**Задание 1.** Провести анализ сетевого трафика (файл .pcap). Решение задания – сдача флага в формате flag{<sometext>}.

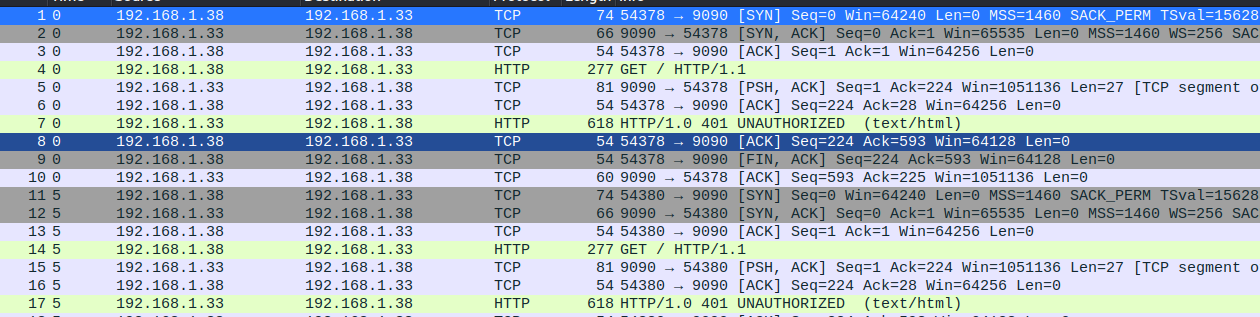
https://disk.yandex.ru/d/ixn37X-Mv9U31g

Ответ: flag{ }

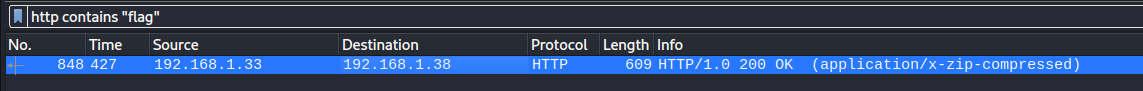
#############################################################################

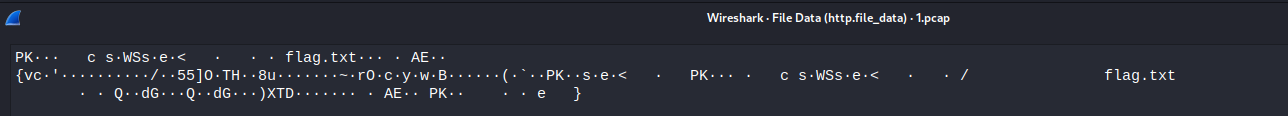
Ответ:

Открываю файл с помощью Wireshark.

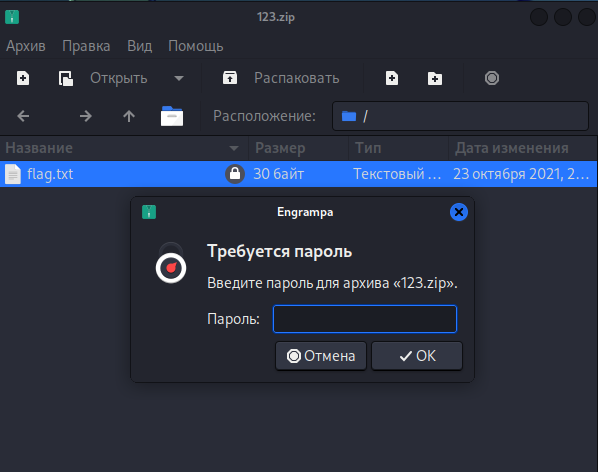


Просмотрев трафик, вижу, что он состоит из одних HTTP и TCP запросов. Их довольно много, поэтому воспользуюсь фильтром, чтобы найти флаг.

