



МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«МИРЭА – Российский технологический университет»

РТУ МИРЭА

Институт кибербезопасности и цифровых технологий (ИКБ)

КБ-2 «Информационно-аналитические системы кибербезопасности»

ОТЧЕТ О ВЫПОЛНЕНИИ ИНДИВИДУАЛЬНОГО ЗАДАНИЯ №4
В РАМКАХ ДИСЦИПЛИНЫ «ТЕХНОЛОГИИ
ХРАНЕНИЯ В СИСТЕМАХ КИБЕРБЕЗОПАСНОСТИ»

Выполнил:

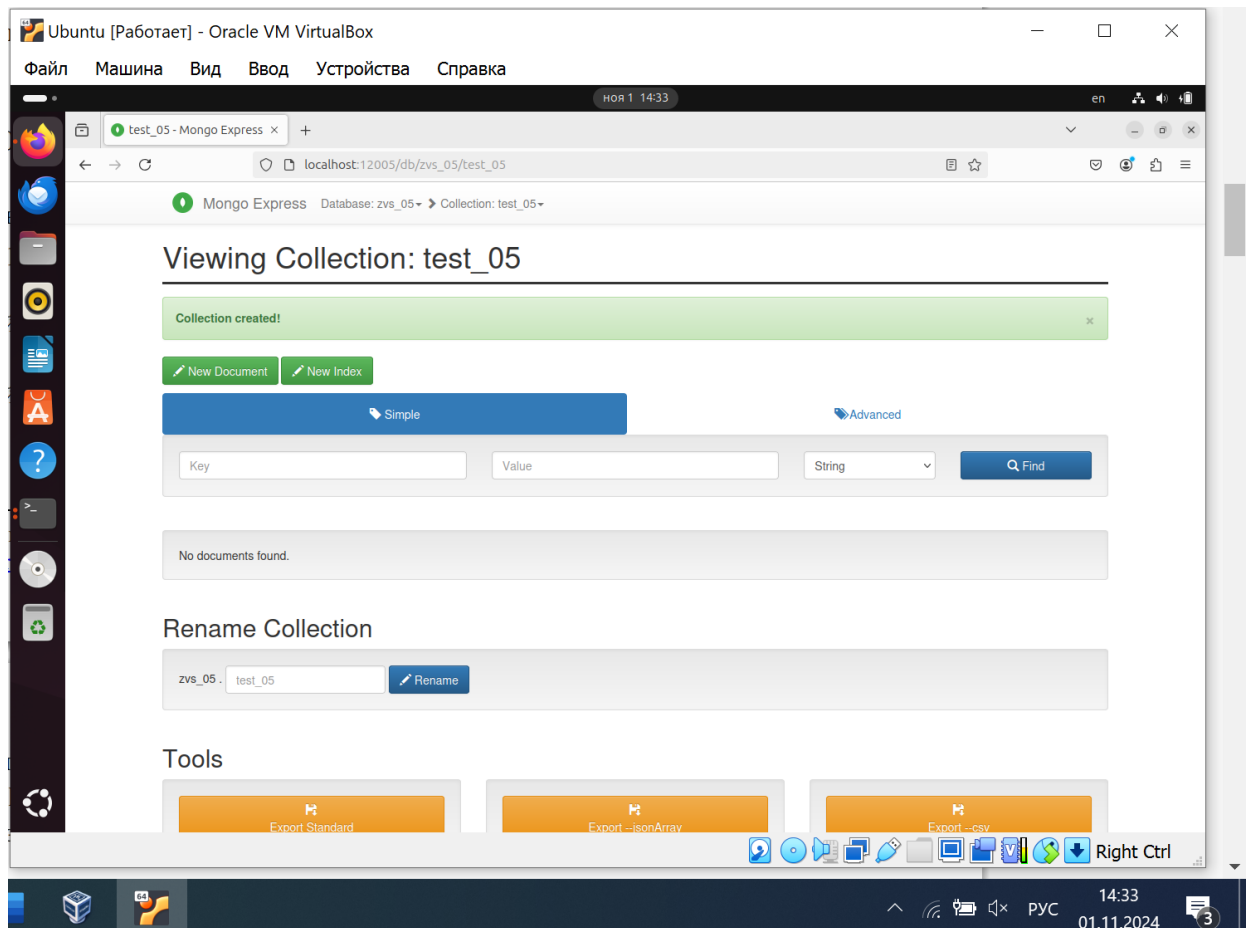
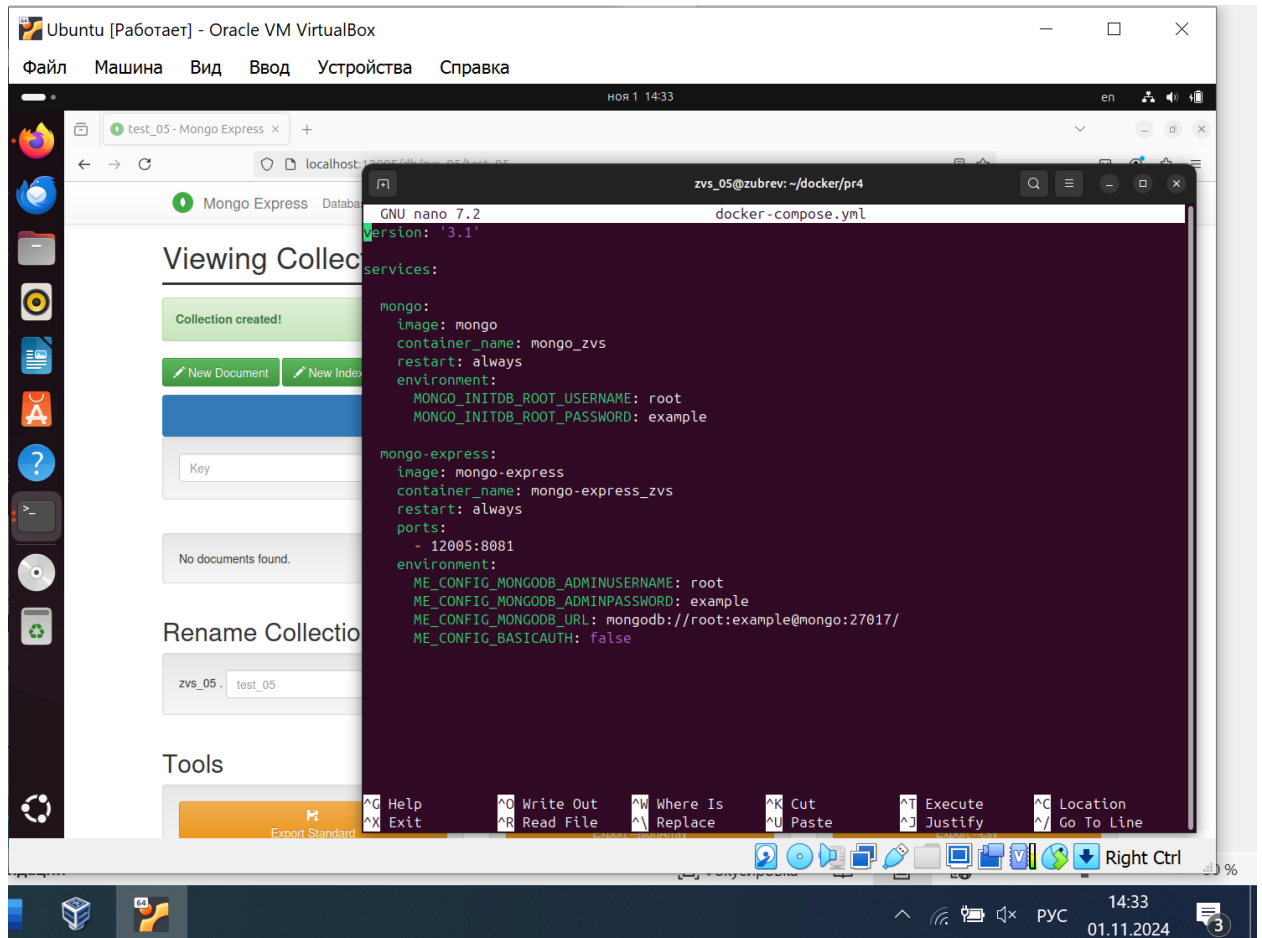
Студент 3-ого курса

