@ubuntuserverforpractic:~$
```

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:~$
```

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$
```

```

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@ubuntu-server-for-practic:~/opensearch-msv$ sudo docker-compose up -d
[+] Running 2/2
! 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@ubuntu-server-for-practic:~/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@ubuntu-server-for-practic:~/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:
  libbcg729-0 libcares2 liblua5.2-0 libnghttp3-3 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:
  libbcg729-0 libcares2 liblua5.2-0 libnghttp3-3 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 объем занятого дискового пространства возрастет 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 libbcg729-0:amd64.
(Чтение базы данных ... на данный момент установлено 137659 файлов и каталого
Подготовка к распаковке .../00-libbcg729-0_1.1.1-2build1_amd64.deb ...
Распаковывается libbcg729-0: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 libnghttp3-3:amd64.
Подготовка к распаковке .../03-libnghttp3-3_0.8.0-2_amd64.deb ...
Распаковывается libnghttp3-3: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) ...
```

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@ubuntu-server-for-practic:~/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 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@ubuntu-server-for-practic:~/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-UR 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@ubuntu-server-for-practic:~/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. 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@ubuntu-server-for-practic:~/opensearch-msv$
```

Теперь распакуем архивы:

```
msv_12@ubuntu-server-for-practic:~/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@ubuntu-server-for-practic:~/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@ubuntu-server-for-practic:~/opensearch-msv$
```

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 dns.qry.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 dns.qry.name \
-e tcp.flags \
-E header=y -E separator=\; -E aggregator=, > result_msv.csv
Running as user "root" and group "root". This could be dangerous.
msv_12@ubuntuserverforpractic:~/opensearch-msv$
```

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 dns.qry.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 dns.qry.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$
```

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 dns.qry.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 dns.qry.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"
```

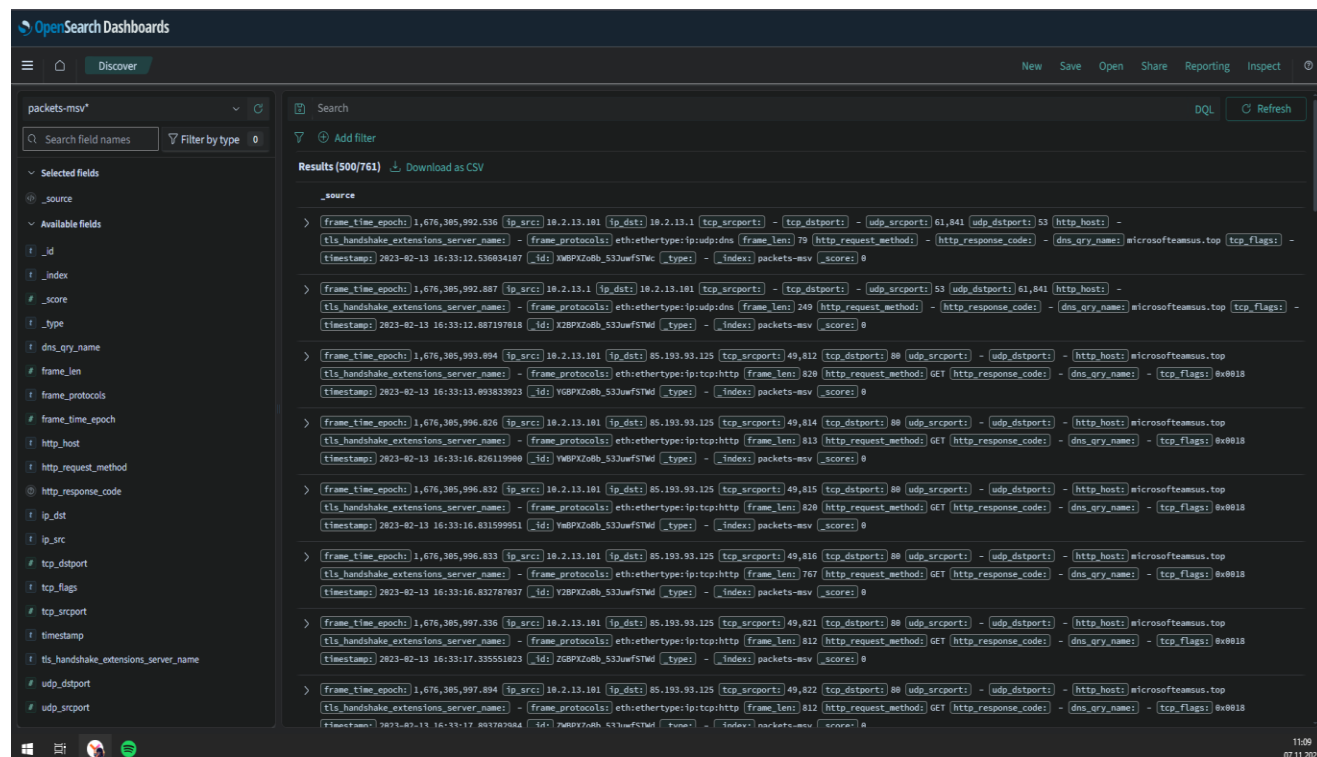
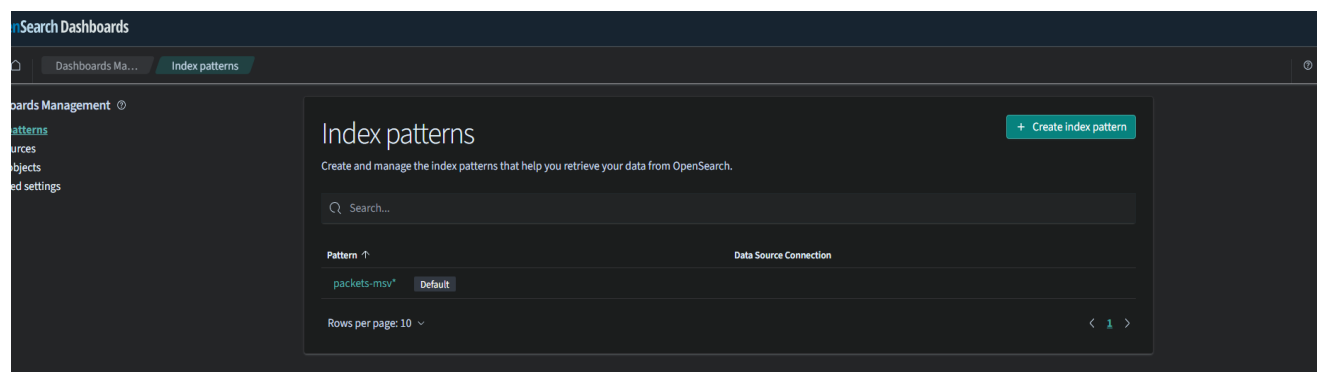
10. Загрузка данных используя Python скрипт.

Используемый Python скрипт:

https://github.com/11ratch/WC_BISO/blob/main/5_sem/TXвСК/practic/pr_5/uto.py

```
(venv) msv_12@ubuntu-server-for-practic:~/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@ubuntu-server-for-practic:~/opensearch-msv$
```

11. Запуск панели, подготовка OpenSearchDashboards.



12. Выполним поиск в разделе Discover.

