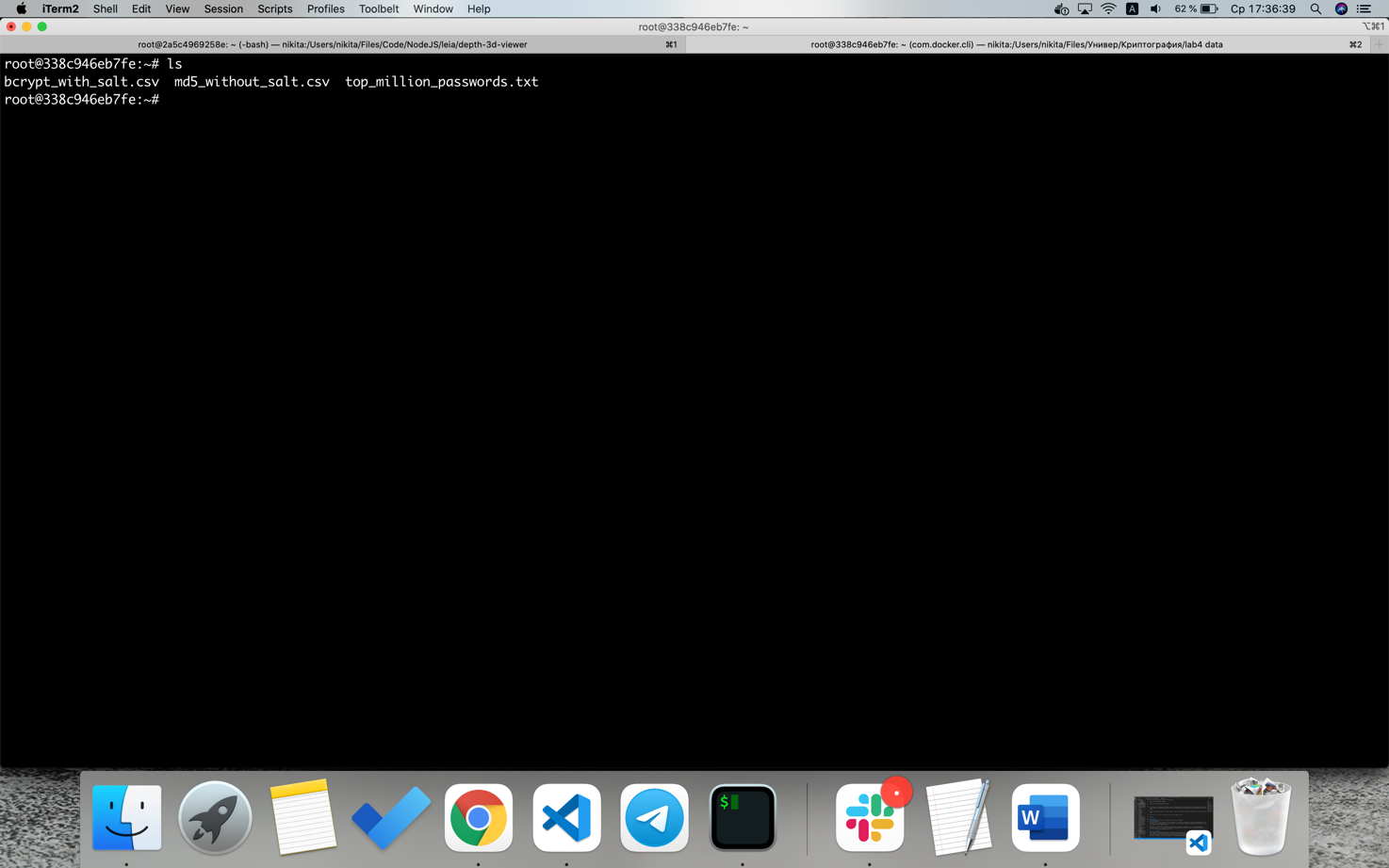
