##### 1/1 Задание 38.3.4 (HW-04)

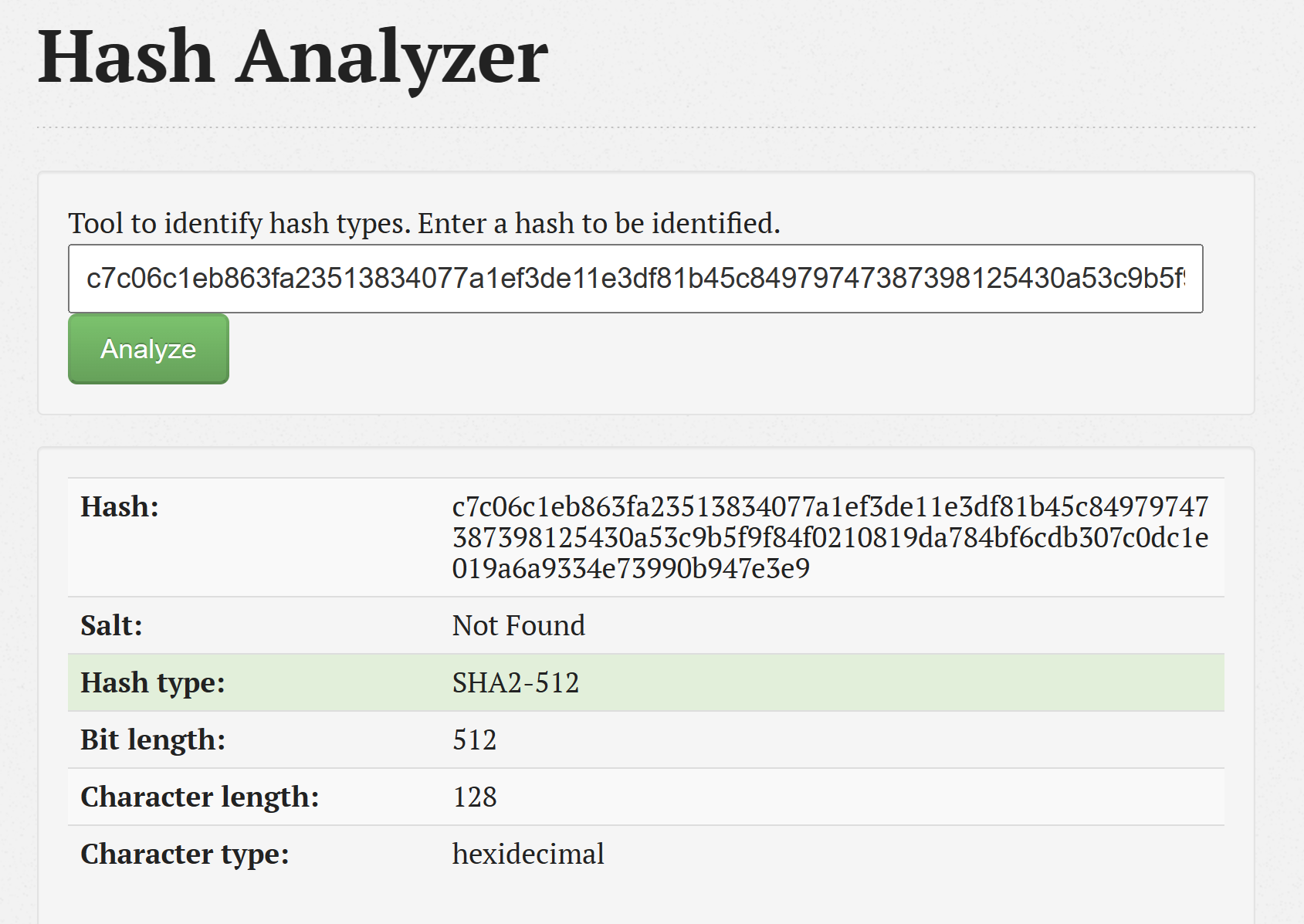
Так как практика брутфорсить пароли онлайн-инструментами у нас так или иначе была, давайте потренируем навыки работы с ****Hashcat****.