The screenshot shows the Elastic Search Discover interface. At the top, the search bar contains the query: `[frame_time_epoch: 1,676,395,992.536 [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:ethertype:ip:udp:dns`. Below the search bar, the results are displayed in a table format. The table has columns for `_id`, `_index`, `_score`, `_type`, `dns_qry_name`, `frame_len`, `frame_protocols`, `frame_time_epoch`, `http_host`, `http_request_method`, `http_response_code`, `ip_dst`, `ip_src`, `tcp_dstport`, `tcp_flags`, `tcp_srcport`, `timestamp`, `tls_handshake_extensions_server_name`, `udp_dstport`, and `udp_srcport`. The results show a single document with the following values:

Field	Value
<code>_id</code>	<code>XMBPXZoBb_53JuwF5TWc</code>
<code>_index</code>	<code>packets-mv</code>
<code>_score</code>	<code>0</code>
<code>_type</code>	<code>-</code>
<code>dns_qry_name</code>	<code>microsoftteamsus.top</code>
<code>frame_len</code>	<code>79</code>
<code>frame_protocols</code>	<code>eth:ethertype:ip:udp:dns</code>
<code>frame_time_epoch</code>	<code>1,676,395,992.536</code>
<code>http_host</code>	<code>-</code>
<code>http_request_method</code>	<code>-</code>
<code>http_response_code</code>	<code>-</code>
<code>ip_dst</code>	<code>10.2.13.1</code>
<code>ip_src</code>	<code>10.2.13.101</code>
<code>tcp_dstport</code>	<code>-</code>
<code>tcp_flags</code>	<code>-</code>
<code>tcp_srcport</code>	<code>-</code>
<code>timestamp</code>	<code>2023-02-13 16:33:12.536834167</code>
<code>tls_handshake_extensions_server_name</code>	<code>-</code>
<code>udp_dstport</code>	<code>53</code>
<code>udp_srcport</code>	<code>61,841</code>

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

GET

Add filter

Results (16/16)

Download as CSV

_source

frame_time_epoch

1,676,365,893.894

[ip_src]

10.2.12.181

[ip_dst]

85.193.93.125

[tcp_srcport]

49,812

[tcp_dstport]

80

[udp_srcport]

-

[udp_dstport]

-

[http_host]

microsoftfeamus.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]

0x0018

[timestamp]

2023-02-13 16:33:13.89383923

[_id]

2d8PZ2oB_533wF5Twe

[_type]

-

[_index]

packets-mov

[_score]

0

frame_time_epoch

1,676,365,896.826

[ip_src]

10.2.12.181

[ip_dst]

85.193.93.125

[tcp_srcport]

49,814

[tcp_dstport]

80

[udp_srcport]

-

[udp_dstport]

-

[http_host]

microsoftfeamus.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]

0x0018

[timestamp]

2023-02-13 16:33:16.83139908

[_id]

2d8PZ2oB_533wF5Twe

[_type]

-

[_index]

packets-mov

[_score]

0

frame_time_epoch

1,676,365,898.832

[ip_src]

10.2.12.181

[ip_dst]

85.193.93.125

[tcp_srcport]

49,815

[tcp_dstport]

80

[udp_srcport]

-

[udp_dstport]

-

[http_host]

microsoftfeamus.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]

0x0018

[timestamp]

2023-02-13 16:33:16.83159901

[_id]

2d8PZ2oB_533wF5Twe

[_type]

-

[_index]

packets-mov

[_score]

0

frame_time_epoch

1,676,365,896.833

[ip_src]

10.2.12.181

[ip_dst]

85.193.93.125

[tcp_srcport]

49,816

[tcp_dstport]

80

[udp_srcport]

-

[udp_dstport]

-

[http_host]

microsoftfeamus.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]

0x0018

[timestamp]

2023-02-13 16:33:16.83278707

[_id]

2d8PZ2oB_533wF5Twe

[_type]

-

[_index]

packets-mov

[_score]

0

frame_time_epoch

1,676,365,897.336

[ip_src]

10.2.12.181

[ip_dst]

85.193.93.125

[tcp_srcport]

49,821

[tcp_dstport]

80

[udp_srcport]

-

[udp_dstport]

-

[http_host]

microsoftfeamus.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]

0x0018

[timestamp]

2023-02-13 16:33:17.335551823

[_id]

2d8PZ2oB_533wF5Twe

[_type]

-

[_index]

packets-mov

[_score]

0

frame_time_epoch

1,676,365,897.894

[ip_src]

10.2.12.181

[ip_dst]

85.193.93.125

[tcp_srcport]

49,822

[tcp_dstport]

80

[udp_srcport]

-

[udp_dstport]

-

[http_host]

microsoftfeamus.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]

0x0018

[timestamp]

2023-02-13 16:33:17.83378284

[_id]

2d8PZ2oB_533wF5Twe

[_type]

-

[_index]

packets-mov

[_score]

0

frame_time_epoch

1,676,365,898.4

[ip_src]

10.2.12.181

[ip_dst]

85.193.93.125

[tcp_srcport]

49,823

[tcp_dstport]

80

[udp_srcport]

-

[udp_dstport]

-

[http_host]

microsoftfeamus.top

[tls_handshake_extensions_server_name]

-

[frame_protocols]

eth:ethertype:ip:tcp:http

[frame_len]

778

[http_request_method]

GET

[http_response_code]

-

[dns_qry_name]

-

[tcp_flags]

0x0018

[timestamp]

2023-02-13 16:33:17.335551823

[_id]

2d8PZ2oB_533wF5Twe

[_type]

-

[_index]

packets-mov

[_score]

0

frame_time_epoch

1,676,365,898.4

[ip_src]

10.2.12.181

[ip_dst]

85.193.93.125

[tcp_srcport]

49,824

[tcp_dstport]

80

[udp_srcport]

-

[udp_dstport]

-

[http_host]

microsoftfeamus.top