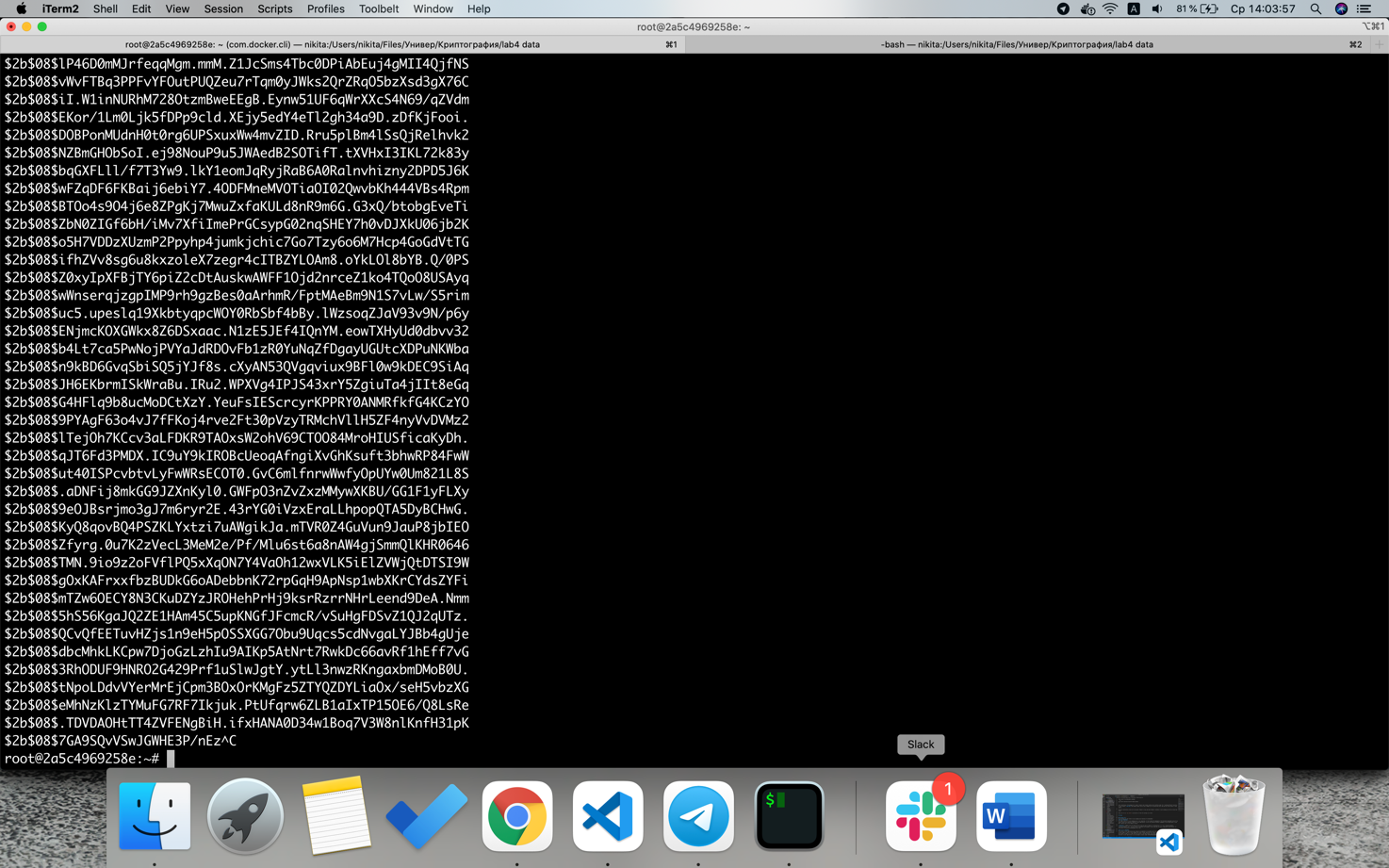
**Отчет 4 лабораторная 2 часть**