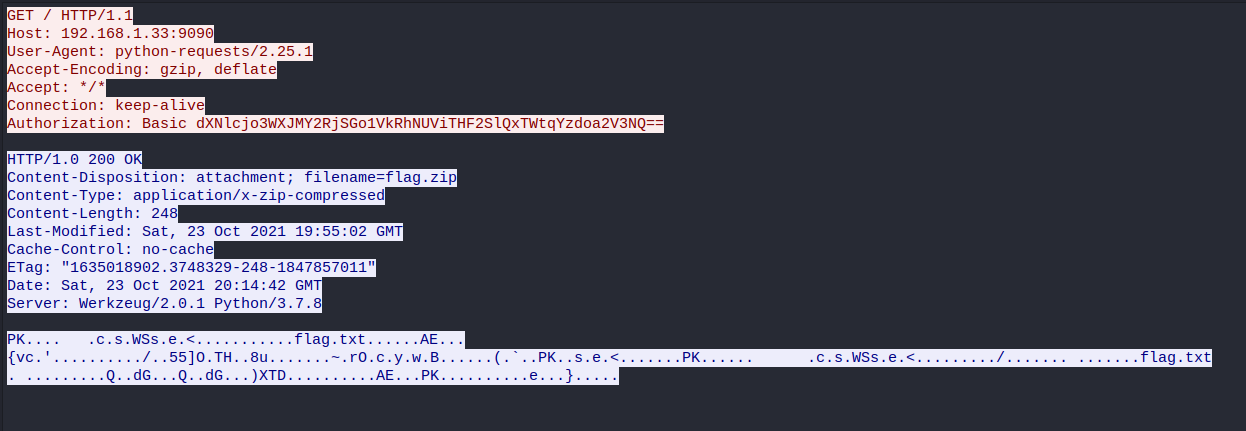




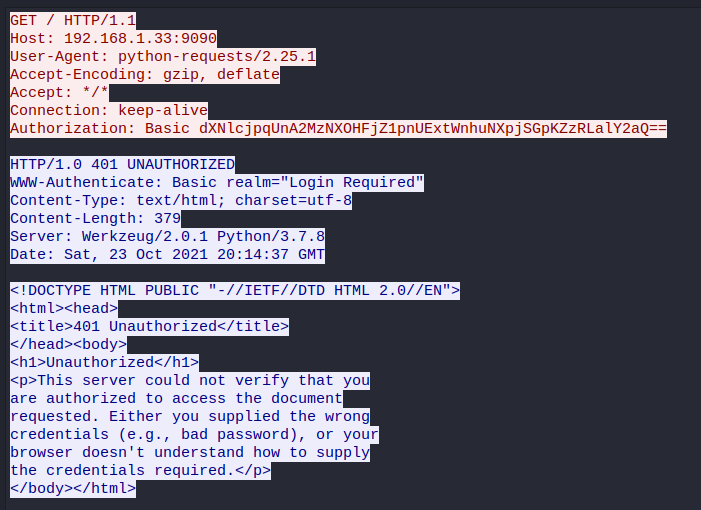
Флаг находится в архиве в текстовом файле flag.txt. Выгружу файл и найду флаг.



Ладно. Так просто до флага не добраться. В трафике встречается и тип text. Возможно, в нём я найду пароль. Пока не получается: пробовал фильтровать по слову «password», отсекать «UNAUTHORIZED». Воспользовался утилитой «zip2john», чтобы взломать архив, но у него ничего не получилось, так же как у «fcrackzip». Вернулся снова к просмотру трафика: решил посмотреть запрос с кодом «200».



Если пройти дальше, то будет уже такое сообщение:



Здесь запросы одинаковые, но различаются в строке «Authorization». Сразу видна кодировка «Base64». Если раскодировать, то получаю такой результат:



Где первое значение – пользователь, а второе – пароль. С этой информацией теперь могу открыть файл «flag.txt»:



#####################################################################################

**Задание 2.** Провести анализ дампа оперативной памяти (файл .raw). Решение задания – сдача флага в формате flag{<sometext>}.

