ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Санкт-Петербургский государственный университет телекоммуникаций

им. проф. М.А. Бонч-Бруевича***»***

(СПБГУТ)

***\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***

Факультет ИКСС

Кафедра ЗСС

Курсовая работа

по дисциплине:

**«Цифровая криминалистика»**

на тему:

**«Определение последовательности действий атакующего путем анализа логов»**

Выполнил:

Зеличенок И.Ю., ИКТБ-98м

Проверила:

Федорченко Е.В

Санкт-Петербург

2020г.

**Оглавление**

Элементы оглавления не найдены.

# **Задание на курсовую работу**

Определить последовательность действий атакующего путем анализа логов событий Windows и оповещений Suricata.

# **Подзадачи**

1. Скачать логи Win Events и Suricata\_alert с сайта: <http://mirrors.rit.edu/cptc/2018/t1/> .
2. Определить последовательность действий команды, сопоставив события Windows и алерты suricata
3. Проанализировать действия команды и предположить уровень ее квалификации.

# **Обзор логов**

Логи предстают перед нами в следующем виде (Рис. 1, 2):

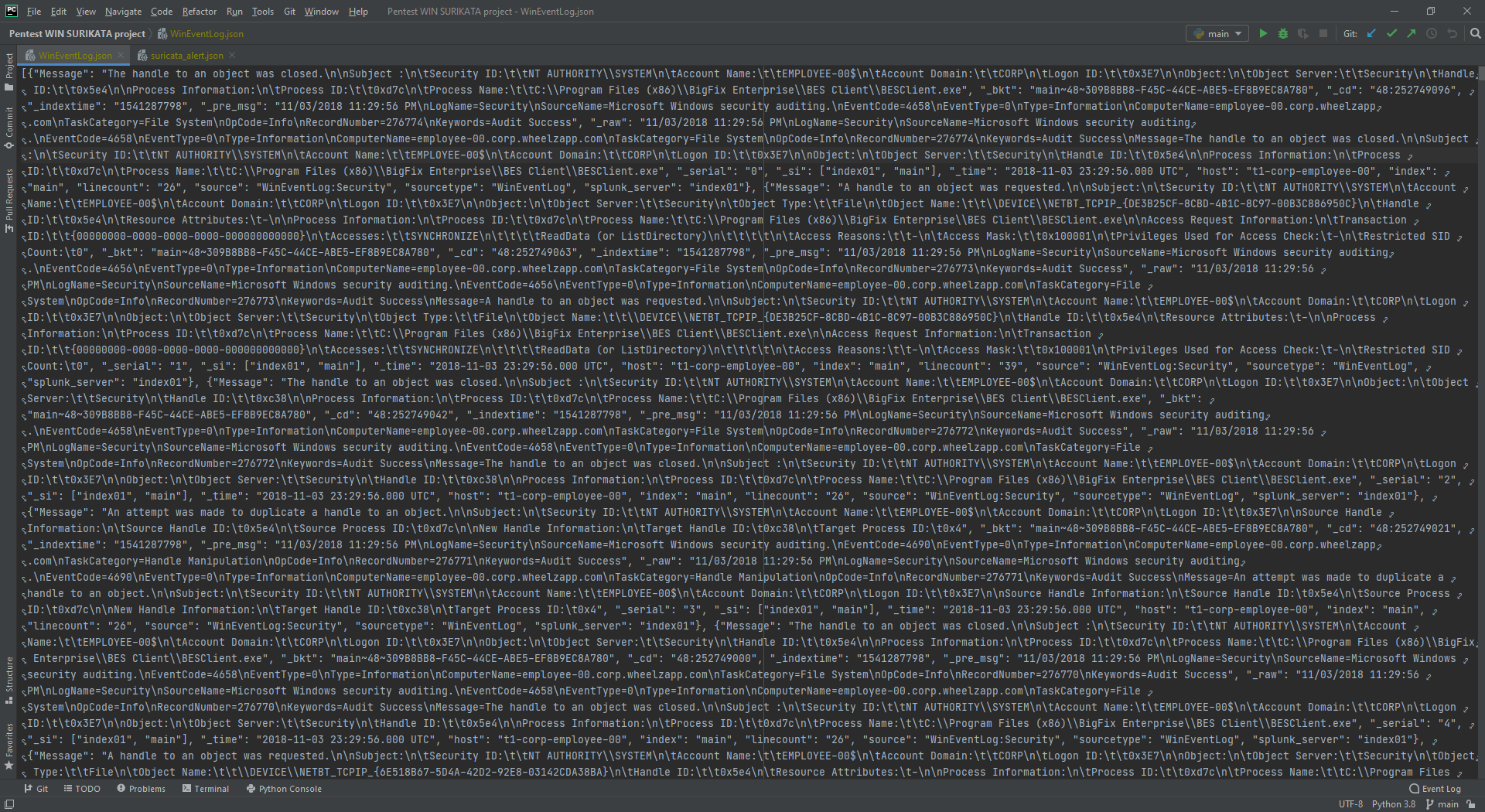


Рис. 1 Данные внутри файла WinEventLog.json.

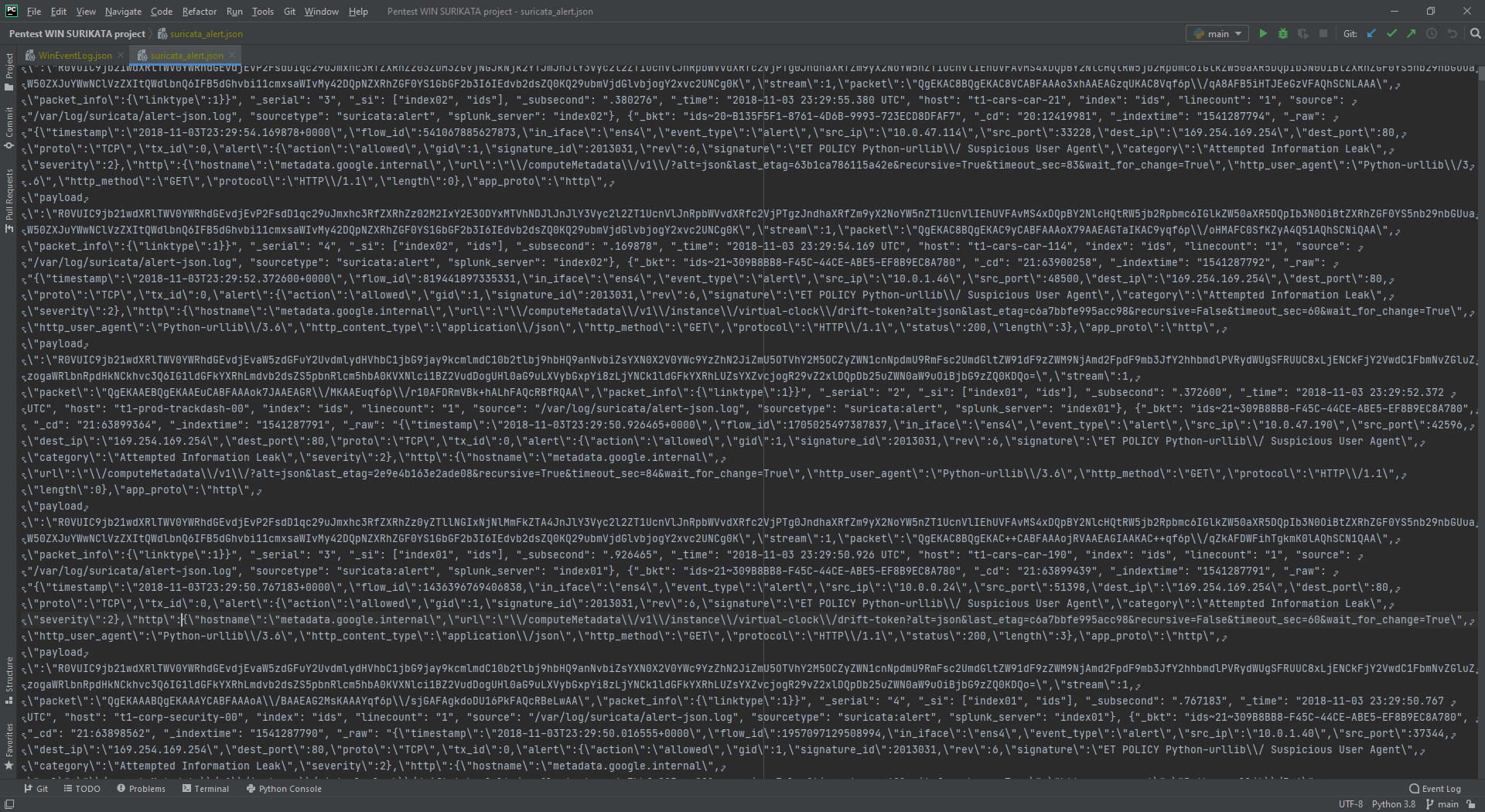


Рис. 2 Данные внутри файла suricata\_alert.json.