Учебной группы БИСО-02-22

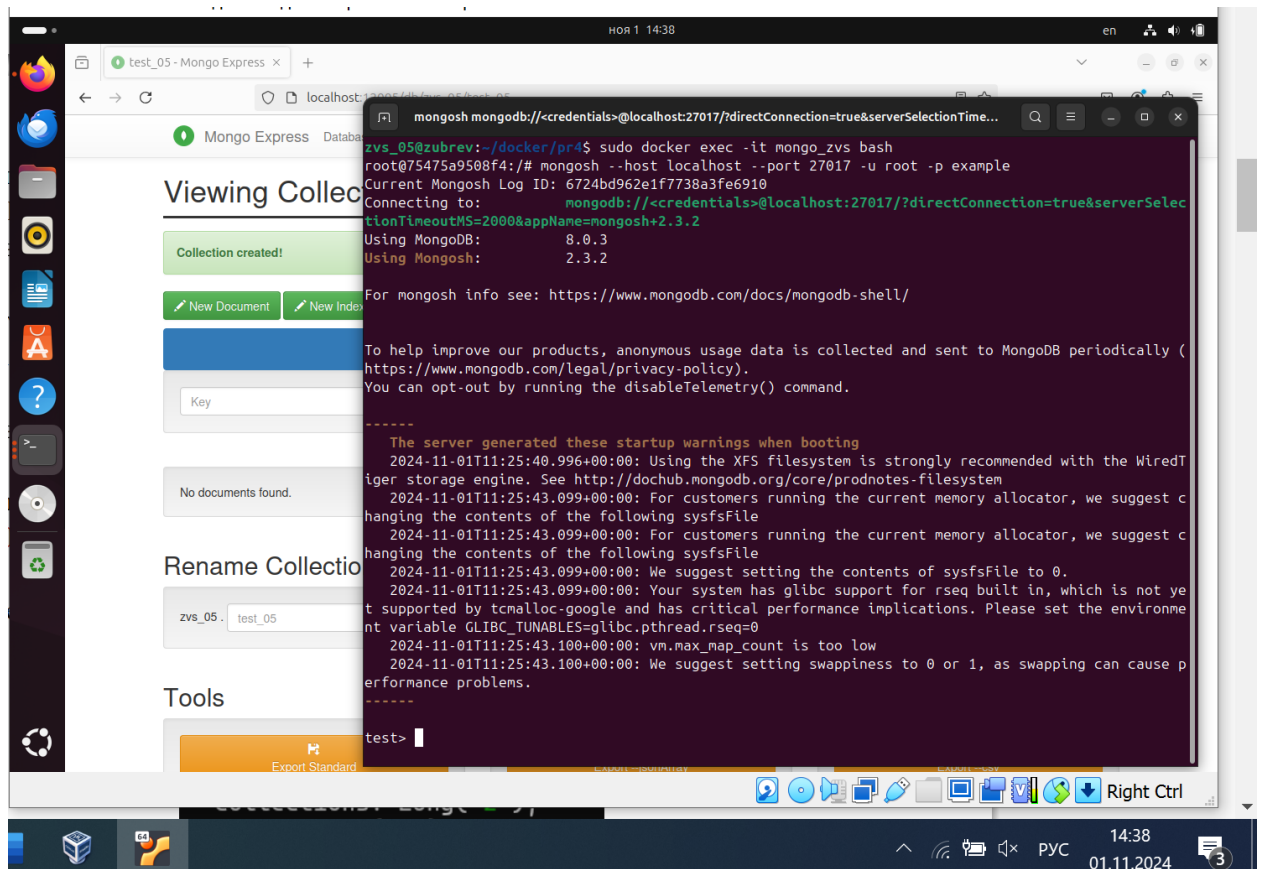
Зубарев В.С.

