***Звіт до лабораторної роботи номер 4, частина 2.***

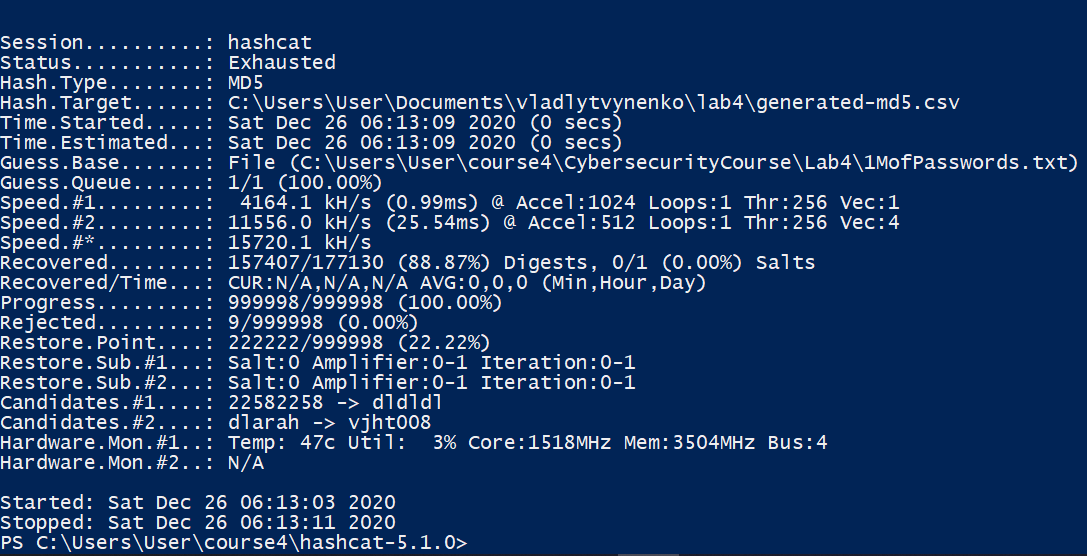
Виконала: Пашко Олеся Віталіївна

Для виконання лабораторної роботи були взяті хеші паролів Литвиненко Владислава, група ІП-72, з репозиторія <https://github.com/vladlytvynenko/crypto-labs/tree/master/lab4>. Дані паролі були захешовані за допомогою MD5, SHA1 та bcrypt.

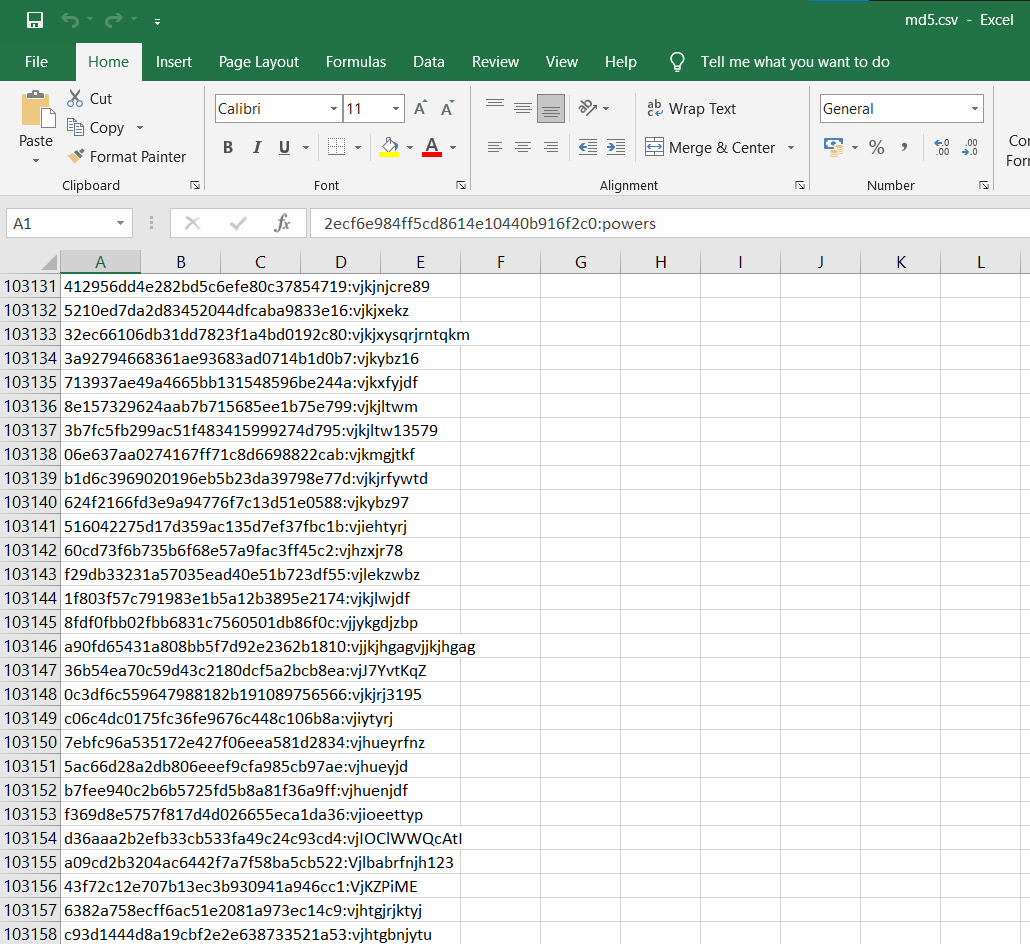
Скористаємось утилітою hashcat та словником із мільйона найпоширеніших слів щоб підібрати паролі, яким відповідають хеші MD5.