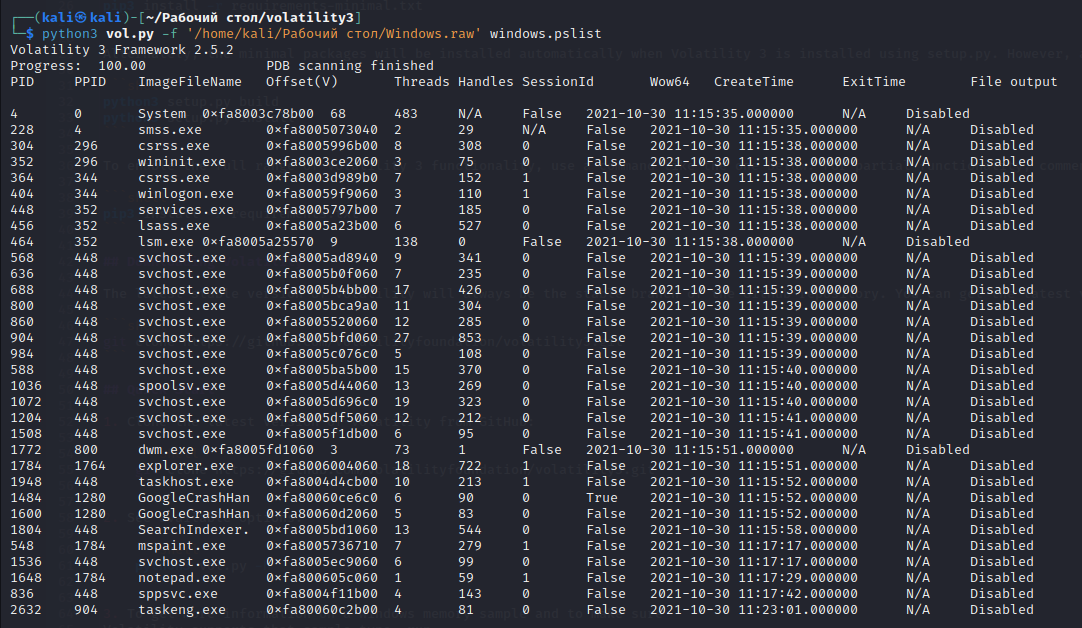
https://disk.yandex.ru/d/ngza0nNybPtWGg

Ответ: FLAG{ }

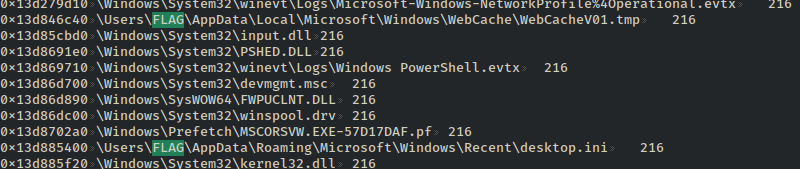
###################################################

Ответ:

Жесть. Не работал с таким раньше, поэтому даже не знал, какая программа нужна для открытия файла. В интернете нашёл разные программы, которые позволят проанализировать дамп, но они устанавливаются только на Windows. Свою основную систему захламлять не захотел, поэтому продолжил искать нужную программу. Мне показалось, что программа «volatility» идеально подходит под задание, но она была написана на python2. Нашёл «volatility3», которая переписана на python3, но некоторые модули на ней не работают. В официальной документации сразу показано применение модуля «windows.pslist»:

