МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное автономное образовательное учреждение высшего образования

«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»

КАФЕДРА №  43

ОТЧЁТ

ЗАЩИЩЁН С ОЦЕНКОЙ

ПРЕПОДАВАТЕЛЬ

### Старший преподаватель                                                      Поляк М.Д.

должность, уч. Степень, звание   подпись, дата                    инициалы, фамилия

ОТЧЁТ О ЛАБОРАТОРНОЙ РАБОТЕ №1.

Работа с текстовыми потоками в командном интерпретаторе Bash

по курсу: [Операционные системы](https://pro.guap.ru/inside/students/subjects/3154495)

РАБОТУ ВЫПОЛНИЛ

СТУДЕНТ ГР. 4136                                                                                Бобрович Н. С.

                                                                         подпись, дата                      инициалы, фамилия

Санкт-Петербург 2024

1. **Цель работы:**

Изучение принципов работы с командным интерпретатором GNU/Linux и основ обработки текстовых файлов с помощью команд grep, awk, sed.

1. **Индивидуальное задание:**

Написать скрипт с использованием grep, sed, awk (необходимо использовать не менее одной из указанных утилит; использовать все три необязательно) для переконвертирования данных в формат XML со следующей структурой:

<dnslog>

<row>

<timestamp>Отметка времени, когда поступил запрос</timestamp>

<client\_ip>IP адрес пользователя</client\_ip>

<client\_port>Порт пользователя</client\_port>

</row>

<row>

<timestamp>Отметка времени, когда поступил запрос</timestamp>

<client\_ip>IP адрес пользователя</client\_ip>

<client\_port>Порт пользователя</client\_port>

</row>

<row>

...

</row>

</dnslog>

Текст внутри тегов <timestamp>, <client\_ip> и <client\_port> необходимо заменить соответствующими значениями из логов. Для отступов использовать символ табуляции (4 пробела в примере выше = одна табуляция). Сохранить в файле results.txt результат применения написанного скрипта к первым 20 строкам файла dns-tunneling.log.  
В переменную VAR\_2 записать количество записей в получившемся текстовом файле, которые содержат запросы от пользователей с IP-адресами из подсети 10.1.\*.\*.

1. **Описание входных данных:**

Файл dns-tunneling.log содержит логи [DNS-сервера](https://ru.wikipedia.org/wiki/DNS), представленные в виде текстового файла, в котором каждая строка соответствует записи о поступившем на вход сервера запросе. В логах сохраняются следующие параметры запроса, разделённые символом табуляции:

1. Название провайдера телекоммуникационных услуг: character array,
2. Название узла, на котором хранятся данные: character array,
3. Порядковый номер запроса: long,
4. Отметка времени, когда поступил запрос: два числа long, разделенных точкой; первое число – количество секунд, прошедших с 1 января 1970 года; второе число – количество микросекунд; т.е. фактически это тип данных float,
5. IP-адрес пользователя: character array,
6. Порт пользователя: int,
7. Локальный IP-адрес, на который поступил запрос: character array,
8. Локальный порт: int,
9. Название оборудования DNS-сервера: character array,
10. Класс запроса: int,
11. [Тип запроса](https://ru.wikipedia.org/wiki/%D0%A2%D0%B8%D0%BF%D1%8B_%D1%80%D0%B5%D1%81%D1%83%D1%80%D1%81%D0%BD%D1%8B%D1%85_%D0%B7%D0%B0%D0%BF%D0%B8%D1%81%D0%B5%D0%B9_DNS): int,
12. Код возвращаемого значения: int,
13. Флаги: int,
14. Вспомогательный идентификатор: int,
15. Запрашиваемый URL: character array,
16. Зона: character array,
17. Вспомогательное поле 1: character array,
18. Вспомогательное поле 2: character array,
19. Вспомогательное поле 3: character array,
20. Вспомогательное поле 4: character array,
21. Ответ сервера: character array,
22. Вспомогательное поле 5: character array,
23. Вспомогательное поле 6: character array,
24. Длина ответа: int
25. **Результат выполнения работы:**