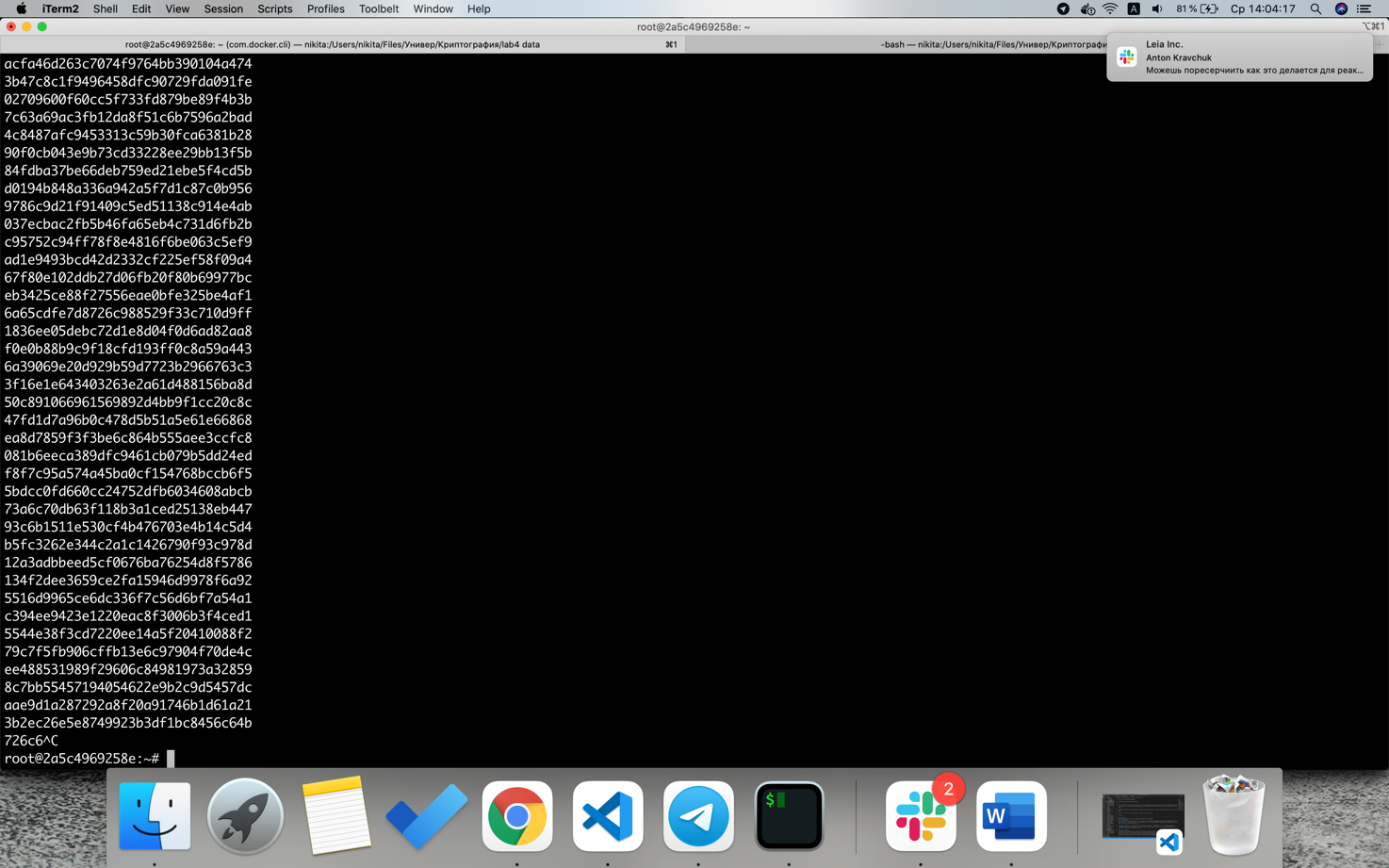
У нас на входе есть два .csv файла: в одном хеши md5 без соли, в другом хеши bcrypt с солью. Также я загрузил словарь с миллионом самых популярных паролей (для Dictionary атаки).