Москва 2024

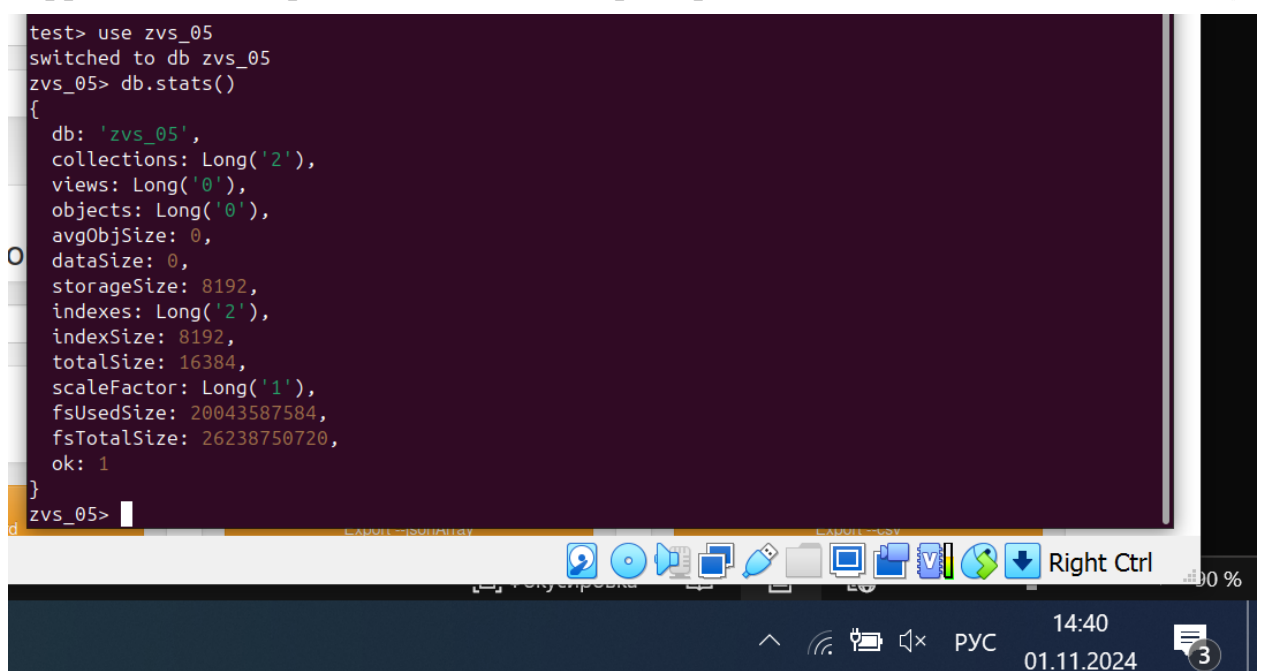
Разверните MongoDB и Mongo Express с помощью Docker Compose.



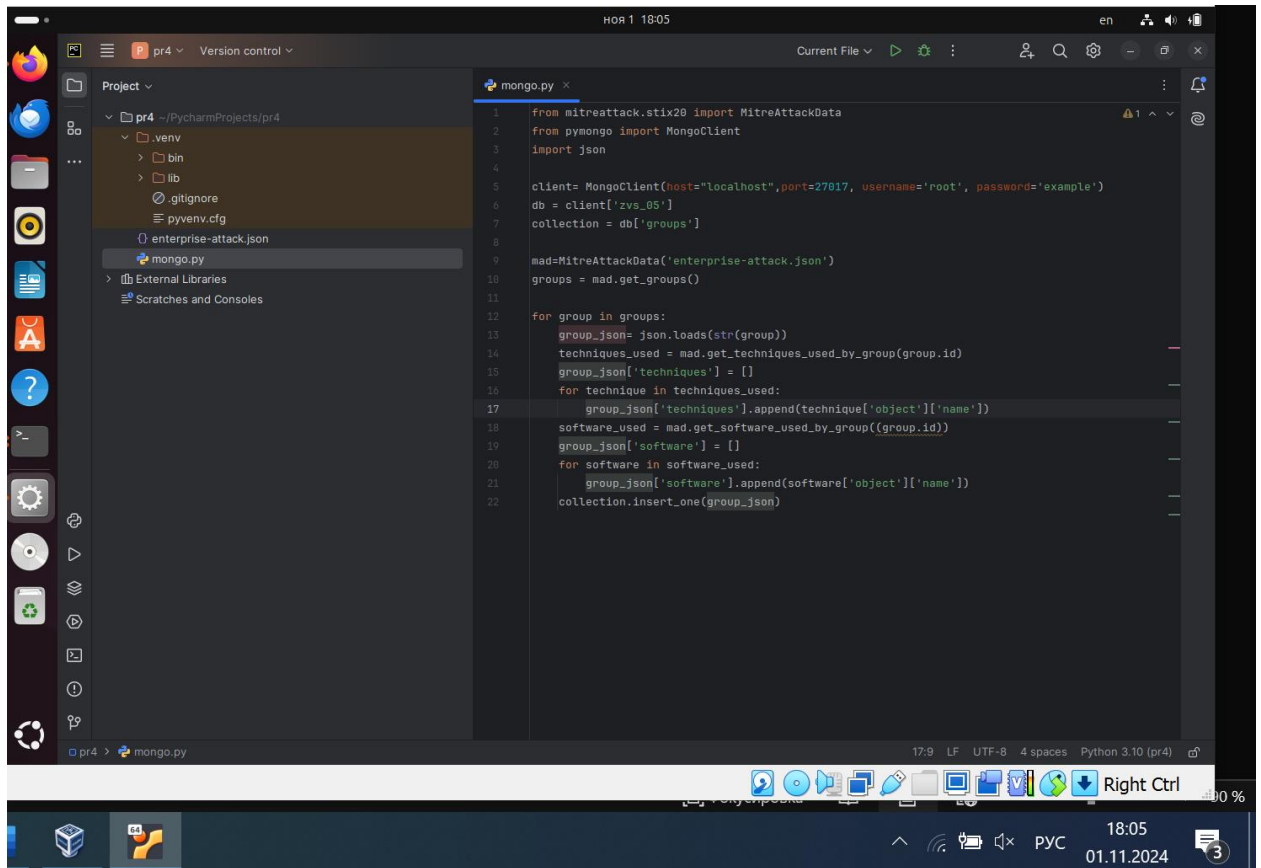
Зайдите в контейнер MongoDB с помощью команды `docker exec`. Выйти из контейнера можно с помощью команды `exit`.