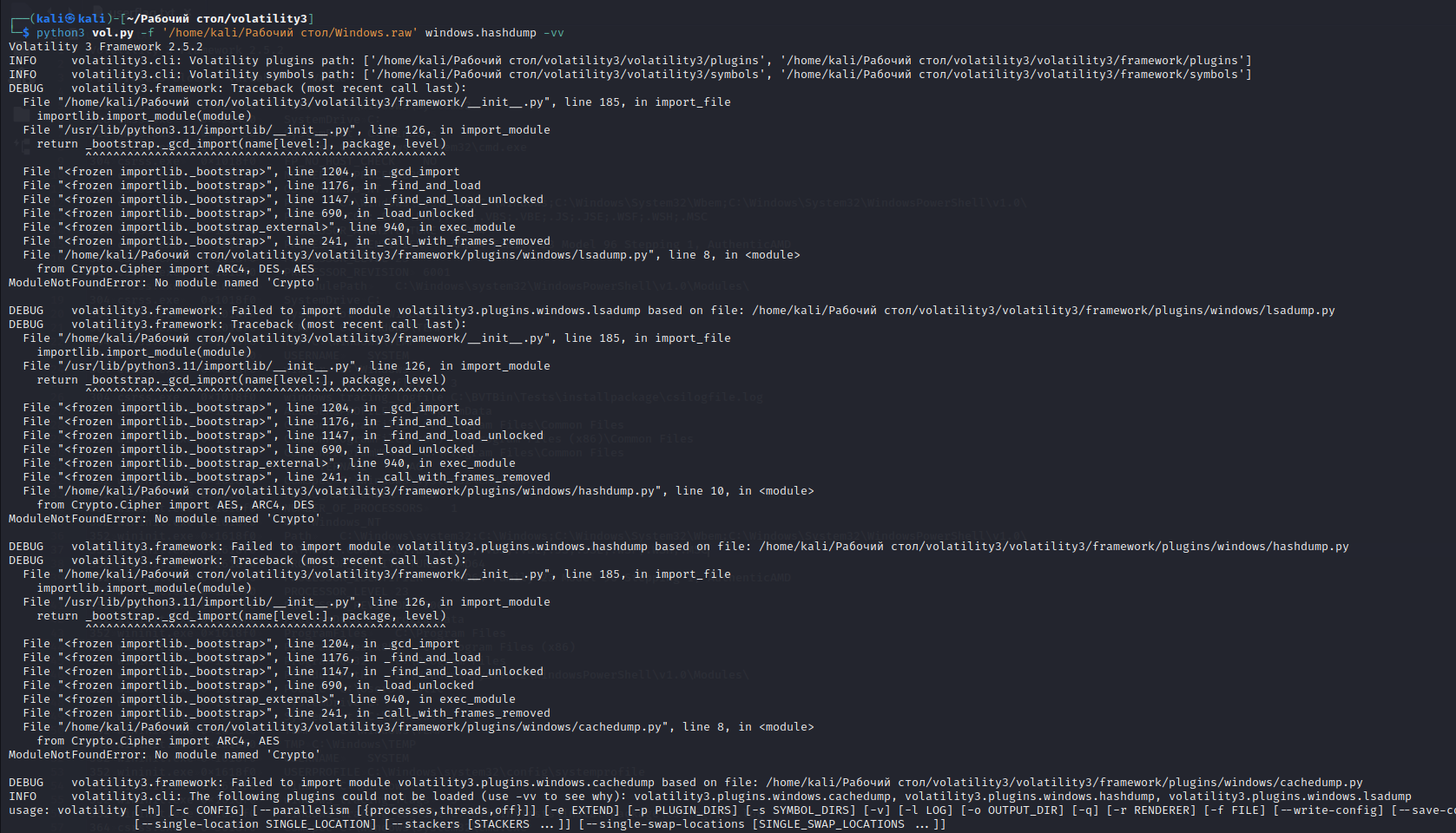


Тогда мне это ничего особого не говорило: «Ну, есть запущенные процессы. И что дальше?» Вытаскивал различные файлы, но это было всё не то:

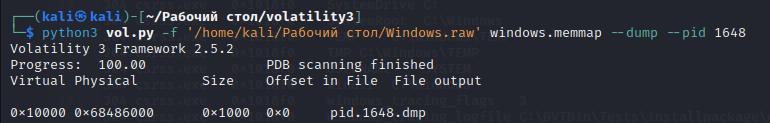




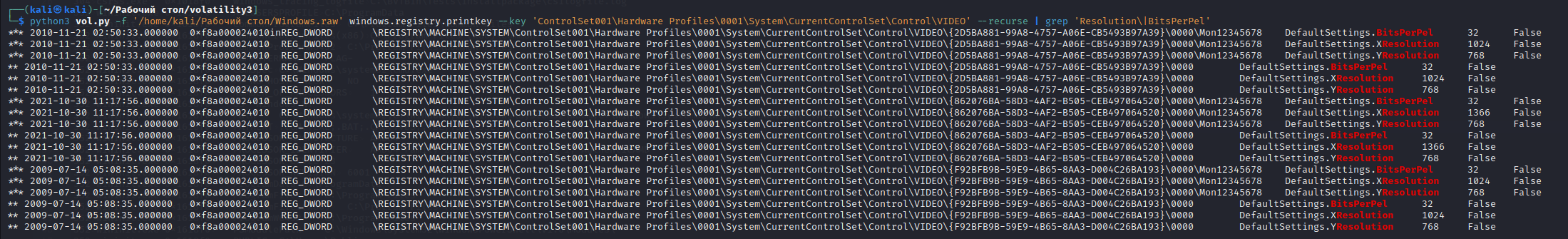
Понял, что и компьютер, и пользователь имеет имя «FLAG». Решил, что тогда пароль будет продолжением этой записи, но модуль «windows.hashdump» выдал ошибку:



Пришлось искать дальше, как достать флаг. Посмотрел видео, как можно вытаскивать скриншот с помощью этой программы. Вспомнил, что при первом вводе команды отображался процесс «notepad.exe». Решил сдампить изображение этого процесса:



Чтобы правильно открыть изображение, нужно узнать на каком разрешении экрана оно открывалось:



Запоминаю нестандартное разрешение: 1366x768. С помощью программы «Gimp» открываю файл «pid.1648.dmp.data». Последнее «.data» добавил, чтобы «Gimp» понял, что это “сырой” файл:



Покрутив ползунки, нашёл флаг. Хоть я и сдампил изображение процесса «notepad.exe», но изображён был «mspaint.exe».