[tls_handshake_extensions_server_name]

-

[frame_protocols]

eth:ethertype:ip:tcp:http

[frame_len]

774

[http_request_method]

GET

[http_response_code]

-

[dns_qry_name]

-

[tcp_flags]

0x0018

[timestamp]

2023-02-13 16:33:16.488251884

[_id]

2d8PZ2oB_533wF5Twe

[_type]

-

[_index]

packets-mov

[_score]

0

frame_time_epoch

1,676,365,899.781

[ip_src]

10.2.12.181

[ip_dst]

85.41.139.138

[tcp_srcport]

49,863

[tcp_dstport]

80

[udp_srcport]

-

[udp_dstport]

-

[http_host]

alishabinderader.com

[tls_handshake_extensions_server_name]

-

[frame_protocols]

eth:ethertype:ip:tcp:http

[frame_len]

368

[http_request_method]

GET

[http_response_code]

-

[dns_qry_name]

-

[tcp_flags]

0x0018

[timestamp]

2023-02-13 16:38:19.798752828

[_id]

2d8PZ2oB_533wF5Twe

[_type]

-

[_index]

packets-mov

[_score]

0

frame_time_epoch

1,677,169,248.552

[ip_src]

10.24.8.189

[ip_dst]

184.156.149.6

[tcp_srcport]

56,655

[tcp_dstport]

80

[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]

GET

[http_response_code]

-

[dns_qry_name]

-

[tcp_flags]

0x0018

[timestamp]

2023-02-23 16:28:48.552176952

[_id]

4d8PZ2oB_533wF5Twe

[_type]

-

[_index]

packets-mov

[_score]

0

Expanded document

Table

JSON

_id

4d8PZ2oB_533wF5Twe

_index

packets-mov

_score

0

_type

-

dns_qry_name

-

frame_len

244

frame_protocols

eth:ethertype:ip:tcp:http

frame_time_epoch

1,677,169,248.552

http_host

184.156.149.6

http_request_method

GET

http_response_code

-

ip_dst

184.156.149.6

View single document

104.156.149.6

Add filter

Results (11/11)

Download as CSV

_source

frame_time_epoch

1,677,169,246.874

[ip_src]

10.24.8.189

[ip_dst]

184.156.149.6

[tcp_srcport]

56,652

[tcp_dstport]

80

[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]

POST

[http_response_code]

-

[dns_qry_name]

-

[tcp_flags]

0x0018

[timestamp]

2023-02-23 16:28:46.874183893

[_id]

3d8PZ2oB_533wF5Twe

[_type]

-

[_index]

packets-mov

[_score]

0

frame_time_epoch

1,677,169,246.896

[ip_src]

10.24.8.189

[ip_dst]

184.156.149.6

[tcp_srcport]

56,652

[tcp_dstport]

80

[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]

POST

[http_response_code]

-

[dns_qry_name]

-

[tcp_flags]

0x0018

[timestamp]

2023-02-23 16:28:46.896113955

[_id]

3d8PZ2oB_533wF5Twe

[_type]

-

[_index]

packets-mov

[_score]

0

frame_time_epoch

1,677,169,246.939

[ip_src]

10.24.8.189

[ip_dst]

184.156.149.6

[tcp_srcport]

56,653

[tcp_dstport]

80

[udp_srcport]

-

[udp_dstport]

-

[http_host]

184.156.149.6

[tls_handshake_extensions_server_name]

-

[frame_protocols]

eth:ethertype:ip:tcp:http

[frame_len]

235

[http_request_method]

POST

[http_response_code]

-

[dns_qry_name]

-

[tcp_flags]

0x0018

[timestamp]

2023-02-23 16:28:46.938873853

[_id]

3d8PZ2oB_533wF5Twe

[_type]

-

[_index]

packets-mov

[_score]

0

frame_time_epoch

1,677,169,246.943

[ip_src]

10.24.8.189

[ip_dst]

184.156.149.6

[tcp_srcport]

56,654

[tcp_dstport]

80

[udp_srcport]

-

[udp_dstport]

-

[http_host]

184.156.149.6

[tls_handshake_extensions_server_name]

-

[frame_protocols]

eth:ethertype:ip:tcp:http

[frame_len]

239

[http_request_method]

POST

[http_response_code]

-

[dns_qry_name]

-

[tcp_flags]

0x0018

[timestamp]

2023-02-23 16:28:46.942673114

[_id]

3d8PZ2oB_533wF5Twe

[_type]

-

[_index]

packets-mov

[_score]

0

frame_time_epoch

1,677,169,246.953

[ip_src]

10.24.8.189

[ip_dst]

184.156.149.6

[tcp_srcport]

56,655

[tcp_dstport]

80

[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]

GET

[http_response_code]

-

[dns_qry_name]

-

[tcp_flags]

0x0018

[timestamp]

2023-02-23 16:28:48.552176952

[_id]

4d8PZ2oB_533wF5Twe

[_type]

-

[_index]

packets-mov

[_score]

0

frame_time_epoch

1,677,169,250.352

[ip_src]

10.24.8.189

[ip_dst]

184.156.149.6

[tcp_srcport]

56,656

[tcp_dstport]

80

[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]

POST

[http_response_code]

-

[dns_qry_name]

-

[tcp_flags]

0x0018

[timestamp]

2023-02-23 16:28:56.351599444

[_id]

4d8PZ2oB_533wF5Twe

[_type]

-

[_index]

packets-mov

[_score]

0

frame_time_epoch

1,677,169,250.422

[ip_src]

10.24.8.189

[ip_dst]

184.156.149.6

[tcp_srcport]

56,657

[tcp_dstport]

80

[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]

POST

[http_response_code]

-

[dns_qry_name]

-

[tcp_flags]

0x0018

[timestamp]

2023-02-23 16:28:56.422363997

[_id]

4d8PZ2oB_533wF5Twe

[_type]

-

[_index]

packets-mov

[_score]

0

frame_time_epoch

1,677,169,250.443

[ip_src]

10.24.8.189

[ip_dst]

184.156.149.6

[tcp_srcport]

56,657

[tcp_dstport]

80

[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]

GET

[http_response_code]