<dnslog>

<row>

<timestamp>1451001600.446786</timestamp>

<client\_ip>10.119.76.168</client\_ip>

<client\_port>42487</client\_port>

</row>

<row>

<timestamp>1451001600.059012</timestamp>

<client\_ip>10.116.74.176</client\_ip>

<client\_port>41280</client\_port>

</row>

<row>

<timestamp>1451001600.473921</timestamp>

<client\_ip>10.47.144.132</client\_ip>

<client\_port>43301</client\_port>

</row>

<row>

<timestamp>1451001600.562429</timestamp>

<client\_ip>10.119.76.168</client\_ip>

<client\_port>45399</client\_port>

</row>

<row>

<timestamp>1451001600.634430</timestamp>

<client\_ip>10.47.144.132</client\_ip>

<client\_port>43301</client\_port>

</row>

<row>

<timestamp>1451001600.756670</timestamp>

<client\_ip>10.119.76.168</client\_ip>

<client\_port>50476</client\_port>

</row>

<row>

<timestamp>1451001600.105204</timestamp>

<client\_ip>10.47.144.132</client\_ip>

<client\_port>43301</client\_port>

</row>

<row>

<timestamp>1451001600.154305</timestamp>

<client\_ip>10.47.144.132</client\_ip>

<client\_port>43301</client\_port>

</row>

<row>

<timestamp>1451001600.225852</timestamp>

<client\_ip>10.47.144.132</client\_ip>

<client\_port>43301</client\_port>

</row>

<row>

<timestamp>1451001600.232628</timestamp>

<client\_ip>10.119.76.168</client\_ip>

<client\_port>59208</client\_port>

</row>

<row>

<timestamp>1451001600.785342</timestamp>

<client\_ip>10.47.144.132</client\_ip>

<client\_port>43301</client\_port>

</row>

<row>

<timestamp>1451001601.164861</timestamp>

<client\_ip>10.47.144.132</client\_ip>

<client\_port>43301</client\_port>

</row>

<row>

<timestamp>1451001601.400704</timestamp>

<client\_ip>10.119.76.168</client\_ip>

<client\_port>51056</client\_port>

</row>

<row>

<timestamp>1451001601.504543</timestamp>

<client\_ip>10.47.144.132</client\_ip>

<client\_port>43301</client\_port>

</row>

<row>

<timestamp>1451001601.858664</timestamp>

<client\_ip>10.116.74.176</client\_ip>

<client\_port>41280</client\_port>

</row>

<row>

<timestamp>1451001601.373581</timestamp>

<client\_ip>10.47.144.132</client\_ip>

<client\_port>43301</client\_port>

</row>

<row>

<timestamp>1451001601.584901</timestamp>

<client\_ip>10.47.144.132</client\_ip>

<client\_port>43301</client\_port>

</row>

<row>

<timestamp>1451001601.883377</timestamp>

<client\_ip>10.47.144.132</client\_ip>

<client\_port>43301</client\_port>

</row>

<row>

<timestamp>1451001601.998364</timestamp>

<client\_ip>10.116.74.176</client\_ip>

<client\_port>41280</client\_port>

</row>

<row>

<timestamp>1451001602.058561</timestamp>

<client\_ip>10.116.74.176</client\_ip>

<client\_port>41280</client\_port>

</row>

</dnslog>

1. **Исходный код программы с комментариями:**

#!/usr/bin/env bash

# edit the code below and add your code

# отредактируйте код ниже и добавьте свой

# Переменная с номером варианта (константа):

TASKID=3

# Дополнительные переменные (должны вычисляться динамически):

VAR\_1=$(wc -l < dns-tunneling.log)

# Используем awk для обработки каждой строки лога

awk -F'\t' 'BEGIN {print "<dnslog>"}

{

print "<row>"

print "\t<timestamp>" $4 "</timestamp>"

print "\t<client\_ip>" $5 "</client\_ip>"

print "\t<client\_port>" $6 "</client\_port>"

print "</row>"

}

END {print "</dnslog>"}' dns-tunneling.log | head -n 101 > results.txt

echo "</dnslog>" >> results.txt

# Подсчитываем количество записей с IP-адресами из подсети 10.1.\*.\*

VAR\_2=$(grep -c "<client\_ip>10\.1\." results.txt)

1. **Выводы:**

Изучение принципов работы с командным интерпретатором GNU/Linux и основ обработки текстовых файлов с помощью команд grep, awk, sed.