Вам дано несколько хэшей:

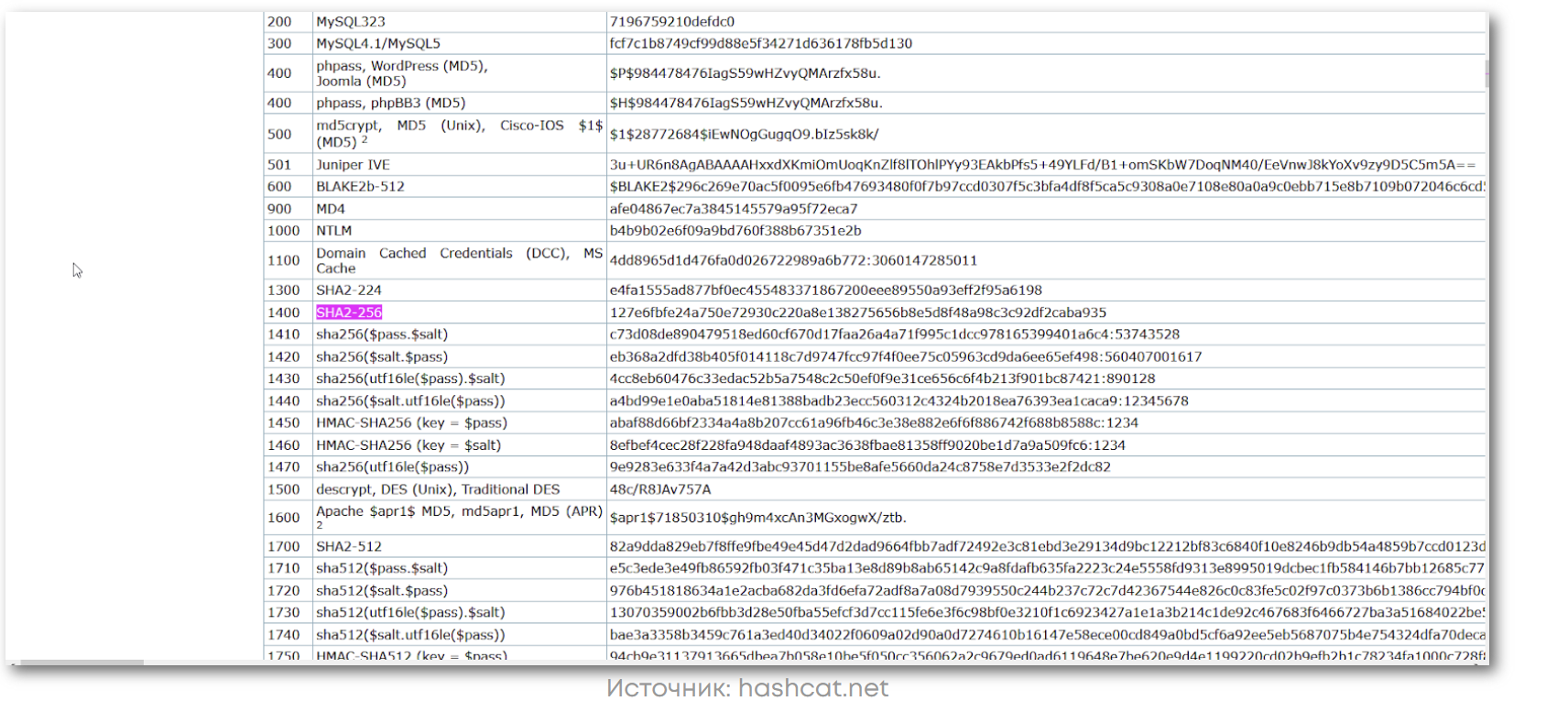
1. c7c06c1eb863fa23513834077a1ef3de11e3df81b45c84979747387398125430a53c9b5f9f84f0210819da784bf6cdb307c0dc1e019a6a9334e73990b947e3e9
2. b43f1d28a3dbf30070bf1ae7c88ee2784047fc86d7be8620c8510debbd8555b3ef0b96376a4dd494ae0561580274bcf7a3069f5c0beceff63d1237a13d4d72b7
3. 0a9b3f20d3d588b98616f5792d957709f62a5ddd2662436e46c752a5000db6877c8c58997bd0cadc3c8f14827510cab5df92170a8ceda6ecb8275fa6b5d8f375