-

[dns_qry_name]

-

[tcp_flags]

0x0018

[timestamp]

2023-02-23 16:28:56.444776858

[_id]

4d8PZ2oB_533wF5Twe

[_type]

-

[_index]

packets-mov

[_score]

0

frame_time_epoch

1,677,169,250.569

[ip_src]

10.24.8.189

[ip_dst]

184.156.149.6

[tcp_srcport]

56,658

[tcp_dstport]

80

[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]

POST

[http_response_code]

-

[dns_qry_name]

-

[tcp_flags]

0x0018

[timestamp]

2023-02-23 16:28:56.565448948

[_id]

3d8PZ2oB_533wF5Twe

[_type]

-

[_index]

packets-mov

[_score]

0

frame_time_epoch

1,677,169,250.613

[ip_src]

10.24.8.189

[ip_dst]

184.156.149.6

[tcp_srcport]

56,662

[tcp_dstport]

80

[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]

POST

[http_response_code]

-

[dns_qry_name]

-

[tcp_flags]

0x0018

[timestamp]

2023-02-23 16:28:56.613158888

[_id]

6d8PZ2oB_533wF5Twe

[_type]

-

[_index]

packets-mov

[_score]

0

frame_time_epoch

1,677,169,250.625

[ip_src]

10.24.8.189

[ip_dst]

184.156.149.6

[tcp_srcport]

56,663

[tcp_dstport]

80

[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]

POST

[http_response_code]

-

[dns_qry_name]

-

[tcp_flags]

0x0018

[timestamp]

2023-02-23 16:28:56.659830118

[_id]

6d8PZ2oB_533wF5Twe

[_type]

-

[_index]

packets-mov

[_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:

12

10.24.8.189

DQL

Refresh

ip_src:10.24.8.189

NOT http_request_method:GET

Add filter

Results (25/25)

Download as CSV

>

frame_time_epoch

1,677,169,246.874

[ip_src]

10.24.8.189

[ip_dst]

104.156.149.6

[tcp_srcport]

50,652

[tcp_dstport]

80

[udp_srcport]

[udp_dstport]

[http_host]

104.156.149.6

[tls_handshake_extensions_server_name]

[frame_protocols]

eth:etherType:ip:tcp:http

[frame_len]

222

http_request_method

PROF2ND

[http_response_code]

[dns_qry_name]

[tcp_flags]

0x0010

[timestamp]

2023-02-23 16:20:46.87483893

[_id]

308PZz0b_53zwf5Twe

[_type]

[_index]

packets-mov

[_score]

0

>

frame_time_epoch

1,677,169,246.896

[ip_src]

10.24.8.189

[ip_dst]

104.156.149.6

[tcp_srcport]

50,652

[tcp_dstport]

80

[udp_srcport]

[udp_dstport]

[http_host]

104.156.149.6

[tls_handshake_extensions_server_name]

[frame_protocols]

eth:etherType:ip:tcp:http

[frame_len]

223

http_request_method

PROF2ND

[http_response_code]

[dns_qry_name]

[tcp_flags]

0x0010

[timestamp]

2023-02-23 16:20:46.89611363

[_id]

308PZz0b_53zwf5Twe

[_type]

[_index]

packets-mov

[_score]

0

>

frame_time_epoch

1,677,169,246.939

[ip_src]

10.24.8.189

[ip_dst]

104.156.149.6

[tcp_srcport]

50,653

[tcp_dstport]

80

[udp_srcport]

[udp_dstport]

[http_host]

104.156.149.6

[tls_handshake_extensions_server_name]

[frame_protocols]

eth:etherType:ip:tcp:http

[frame_len]

235

http_request_method

PROF2ND

[http_response_code]

[dns_qry_name]

[tcp_flags]

0x0010

[timestamp]

2023-02-23 16:20:46.938873053

[_id]

308PZz0b_53zwf5Twe

[_type]

[_index]

packets-mov

[_score]

0

>

frame_time_epoch

1,677,169,246.963

[ip_src]

10.24.8.189

[ip_dst]

104.156.149.6

[tcp_srcport]

50,654

[tcp_dstport]

80

[udp_srcport]

[udp_dstport]

[http_host]

104.156.149.6

[tls_handshake_extensions_server_name]

[frame_protocols]

eth:etherType:ip:tcp:http

[frame_len]

233

http_request_method

PROF2ND

[http_response_code]

[dns_qry_name]

[tcp_flags]

0x0010

[timestamp]

2023-02-23 16:20:46.962875134

[_id]

308PZz0b_53zwf5Twe

[_type]

[_index]

packets-mov

[_score]

0

>

frame_time_epoch

1,677,169,250.352

[ip_src]

10.24.8.189

[ip_dst]

104.156.149.6

[tcp_srcport]

50,656

[tcp_dstport]

80

[udp_srcport]

[udp_dstport]

[http_host]

104.156.149.6

[tls_handshake_extensions_server_name]

[frame_protocols]

eth:etherType:ip:tcp:http

[frame_len]

240

http_request_method

PROF2ND

[http_response_code]

[dns_qry_name]

[tcp_flags]

0x0010

[timestamp]

2023-02-23 16:20:50.35199844

[_id]

408PZz0b_53zwf5Twe

[_type]

[_index]

packets-mov

[_score]

0

>

frame_time_epoch

1,677,169,250.422

[ip_src]

10.24.8.189

[ip_dst]

104.156.149.6

[tcp_srcport]

50,657

[tcp_dstport]

80

[udp_srcport]

[udp_dstport]

[http_host]

104.156.149.6

[tls_handshake_extensions_server_name]

[frame_protocols]

eth:etherType:ip:tcp:http

[frame_len]

231

http_request_method

PROF2ND

[http_response_code]

[dns_qry_name]

[tcp_flags]

0x0010

[timestamp]

2023-02-23 16:20:50.422363997

[_id]

408PZz0b_53zwf5Twe

[_type]

[_index]

packets-mov

[_score]

0

>

frame_time_epoch

1,677,169,250.445

[ip_src]

10.24.8.189

[ip_dst]

10.24.8.8

[tcp_srcport]

50,683

[tcp_dstport]

53

[http_host]

[tls_handshake_extensions_server_name]

[frame_protocols]

eth:etherType:ip:udp:dns

[frame_len]

78

[http_request_method]

[http_response_code]