Bcrypt:



Md5:



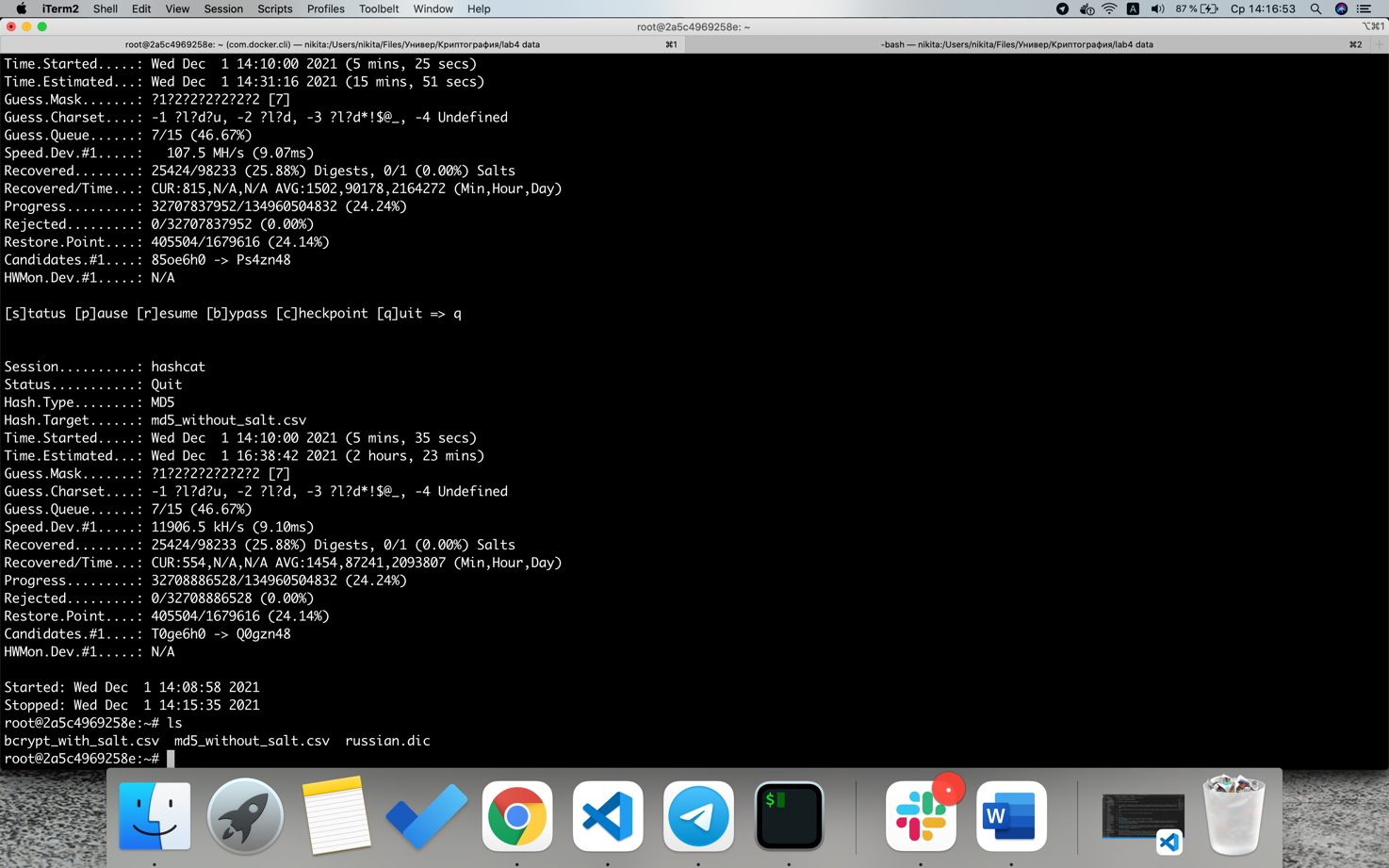
MD5 не рекомендуется для использования в качестве хеш-функции для паролей, т.к. имеет очень высокую скорость перебора, а также высокую вероятность коллизий.

Bcrypt часто используется для хеширования паролей. Единственный его недостаток – быстрый перебор на GPU / спец. микросхемах.