Команда для підбору:

./hashcat64.exe --optimized-kernel-enable -w 4 --force -a 0 -m 0 C:\Users\User\Documents\vladlytvynenko\lab4\generated-md5.csv "C:\Users\User\course4\CybersecurityCourse\Lab4\1MofPasswords.txt" -o md5.csv

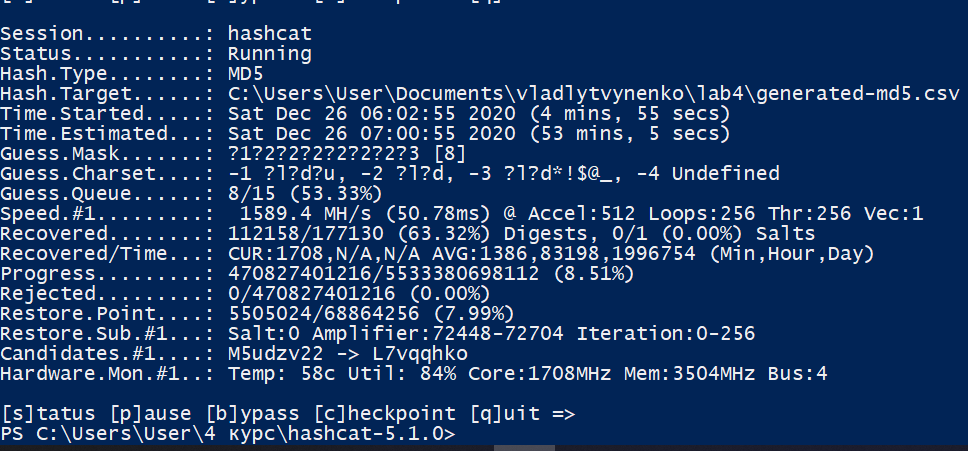


Як бачимо, майже миттєво на відеокарті підібрано 103 158 паролів із 200 000. Це свідчить про слабкість алгоритму хешування MD5. Далі показано самі підібрані паролі.