Для дальнейшего анализа, данные были приведены в читаемый вид средствами отладки используемого интерпретатора.

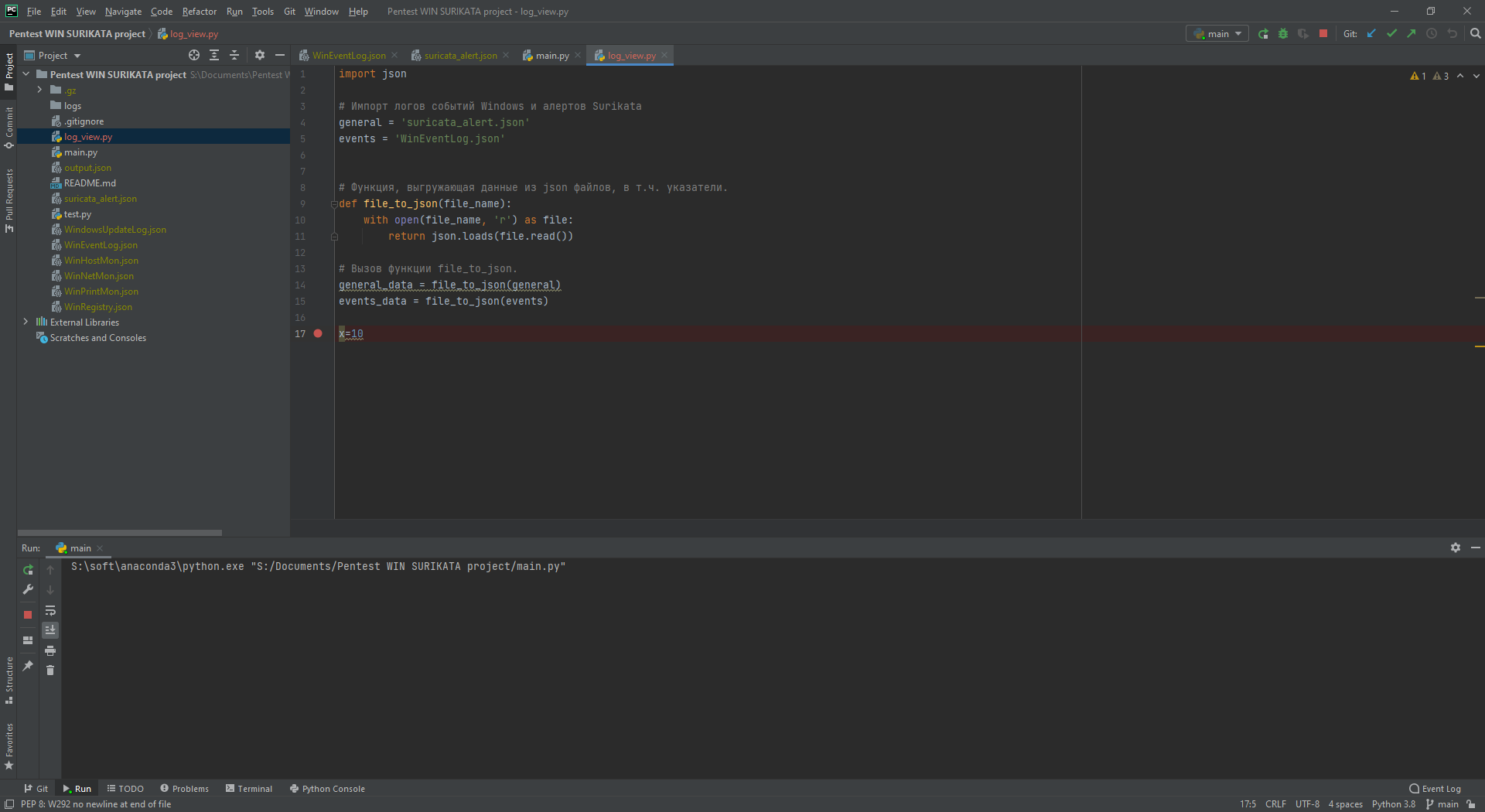


Рис. 3 Код для первичного анализа логов.