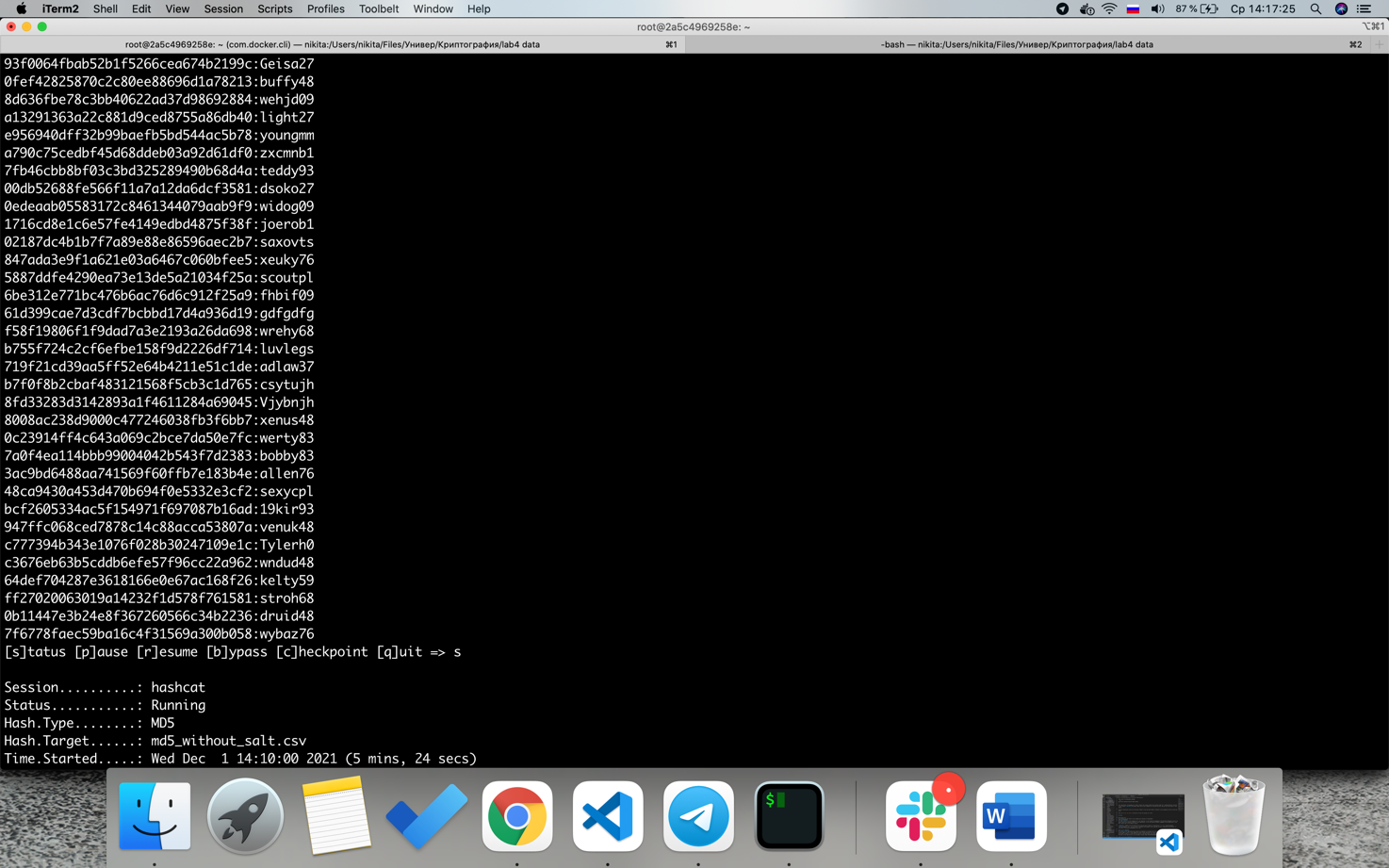
Для взлома выбрал утилиту “hashcat”, которая умеет работать с большим количеством алгоритмов хеширования а также оперировать пятью видами атак.