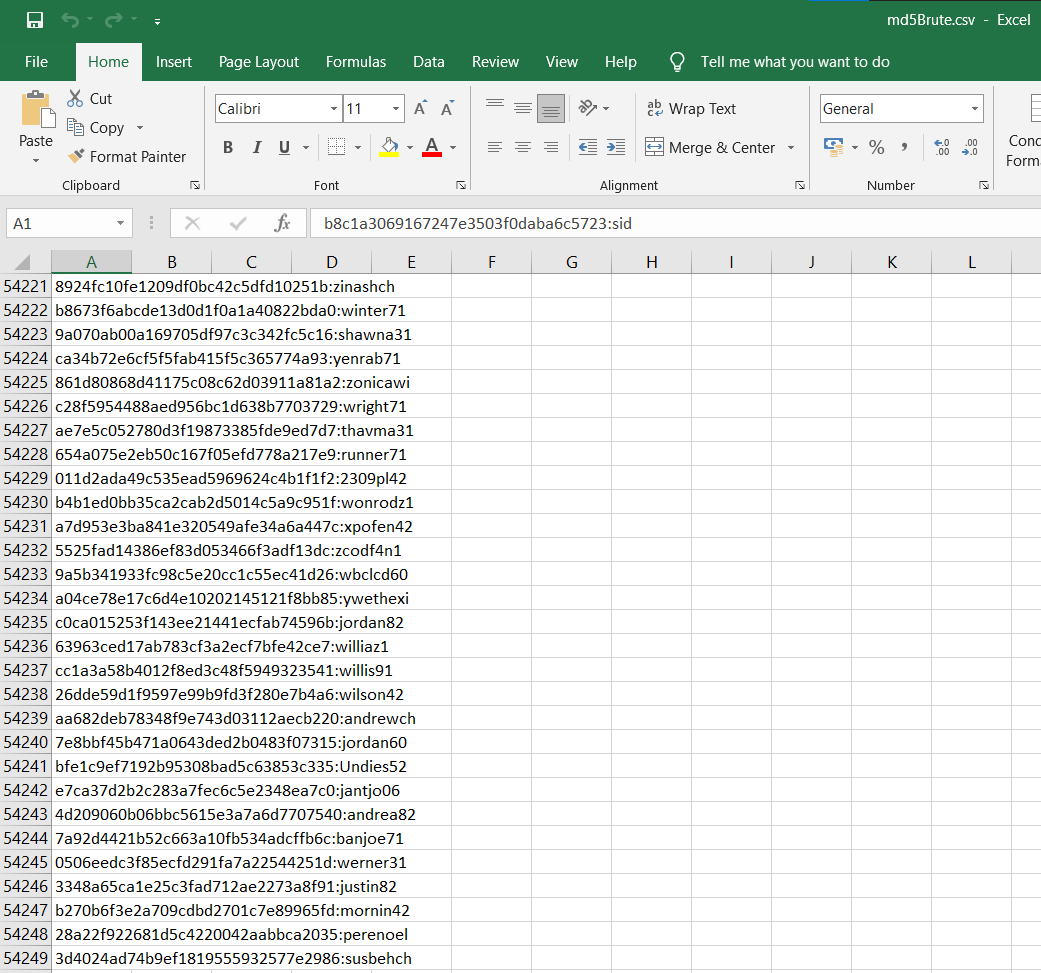


Спробуємо підібрати паролі методом прямого перебору, вже без словника. Відповідна команда:

./hashcat64.exe --optimized-kernel-enable -w 3 -a 3 -m 0 "C:\Users\User\Documents\vladlytvynenko\lab4\generated-md5.csv" -o md5Brute.csv1



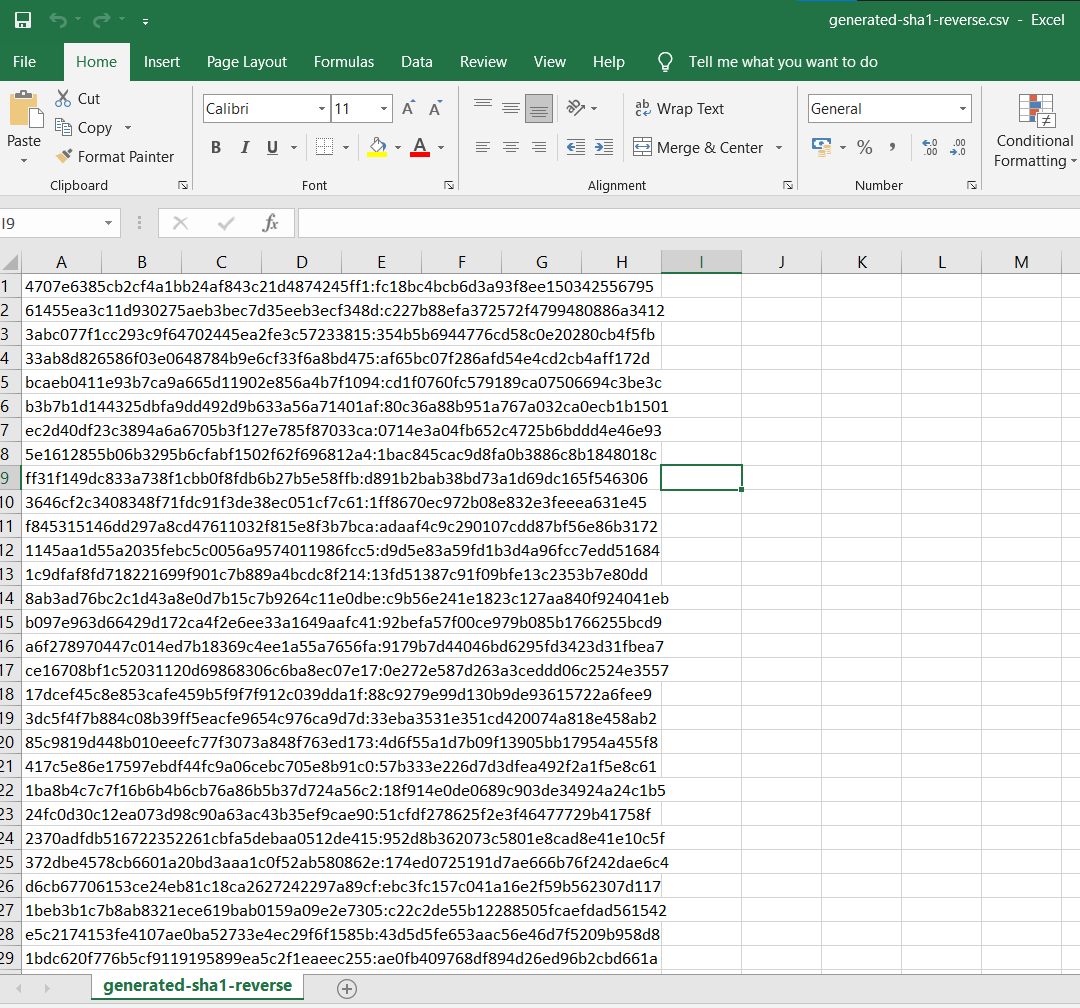
Як бачимо, за 5 хвилин було підібрано лише 54 249 паролів, що значно менше за результати зі словником. Самі паролі наведено нижче.