[dns_qry_name]

bandalarenote.com

[tcp_flags]

[timestamp]

2023-02-23 16:20:50.445182987

[_id]

508PZz0b_53zwf5Twe

[_type]

[_index]

packets-mov

[_score]

0

>

frame_time_epoch

1,677,169,250.569

[ip_src]

10.24.8.189

[ip_dst]

104.156.149.6

[tcp_srcport]

50,668

[tcp_dstport]

80

[udp_srcport]

[udp_dstport]

[http_host]

104.156.149.6

[tls_handshake_extensions_server_name]

[frame_protocols]

eth:etherType:ip:tcp:http

[frame_len]

244

http_request_method

PROF2ND

[http_response_code]

[dns_qry_name]

[tcp_flags]

0x0010

[timestamp]

2023-02-23 16:20:50.569440840

[_id]

508PZz0b_53zwf5Twe

[_type]

[_index]

packets-mov

[_score]

0

>

frame_time_epoch

1,677,169,250.613

[ip_src]

10.24.8.189

[ip_dst]

104.156.149.6

[tcp_srcport]

50,667

[tcp_dstport]

80

[udp_srcport]

[udp_dstport]

[http_host]

104.156.149.6

[tls_handshake_extensions_server_name]

[frame_protocols]

eth:etherType:ip:tcp:http

[frame_len]

244

http_request_method

PROF2ND

[http_response_code]

[dns_qry_name]

[tcp_flags]

0x0010

[timestamp]

2023-02-23 16:20:50.613150886

[_id]

608PZz0b_53zwf5Twe

[_type]

[_index]

packets-mov

[_score]

0

>

frame_time_epoch

1,677,169,250.620

[ip_src]

10.24.8.189

[ip_dst]

104.156.149.6

[tcp_srcport]

50,663

[tcp_dstport]

80

[udp_srcport]

[udp_dstport]

[http_host]

104.156.149.6

[tls_handshake_extensions_server_name]

[frame_protocols]

eth:etherType:ip:tcp:http

[frame_len]

240

http_request_method

PROF2ND

[http_response_code]

[dns_qry_name]

[tcp_flags]

0x0010

[timestamp]

2023-02-23 16:20:50.620881114

[_id]

608PZz0b_53zwf5Twe

[_type]

[_index]

packets-mov

[_score]

0

>

frame_time_epoch

1,677,169,252.389

[ip_src]

10.24.8.189

[ip_dst]

10.24.8.8

[tcp_srcport]

[tcp_dstport]

[udp_srcport]

64,644

[udp_dstport]

53

[http_host]

[tls_handshake_extensions_server_name]

[frame_protocols]

eth:etherType:ip:udp:dns

[frame_len]

71

[http_request_method]

[http_response_code]

[dns_qry_name]

tuittenet

[tcp_flags]

[timestamp]

2023-02-23 16:20:52.389008969

[_id]

608PZz0b_53zwf5Twe

[_type]

[_index]

packets-mov

[_score]

0

>

frame_time_epoch

1,677,169,252.621

[ip_src]

10.24.8.189

[ip_dst]

5.61.47.8

[tcp_srcport]

50,664

[tcp_dstport]

443

[udp_srcport]

[udp_dstport]

[http_host]

[tls_handshake_extensions_server_name]

tuittenet

[frame_protocols]

eth:etherType:ip:tcp:tls

[frame_len]

232

[http_request_method]

[http_response_code]

[dns_qry_name]

[tcp_flags]

0x0010

[timestamp]

2023-02-23 16:20:52.62120885

[_id]

708PZz0b_53zwf5Twe

[_type]

[_index]

packets-mov

[_score]

0

>

frame_time_epoch

1,677,169,314.231

[ip_src]

10.24.8.189

[ip_dst]

10.24.8.8

[tcp_srcport]

[tcp_dstport]

[udp_srcport]

37,368

[udp_dstport]

53

[http_host]

[tls_handshake_extensions_server_name]

[frame_protocols]

eth:etherType:ip:udp:dns

[frame_len]

75

[http_request_method]

[http_response_code]

[dns_qry_name]

renomesolar.com

[tcp_flags]

[timestamp]

2023-02-23 16:21:54.231316896

[_id]

708PZz0b_53zwf5Twe

[_type]

[_index]

packets-mov

[_score]

0

>

frame_time_epoch

1,677,169,314.392

[ip_src]

10.24.8.189

[ip_dst]

38.180.0.89

[tcp_srcport]

50,666

[tcp_dstport]

443

[udp_srcport]

[udp_dstport]

[http_host]

[tls_handshake_extensions_server_name]

renomesolar.com

[frame_protocols]

eth:etherType:ip:tcp:tls

[frame_len]

236

[http_request_method]

[http_response_code]

[dns_qry_name]

[tcp_flags]

0x0010

[timestamp]

2023-02-23 16:21:54.391580185

[_id]

808PZz0b_53zwf5Twe

[_type]

[_index]

packets-mov

[_score]

0

>

frame_time_epoch

1,677,169,315.931

[ip_src]

10.24.8.189

[ip_dst]

38.180.0.89

[tcp_srcport]

50,668

[tcp_dstport]

443

[udp_srcport]

[udp_dstport]

[http_host]

[tls_handshake_extensions_server_name]

renomesolar.com

[frame_protocols]

eth:etherType:ip:tcp:tls

[frame_len]

236

[http_request_method]

[http_response_code]

[dns_qry_name]

[tcp_flags]

0x0010

[timestamp]

2023-02-23 16:21:55.931886863

[_id]

808PZz0b_53zwf5Twe

[_type]

[_index]

packets-mov

[_score]

0

>

frame_time_epoch

1,677,169,315.932

[ip_src]

10.24.8.189

[ip_dst]

38.180.0.89

[tcp_srcport]

50,667

[tcp_dstport]

443

[udp_srcport]

[udp_dstport]

[http_host]

[tls_handshake_extensions_server_name]

renomesolar.com

[frame_protocols]

eth:etherType:ip:tcp:tls

[frame_len]

236

[http_request_method]

[http_response_code]

[dns_qry_name]

[tcp_flags]

0x0010

[timestamp]

2023-02-23 16:21:55.931874837

[_id]

808PZz0b_53zwf5Twe

[_type]

[_index]

packets-mov

[_score]

0

>

frame_time_epoch

1,677,169,322.293

[ip_src]

10.24.8.189

[ip_dst]

10.24.8.8

[tcp_srcport]

[tcp_dstport]

[udp_srcport]

53,403

[udp_dstport]

53