Для начала попробуем взломать md5 хеши. Метод взлома – brute-force:

hashcat -a 3 -m 0 --force md5\_without\_salt.csv

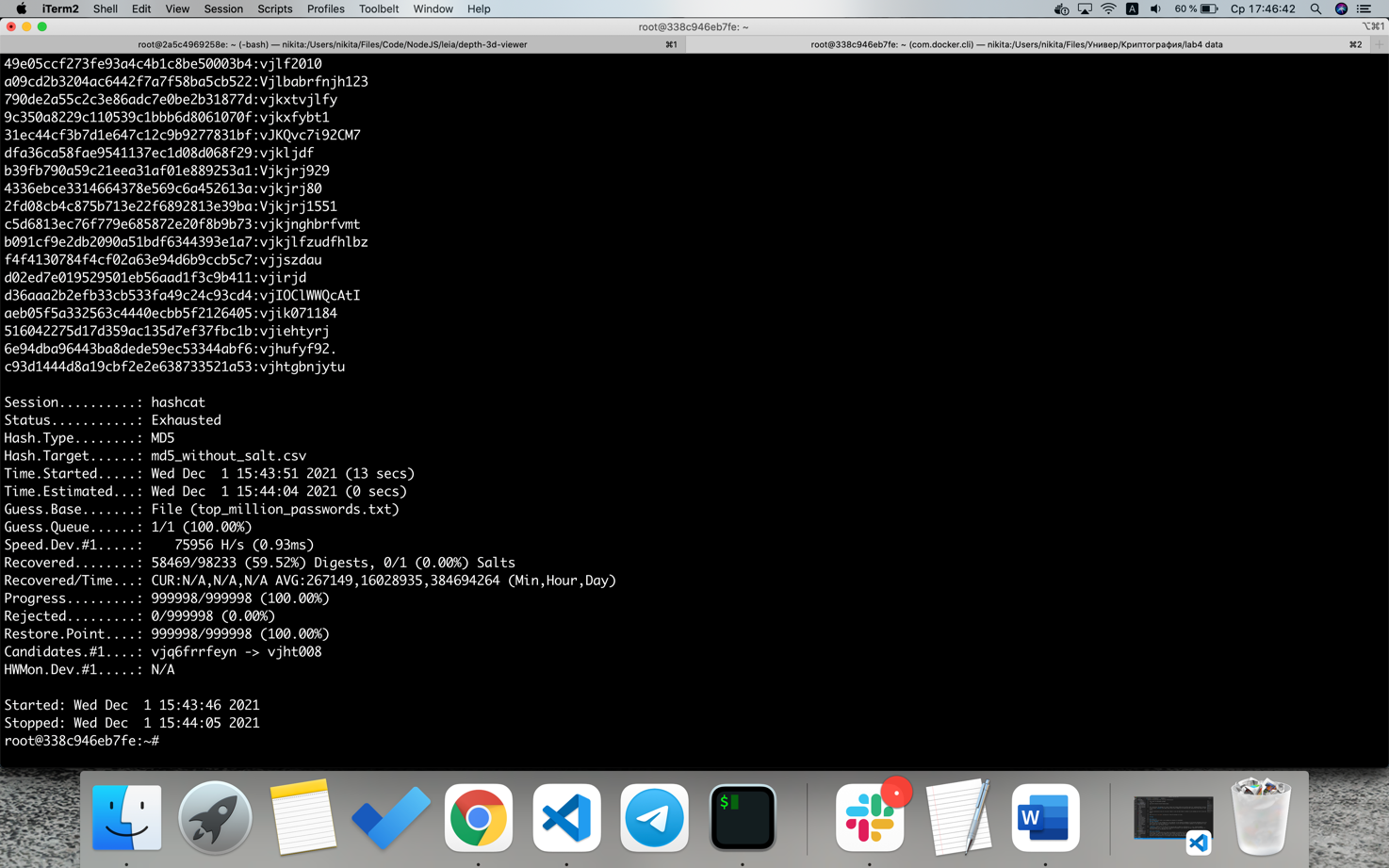


За 5 минут 35 секунд мы перебрали 327088886528 паролей (почти 100 млн. в секунду), было взломано 25424/98233 паролей. Пароли выводились в стандартный поток вывода:



Теперь попробуем метод взлома dictionary:

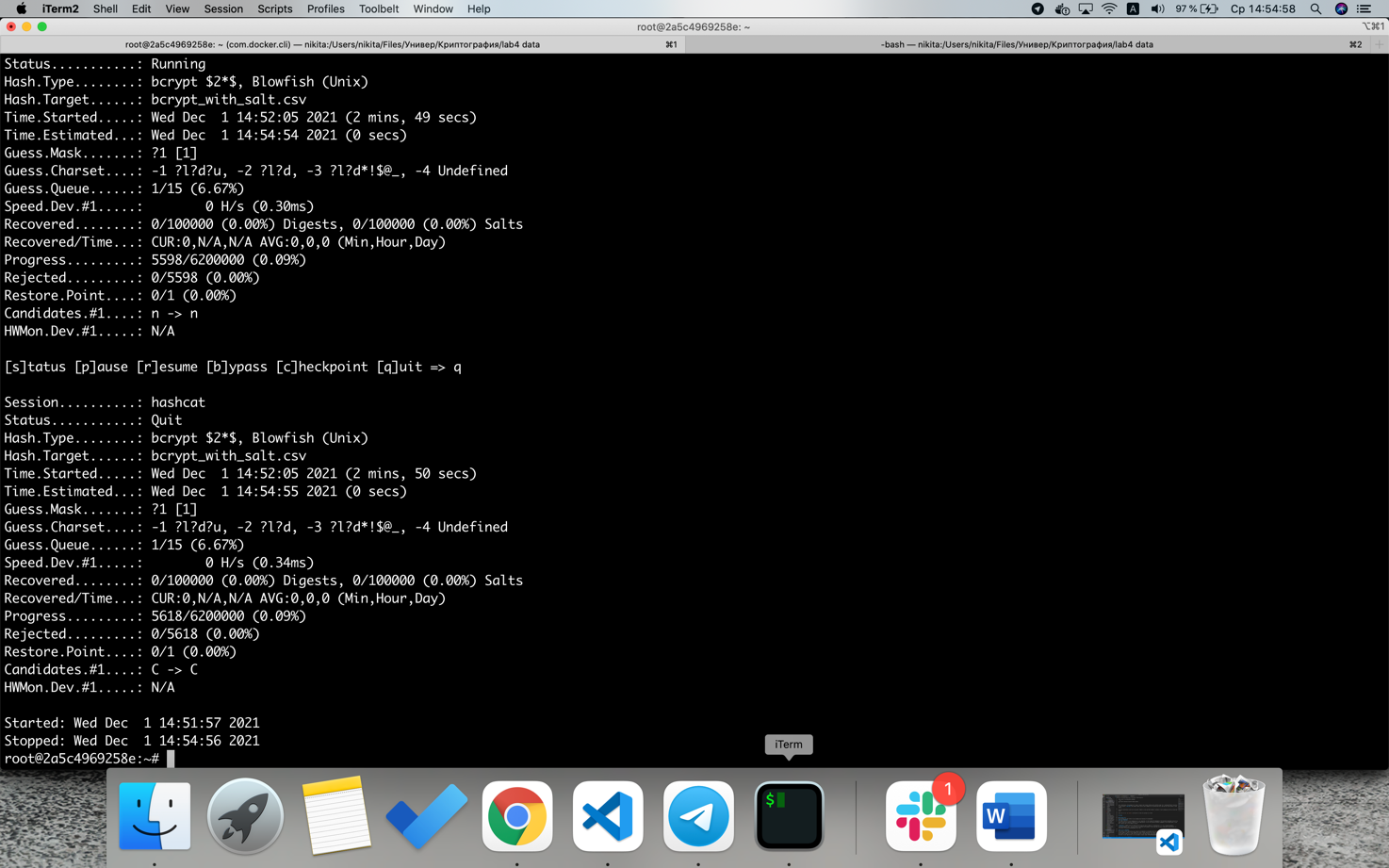
hashcat -a 0 -m 0 --force md5\_without\_salt.csv top\_million\_passwords.txt



За 13 секунд мы перебрали миллион паролей, взломано 58469/98233 (59.52%) паролей.

Теперь попробуем взломать bcrypt с солью через brute-force метод:

hashcat -a 3 -m 3200 --force bcrypt\_with\_salt.csv



Мы видим что скорость перебора сильно упала. За 2 минуты 50 секунд мы перебрали всего 5618 паролей (33 пароля в секунду). Не было взломано ни одного пароля.