ГУАП КАФЕДРА № 43

ОТЧЕТ

ЗАЩИЩЕН С ОЦЕНКОЙ ПРЕПОДАВАТЕЛЬ

ст. преп. М.Д. Поляк

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

ОТЧЕТ О ЛАБОРАТОРНОЙ РАБОТЕ №1

СОЗДАНИЕ ПОЛЬЗОВАТЕЛЬСКИХ ФУНКЦИЙ В ПРИЛОЖЕНИИ EXCEL

по курсу: ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

РАБОТУ ВЫПОЛНИЛ

СТУДЕНТ ГР. № 4936 Е. И. Белов

подпись, дата инициалы, фамилия

Санкт-Петербург 2022

**Цель работы:**

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

**Индивидуальное задание:**

1. 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.\*.\*.

**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, разделенные 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

**Результат выполнения работы:**

Файл results.txt:

<dnslog>

<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>

<row>

<timestamp>1451001602.615097</timestamp>

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

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

</row>

<row>

<timestamp>1451001602.888733</timestamp>

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

<client\_port>55241</client\_port>

</row>

<row>

<timestamp>1451001601.958628</timestamp>

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

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

</row>

<row>

<timestamp>1451001602.074063</timestamp>

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

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

</row>

<row>

<timestamp>1451001602.118675</timestamp>

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

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

</row>

<row>

<timestamp>1451001602.264108</timestamp>

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

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

</row>

<row>

<timestamp>1451001602.318492</timestamp>

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

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

</row>

<row>

<timestamp>1451001602.318508</timestamp>

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

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

</row>

<row>

<timestamp>1451001602.398793</timestamp>

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

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

</row>

<row>

<timestamp>1451001682.894400</timestamp>

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

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

</row>

<row>

<timestamp>1451001682.058516</timestamp>

<client\_ip>10.1.178.208</client\_ip>

<client\_port>36004</client\_port>

</row>

<row>

<timestamp>1451001682.098897</timestamp>

<client\_ip>10.1.178.208</client\_ip>

<client\_port>36004</client\_port>

</row>

<row>

<timestamp>1451001682.098881</timestamp>

<client\_ip>10.1.178.208</client\_ip>

<client\_port>36004</client\_port>

</row>

<row>

<timestamp>1451001682.198274</timestamp>

<client\_ip>10.1.178.208</client\_ip>

<client\_port>36004</client\_port>

</row>

<row>

<timestamp>1451001682.396615</timestamp>

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

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

</row>

</dnslog>

**Исходный код программы с комментариями:**

#!/usr/bin/env bash

# edit the code below and add your code

# отредактируйте код ниже и добавьте свой

head -n 20 dns-tunneling.log | awk 'BEGIN {print "<dnslog>";}

{print "<row>\n\t<timestamp>"$4"</timestamp>\n\t<client\_ip>"$5"</client\_ip>\n\t<client\_port>"$6"</client\_port>\n</row>";}

END {print "</dnslog>";}' > results.txt

# Переменная с номером варианта (константа):

TASKID=2

# Дополнительные переменные (должны вычисляться динамически):

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

VAR\_2=$(cat results.txt | grep '10\.1\.' -c)

**Выводы:**

В ходе работы были изучены принципы работы с командным интерпретатором GNU/Linux и основы обработки текстовых файлов с помощью команд grep и awk.