Подключитесь к ранее созданной БД. Пример: `use ipd_07`. Проверьте, что все работает. Например, командой `db.stats()`:

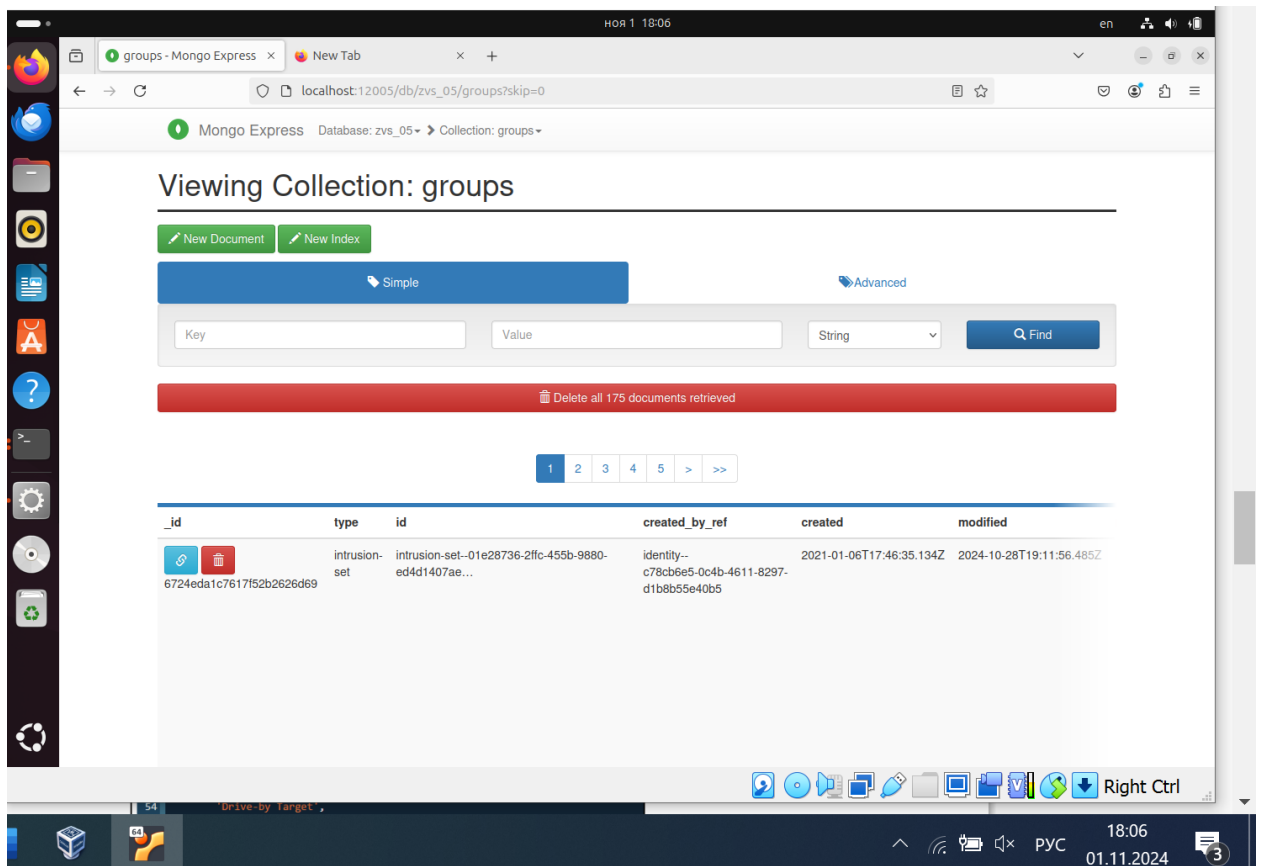


Напишите скрипт

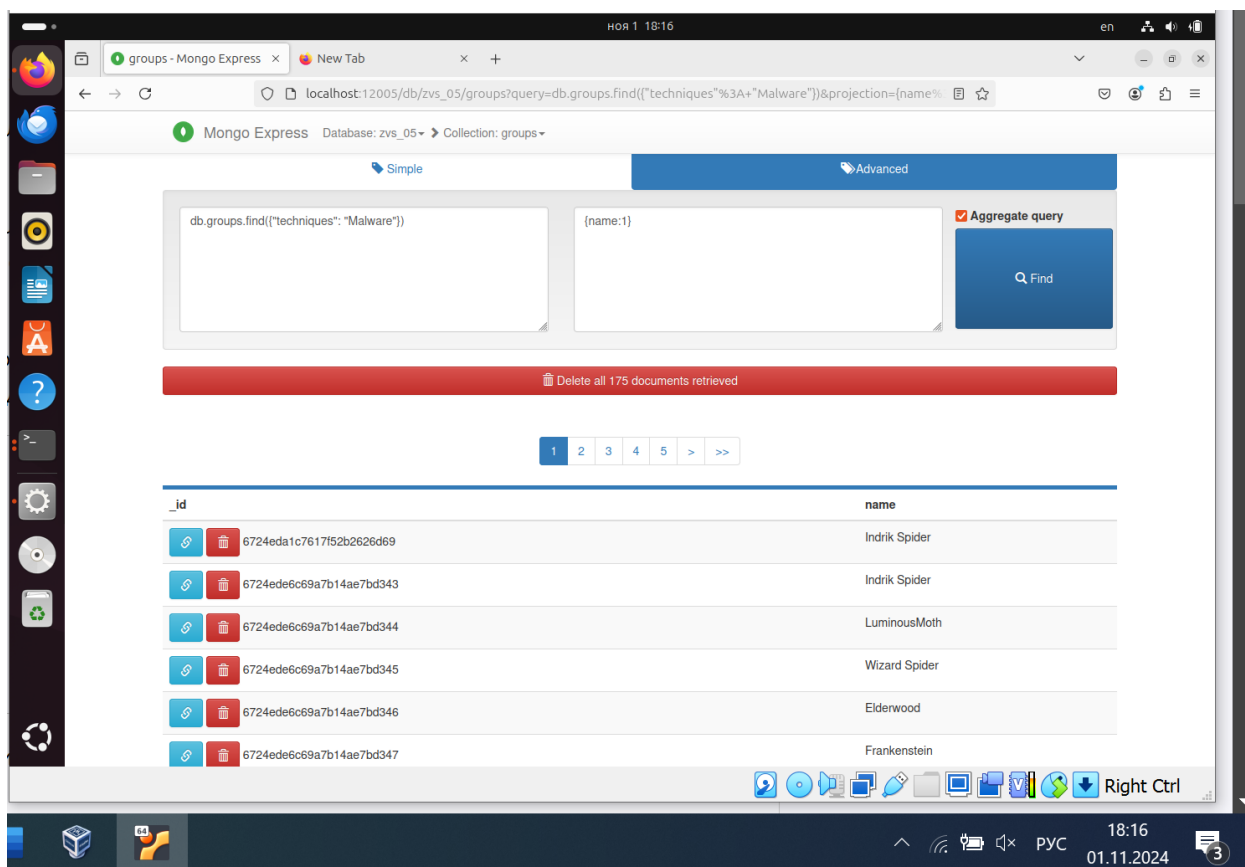


```
1 from mitreattack.stix20 import MitreAttackData
2 from pymongo import MongoClient
3 import json
4
5 client= MongoClient(host="localhost",port=27017, username='root', password='example')
6 db = client['zvs_05']
7 collection = db['groups']
8
9 mad=MitreAttackData('enterprise-attack.json')
10 groups = mad.get_groups()
11
12 for group in groups:
13     group_json= json.loads(str(group))
14     techniques_used = mad.get_techniques_used_by_group(group.id)
15     group_json['techniques'] = []
16     for technique in techniques_used:
17         group_json['techniques'].append(technique['object']['name'])
18     software_used = mad.get_software_used_by_group((group.id))
19     group_json['software'] = []
20     for software in software_used:
21         group_json['software'].append(software['object']['name'])
22     collection.insert_one(group_json)
```