[http_host]

[tls_handshake_extensions_server_name]

[frame_protocols]

eth:etherType:ip:udp:dns

[frame_len]

81

[http_request_method]

[http_response_code]

[dns_qry_name]

palasdelareforma.com

[tcp_flags]

[timestamp]

2023-02-23 16:22:02.293471898

[_id]

808PZz0b_53zwf5Twe

[_type]

[_index]

packets-mov

[_score]

0

>

frame_time_epoch

1,677,169,322.72

[ip_src]

10.24.8.189

[ip_dst]

37.252.4.77

[tcp_srcport]

50,674

[tcp_dstport]

443

[udp_srcport]

[udp_dstport]

[http_host]

[tls_handshake_extensions_server_name]

palasdelareforma.com

[frame_protocols]

eth:etherType:ip:tcp:tls

[frame_len]

242

[http_request_method]

[http_response_code]

[dns_qry_name]

[tcp_flags]

0x0010

[timestamp]

2023-02-23 16:22:02.723888878

[_id]

908PZz0b_53zwf5Twe

[_type]

[_index]

packets-mov

[_score]

0

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 (0/0)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]: [tcp_dstport]: [udp_srcport]:37,368 [udp_dstport]:53 [http_host]: [tls_handshake_extensions_server_name]: [frame_protocols]:eth:etherType:ip:udp:dns [frame_len]:75 [http_request_method]: [http_response_code]: [dns_qry_name]:renomesolar.com [tcp_flags]: [timestamp]:2023-02-23 16:21:54.231316896 [_id]:708PZz0b_53zwf5Twe [_type]: [_index]:packets-mov [_score]:0

>

[frame_time_epoch]:1,677,169,314.285 [ip_src]:10.24.8.189 [ip_dst]:10.24.8.189 [tcp_srcport]: [tcp_dstport]: [udp_srcport]:37,368 [udp_dstport]:53 [http_host]: [tls_handshake_extensions_server_name]: [frame_protocols]:eth:etherType:ip:udp:dns [frame_len]:91 [http_request_method]: [http_response_code]: [dns_qry_name]:renomesolar.com [tcp_flags]: [timestamp]:2023-02-23 16:21:54.285239988 [_id]:708PZz0b_53zwf5Twe [_type]: [_index]:packets-mov [_score]:0

>

[frame_time_epoch]:1,677,169,314.392 [ip_src]:10.24.8.189 [ip_dst]:38.180.0.89 [tcp_srcport]:50,666 [tcp_dstport]:443 [udp_srcport]: [udp_dstport]: [http_host]: [tls_handshake_extensions_server_name]:renomesolar.com [frame_protocols]:eth:etherType:ip:tcp:tls [frame_len]:236 [http_request_method]: [http_response_code]: [dns_qry_name]: [tcp_flags]:0x0010 [timestamp]:2023-02-23 16:21:54.391580185 [_id]:808PZz0b_53zwf5Twe [_type]: [_index]:packets-mov [_score]:0

>

[frame_time_epoch]:1,677,169,315.931 [ip_src]:10.24.8.189 [ip_dst]:38.180.0.89 [tcp_srcport]:50,668 [tcp_dstport]:443 [udp_srcport]: [udp_dstport]: [http_host]: [tls_handshake_extensions_server_name]:renomesolar.com [frame_protocols]:eth:etherType:ip:tcp:tls [frame_len]:236 [http_request_method]: [http_response_code]: [dns_qry_name]: [tcp_flags]:0x0010 [timestamp]:2023-02-23 16:21:55.931886863 [_id]:808PZz0b_53zwf5Twe [_type]: [_index]:packets-mov [_score]:0

>

[frame_time_epoch]:1,677,169,315.932 [ip_src]:10.24.8.189 [ip_dst]:38.180.0.89 [tcp_srcport]:50,667 [tcp_dstport]:443 [udp_srcport]: [udp_dstport]: [http_host]: [tls_handshake_extensions_server_name]:renomesolar.com [frame_protocols]:eth:etherType:ip:tcp:tls [frame_len]:236 [http_request_method]: [http_response_code]: [dns_qry_name]: [tcp_flags]:0x0010 [timestamp]:2023-02-23 16:21:55.931874837 [_id]:808PZz0b_53zwf5Twe [_type]: [_index]:packets-mov [_score]:0

>

[frame_time_epoch]:1,677,169,616.189 [ip_src]:10.24.8.189 [ip_dst]:38.180.0.89 [tcp_srcport]:50,677 [tcp_dstport]:443 [udp_srcport]: [udp_dstport]: [http_host]: [tls_handshake_extensions_server_name]:renomesolar.com [frame_protocols]:eth:etherType:ip:tcp:tls [frame_len]:236 [http_request_method]: [http_response_code]: [dns_qry_name]: [tcp_flags]:0x0010 [timestamp]:2023-02-23 16:26:36.188749854 [_id]:908PZz0b_53zwf5Twe [_type]: [_index]:packets-mov [_score]:0

>

[frame_time_epoch]:1,677,169,917.647 [ip_src]:10.24.8.189 [ip_dst]:38.180.0.89 [tcp_srcport]:50,679 [tcp_dstport]:443 [udp_srcport]: [udp_dstport]: [http_host]: [tls_handshake_extensions_server_name]:renomesolar.com [frame_protocols]:eth:etherType:ip:tcp:tls [frame_len]:236 [http_request_method]: [http_response_code]: [dns_qry_name]: [tcp_flags]:0x0010 [timestamp]:2023-02-23 16:31:57.646892871 [_id]:908PZz0b_53zwf5Twe [_type]: [_index]:packets-mov [_score]:0

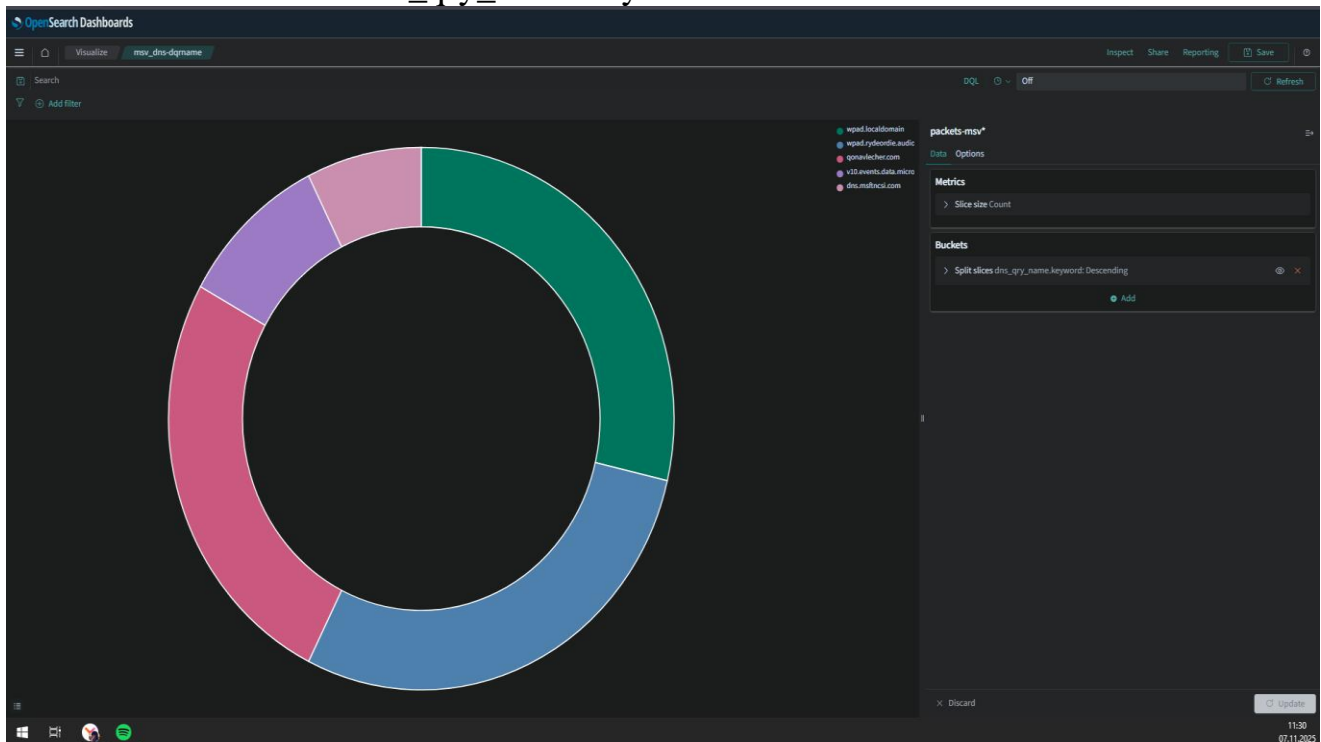
>

[frame_time_epoch]:1,677,179,219.237 [ip_src]:10.24.8.189 [ip_dst]:38.180.0.89 [tcp_srcport]:50,680 [tcp_dstport]:443 [udp_srcport]: [udp_dstport]: [http_host]: [tls_handshake_extensions_server_name]:renomesolar.com [frame_protocols]:eth:etherType:ip:tcp:tls [frame_len]:236 [http_request_method]: [http_response_code]: [dns_qry_name]: [tcp_flags]:0x0010 [timestamp]:2023-02-23 16:36:39.237183939 [_id]:908PZz0b_53zwf5Twe [_type]: [_index]:packets-mov [_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.

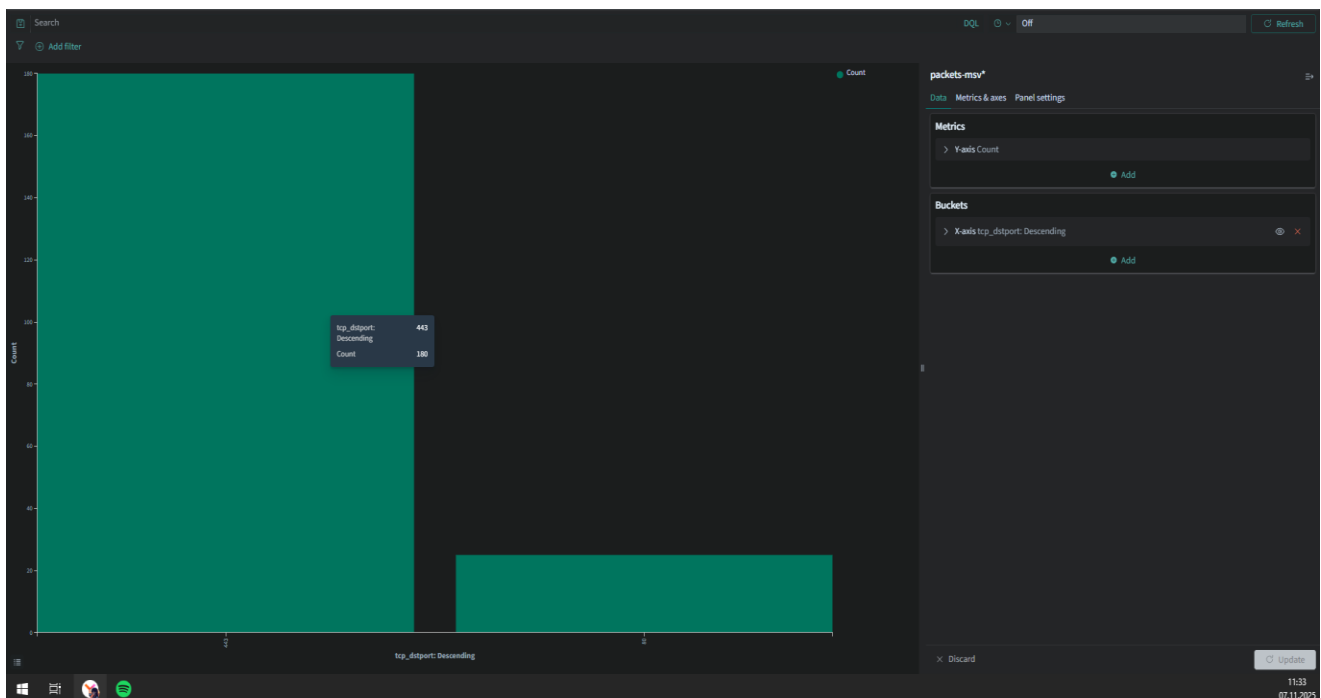
13. Создадим несколько визуализаций.