Далі спробуємо підібрати паролі для SHA1. Файл з репозиторію Влада Литвиненка має не підходящий для hashcat формат, тож я застосувала маленький скріптик для його перетворення.

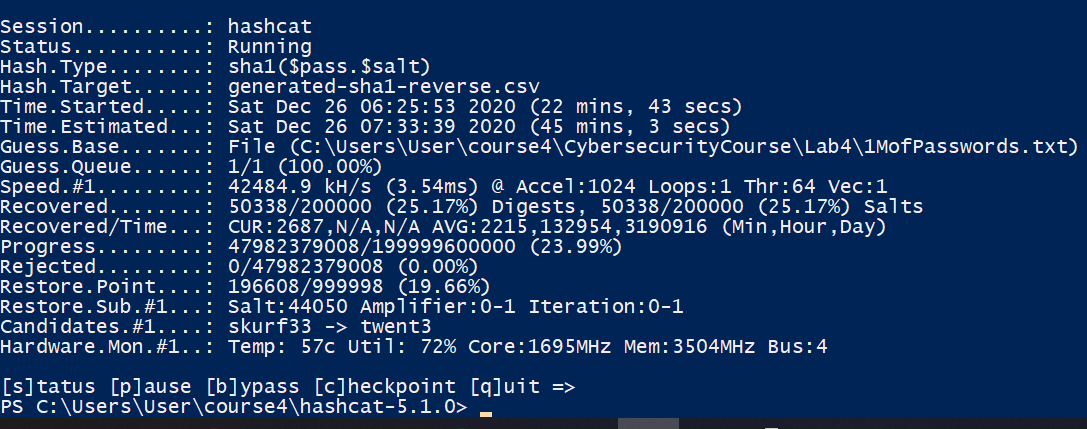


Відповідно відформатовані хеші наведено нижче:

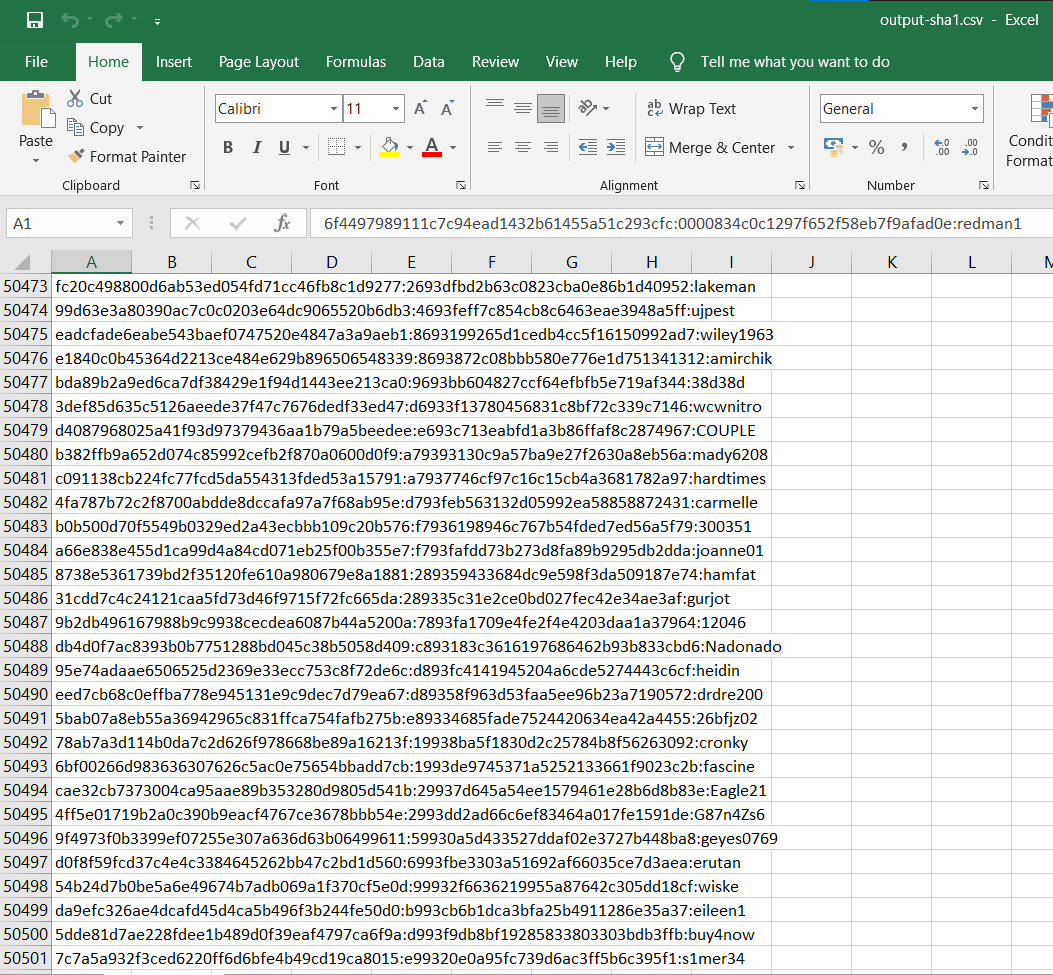


Перетворений набір хешів пропустимо через hashcat із словником частовживаних паролів за допомогою наступної команди:

./hashcat64.exe -w 3 -d 1 -a 0 -m 110 generated-sha1-reverse.csv "C:\Users\User\course4\CybersecurityCourse\Lab4\1MofPasswords.txt" -o output-sha1.csv

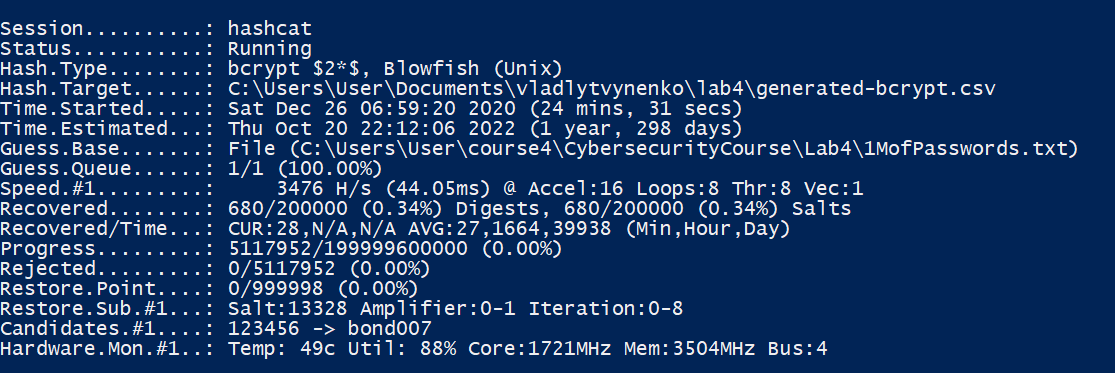


Як бачимо, за 22 хвилини було підібрано 50 501 пароль. Це свідчить про те, що SHA1 є трішки кращим за MD5 та все ще слабким алгоритмом хешування. Знайдені паролі наведено нижче:

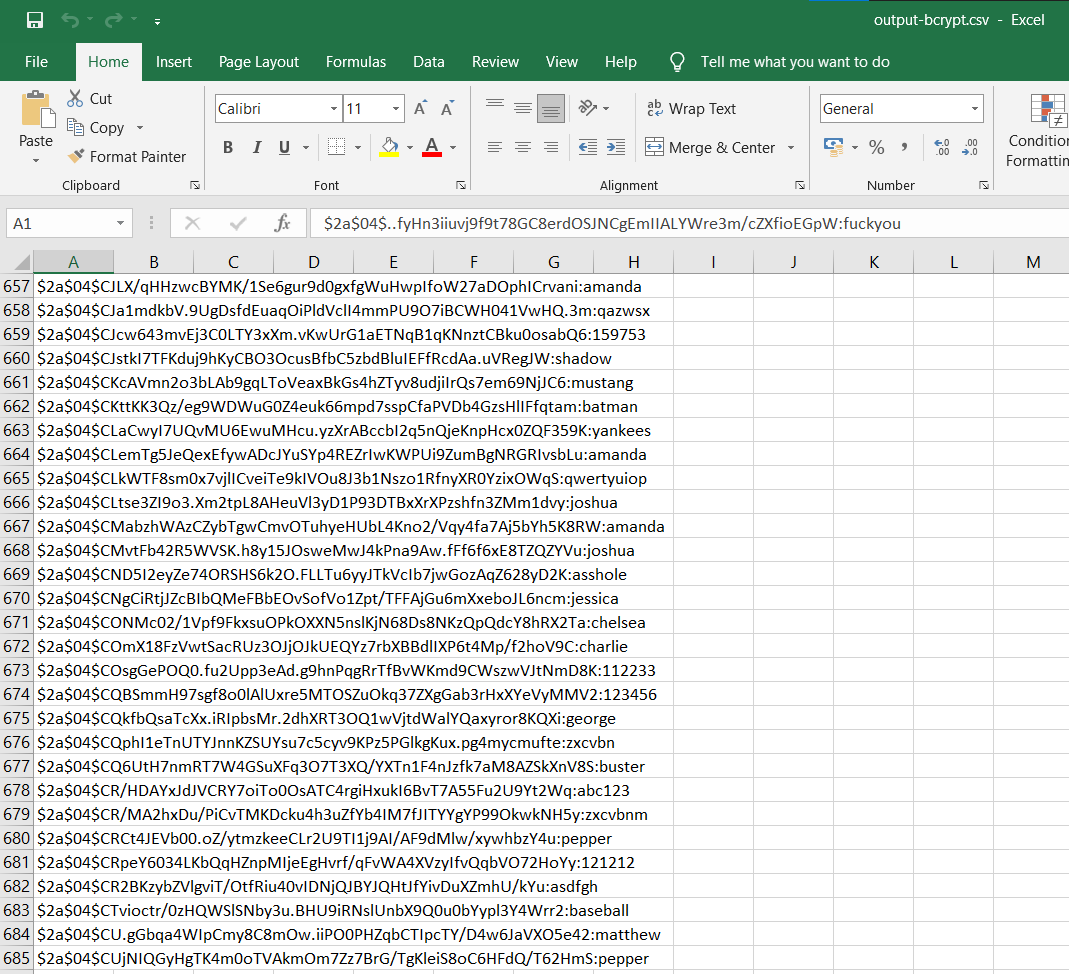


Останніми розглянемо паролі, що були захешовані за допомогою bcrypt. Спробуємо їх підібрати за допомогою словника і наступної команди hashcat:

./hashcat64.exe -w 3 -d 1 -a 0 -m 3200 "C:\Users\User\Documents\vladlytvynenko\lab4\generated-bcrypt.csv" "C:\Users\User\course4\CybersecurityCourse\Lab4\1MofPasswords.txt" -o output-bcrypt.csv



Як бачимо, за 24 хвилини було підібрано тільки 0.34% паролів, а щоб підібрати усі нам потрібно 2 роки. Це свідчить про високу якість алгоритму хешування Bcrypt. Відповідні паролі наведено нижче:



***Висновок:*** Отже, нам було неважко підбирати паролі під алгоритми хешування MD5 та SHA1, що свідчить про їхню слабкість. Ці алгоритми не можна використовувати щоб зберігати паролі реальних користувачів. Що ж до алгоритму bcrypt, то він показав себе дуже добре і може використовуватися для збереження паролів реальних користувачів, адже підбирати паролі до нього дуже довго.

Також, словник із часто вживаними паролями дуже сильно облегшує задачу підбору паролів та зламу. Тому дуже важливо щоб користувачі вводили довгі (як мінімум 8 символів), складні паролі, що містять цифри, символи, що не є ні буквами ні цифрами, та літери в обох регістрах.