Загрузите с помощью программы/скрипта данные в MongoDB.



Выполните несколько поисковых запросов в данной коллекции. Например: поиск групп, которые используют определенную технику или ПО; поиск группы по названию.



С помощью запроса в MongoDB выведите списки техник и ПО, используемых группировками по убыванию частоты использования (название техники – сколько групп использует; название ПО – сколько групп использует).

groups - Mongo Express x New Tab x Мессенджер x +

localhost:12005/db/zvs_05/groups?query=[%0D%0A++{%24unwind%3A+%24techniques*+}%2C%0D%0A++{+}]

Mongo Express Database: zvs_05 Collection: groups

Viewing Collection: groups

New Document New Index

Simple Advanced

```
{ $unwind: "$techniques",
  { $group: { _id: "$techniques", count: { $sum: 1 } } },
  { $sort: { count: -1 } }
}
```

Projection

Aggregate query Find

Delete all 435 documents retrieved

1 2 3 4 5 > >>

_id	count
Ingress Tool Transfer	83
Malicious File	83
Spearphishing Attachment	81

Right Ctrl 19:24 01.11.2024 2

groups - Mongo Express x New Tab x Мессенджер x +

localhost:12005/db/zvs_05/groups?query=[%0D%0A++{%24unwind%3A+%24software*+}%2C%0D%0A++{+}]

Mongo Express Database: zvs_05 Collection: groups

Viewing Collection: groups

New Document New Index

Simple Advanced

```
{ $unwind: "$software",
  { $group: { _id: "$software", count: { $sum: 1 } } },
  { $sort: { count: -1 } }
}
```

Projection

Aggregate query Find

Delete all 529 documents retrieved

1 2 3 4 5 > >>

_id	count
Mimikatz	49
PsExec	36
Net	31

Right Ctrl 19:25 01.11.2024 3

Выберите две техники и две программы, используемых АРТ-группами, из выборки.

Техники: WindowsCommandShell, PowerShell

ПО – Cobalt Strike, Empire

Опишите две выбранные техники (название, описание техники; ссылка на страницу техники на любом из двух ресурсов из п. 12).

WindowsCommandShell

Злоумышленники могут использовать командную оболочку Windows для выполнения команд. Командная оболочка Windows ([cmd](#)) является основным командным интерфейсом в системах Windows. Командный интерфейс Windows можно использовать для управления практически любым аспектом системы, при этом для разных наборов команд требуются разные уровни разрешений. Командный интерфейс можно вызывать удалённо с помощью [удалённых служб](#), таких как [SSH](#).

<https://attack.mitre.org/techniques/T1059/003/>

PowerShell

Злоумышленники могут использовать команды и скрипты PowerShell для выполнения действий. PowerShell — это мощный интерактивный интерфейс командной строки и среда разработки сценариев, включенная в операционную систему Windows.

<https://attack.mitre.org/techniques/T1059/001/>

Опишите две выбранных программы (название ПО; для чего и как используется; ссылка на ПО, если есть в открытом доступе – часто размещены на GitHub)

Cobalt Strike

Cobalt Strike — это программное обеспечение для моделирования угроз, которое используется красными командами и тестировщиками проникновения для симуляции продвинутых угроз и выполнения целевых атак.

Оно сочетает различные инструменты и техники, такие как социальная инженерия, обфускация сети и выполнение вредоносного кода, для оценки защиты организации.

<https://www.cobaltstrike.com/>

Empire

Empire — это **фреймворк для пост-эксплуатации**, который сочетает в себе возможности Powershell и Python и позволяет развертывать модули пост-эксплуатации, такие как кейлоггеры или Mimikatz, в целевых системах.

<https://github.com/EmpireProject/Empire>