13.1. По полю dns_qry_name.keyword



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

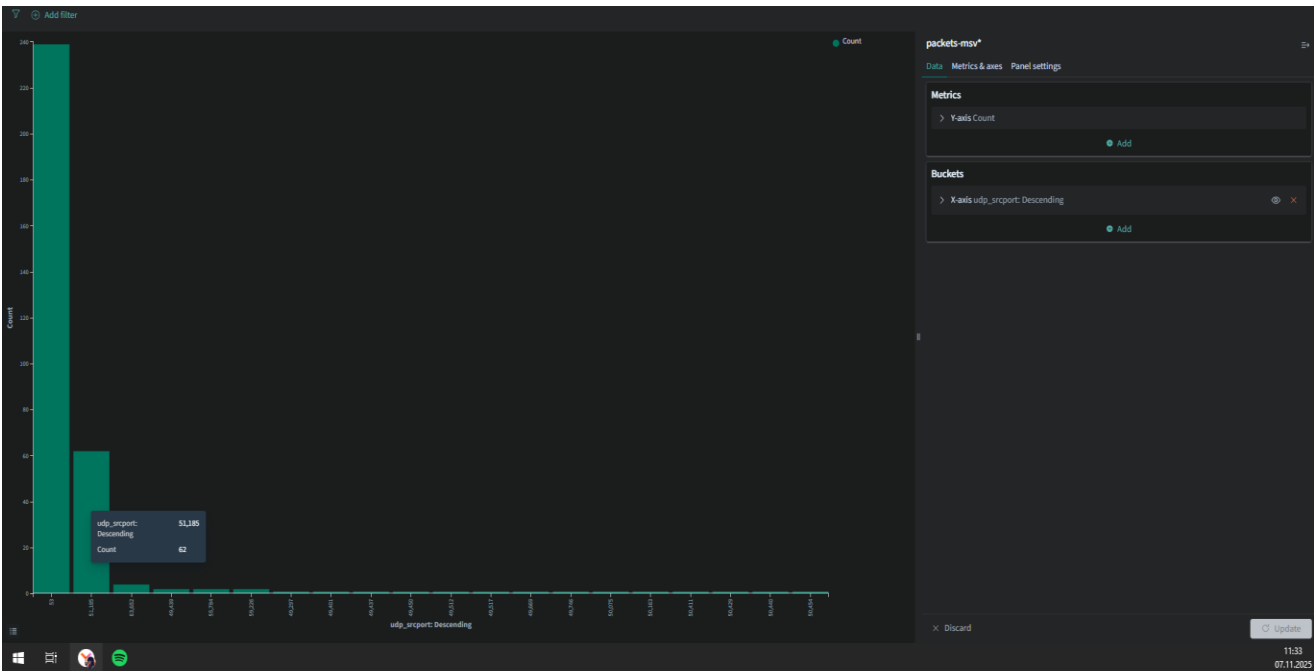
13.2. По полю tcp_dstport



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

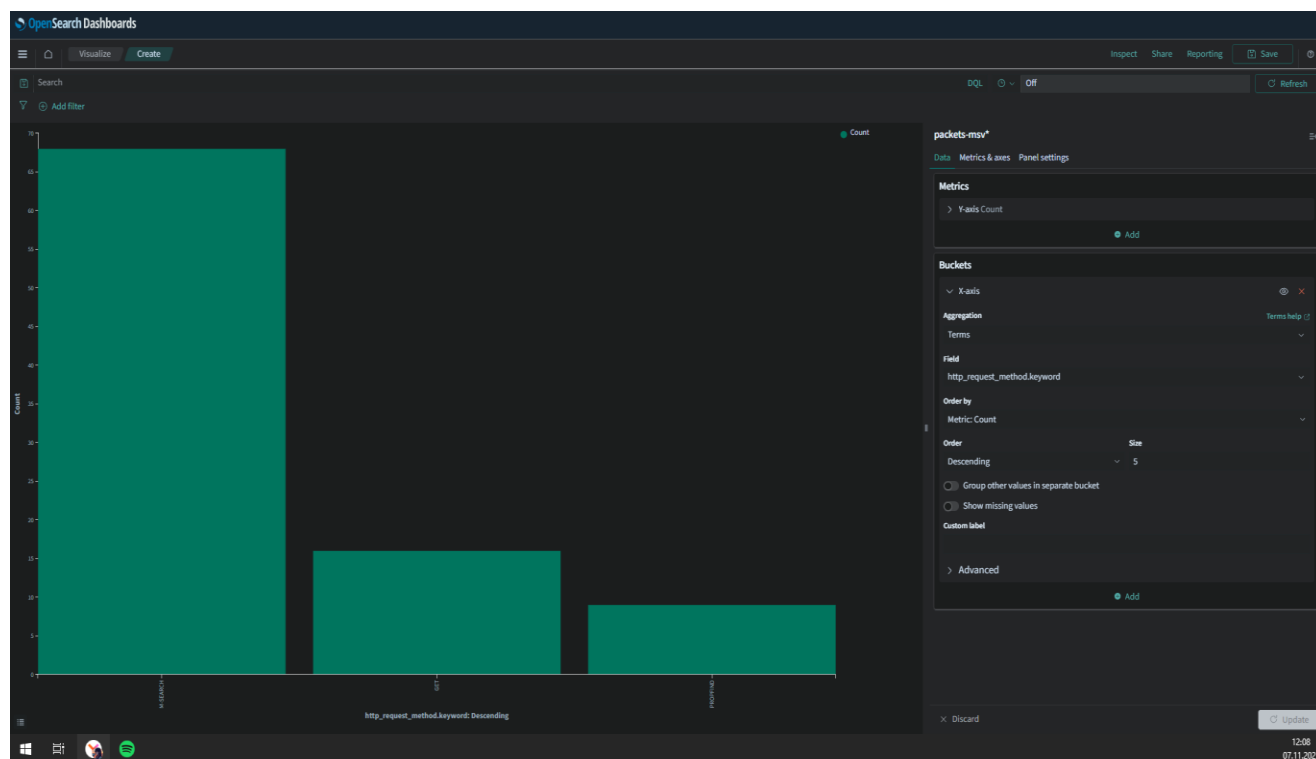
защищенному протоколу, лишь 25 запросов относятся к 80 порту.

13.3. По полю udp_srcport



На 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_request_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:

Create monitor

Monitor details

Monitor name:

Monitor type:

- ☐ Per query monitor: Per query monitors run a query and generate alerts based on trigger criteria that match query results.
- ☐ Per bucket monitor: Per bucket monitors run a query that evaluates trigger criteria based on aggregated values in the dataset.
- ☐ Per cluster metrics monitor: Per cluster metrics monitors run API requests to monitor the cluster's health.
- ☒ Per document monitor: Per document monitors run queries that select individual documents matching the trigger conditions.
- ☐ Composite monitor: Composite monitors chain the outputs of different monitor types and focus trigger conditions to reduce alert noise and generate clear results.

Monitor defining method: Specify the way you want to define your query and triggers. [Learn more](#)

☒ Visual editor ☐ Extraction query editor

Schedule

Frequency: By interval

Run every: Minute(s)

Select data

Index: packets-mov

You can use a "*" as a wildcard or data match index resolution in your index pattern.

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

Query

Query name: http_host

Field: http_host

Tag - optional: http_host

No tags defined. [+ Add tag](#)
You can add up to 10 more tags.

Query name: http_traffic [Remove query](#)

Field: http_host

Tag - optional: http_host

No tags defined. [+ Add tag](#)
You can add up to 10 more tags.

[Add another query](#)
You can add up to 8 more queries.

[Preview query and performance](#)

Создаем триггер:

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

Triggers (1) [Remove trigger](#)

Trigger name: test

Severity level: 2 (High)

Trigger conditions: Triggers on documents that match the following conditions.

Specify queries or tags:

http_host

AND http_traffic [Remove condition](#)

[+ Add condition](#)
You can add up to 8 more trigger conditions.

Actions (0): [Manage channels](#)

There are no existing channels. Add a channel to create an action.

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

15. Изучим возможности OpenSearch Dashboards по анализу гео-данных

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 “выдуманскими” данными, для чего будем использовать Python скрипт:

https://github.com/11ratch/WC_BISO/blob/main/5_sem/TXвCK/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.

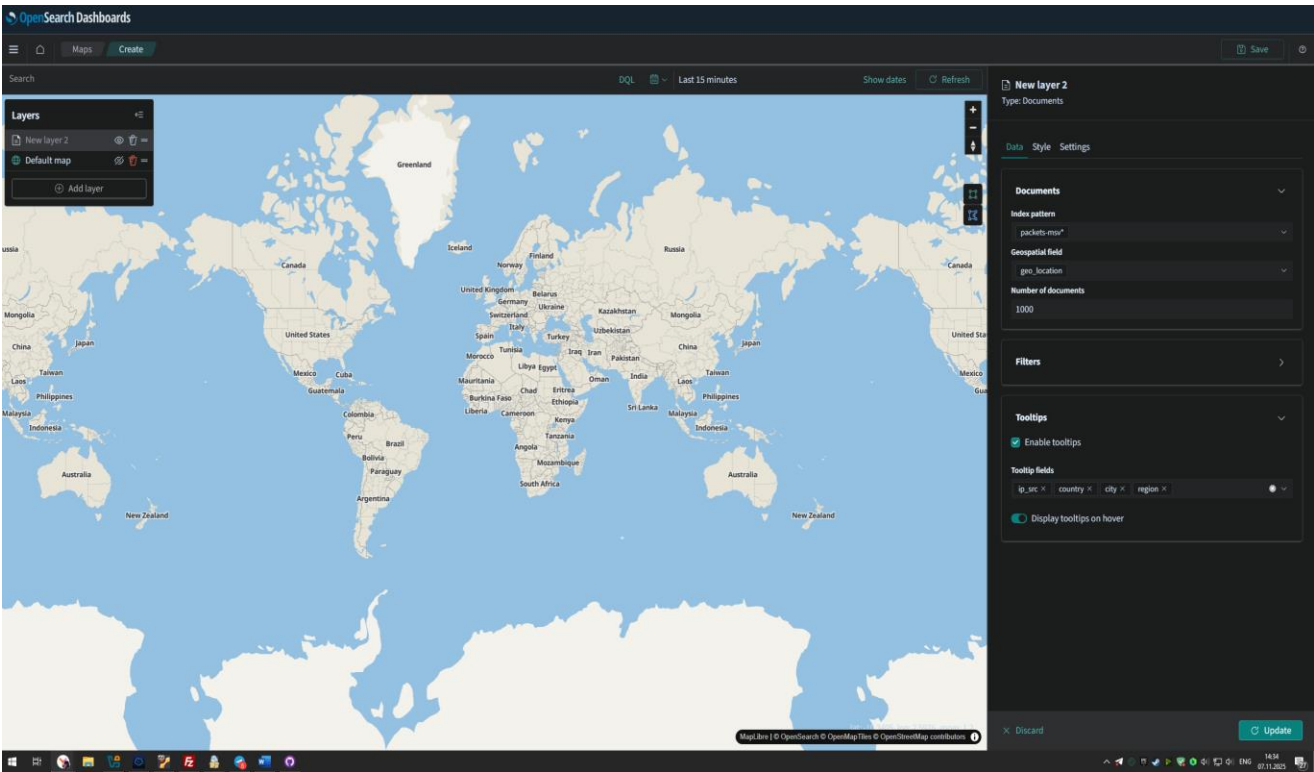
Приступим к обогащению:

```
INFO:opensearch:POST http://localhost:9212/packets-msv/_update/6uBPXZoBb_53JwufSTwe?refresh=false [status:200 request:0.008s]
INFO:opensearch:POST http://localhost:9212/packets-msv/_update/6zBPXZoBb_53JwufSTwe?refresh=false [status:200 request:0.009s]
INFO:opensearch:POST http://localhost:9212/packets-msv/_update/1uBPXZoBb_53JwufSTwe?refresh=false [status:200 request:0.012s]
INFO:opensearch:POST http://localhost:9212/packets-msv/_update/1uBPXZoBb_53JwufSTwe?refresh=false [status:200 request:0.011s]
INFO:opensearch:POST http://localhost:9212/packets-msv/_update/1uBPXZoBb_53JwufSTwe?refresh=false [status:200 request:0.011s]
INFO:opensearch:POST http://localhost:9212/packets-msv/_update/1uBPXZoBb_53JwufSTwe?refresh=false [status:200 request:0.010s]
INFO:opensearch:POST http://localhost:9212/packets-msv/_update/1uBPXZoBb_53JwufSTwe?refresh=false [status:200 request:0.009s]
INFO:opensearch:POST http://localhost:9212/packets-msv/_update/1uBPXZoBb_53JwufSTwe?refresh=false [status:200 request:0.007s]
INFO:opensearch:POST http://localhost:9212/packets-msv/_update/3uBPXZoBb_53JwufSTwe?refresh=false [status:200 request:0.006s]
INFO:opensearch:POST http://localhost:9212/packets-msv/_update/3uBPXZoBb_53JwufSTwe?refresh=false [status:200 request:0.007s]
INFO: _meta: _Обновлено 200 документов
INFO: _meta: _Обогащение завершено. Всего обновлено 200 документов
INFO:opensearch:POST http://localhost:9212/packets-msv/_search [status:200 request:0.009s]
INFO: _meta: _Примеры обновленных документов:
INFO: _meta: _ IP: 10.2.13.101 -> São Paulo, Brazil
INFO: _meta: _ IP: 10.2.13.1 -> New York, USA
INFO: _meta: _ IP: 10.2.13.101 -> Paris, France
INFO: _meta: _ IP: 10.2.13.101 -> Paris, France
INFO: _meta: _ IP: 10.2.13.101 -> Berlin, Germany
INFO:opensearch:POST http://localhost:9212/packets-msv/_doc?refresh=true [status:201 request:0.248s]
INFO: _meta: _Добавлен демо-документ: 53.104.210.34 -> Frankfurt
INFO:opensearch:POST http://localhost:9212/packets-msv/_doc?refresh=true [status:201 request:0.034s]
INFO: _meta: _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: _meta: _Добавлен демо-документ: 77.88.55.80 -> Moscow
INFO: _meta: _Обогащение данных завершено успешно!
(venv) msv_12@ubuntu-server-for-practic:~/opensearch-msv$
```

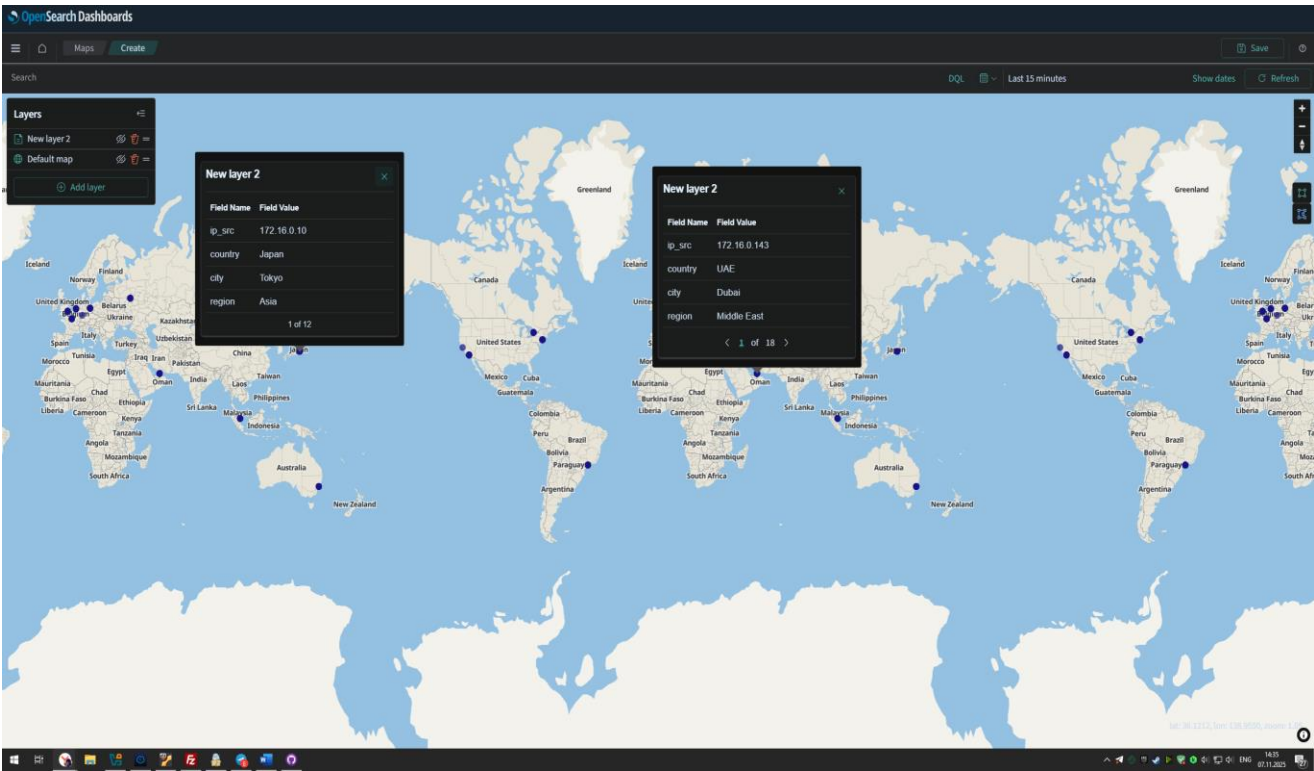
Проверим добавление данных:

```
(venv) msv_12@ubuntu-server-for-practic:~/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":12,"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_53JwufSTwe","_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":"xGPXZoBb_53JwufSTwe","_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":"wBPXZoBb_53JwufSTwe","_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@ubuntu-server-for-practic:~/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 структурированными данными и получения аналитической информации на основе сетевого трафика с использованием современных технологий контейнеризации и анализа данных.