**В рамках проведения атаки с использование *Hashcat*** **необходимо знать тип хэша. Для того чтобы узнать тип хэша, можно воспользоваться большим спектром опций, например, [представленный ниже](https://www.tunnelsup.com/hash-analyzer/):**

1) c7c06c1eb863fa23513834077a1ef3de11e3df81b45c84979747387398125430a53c9b5f9f84f0210819da784bf6cdb307c0dc1e019a6a9334e73990b947e3e9

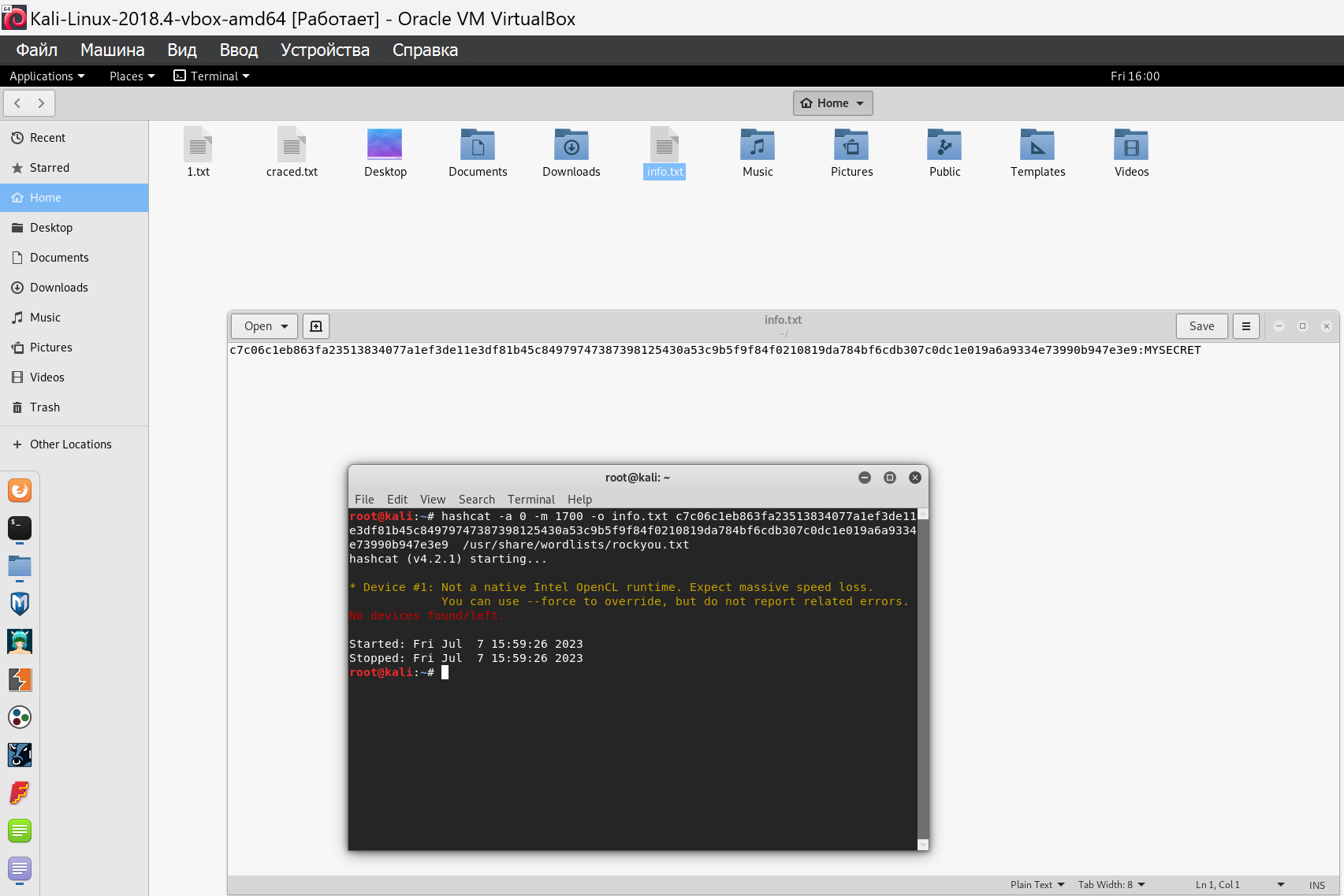


Тип: SHA2-512. В таблице хэш-код ищем соответствующий код.

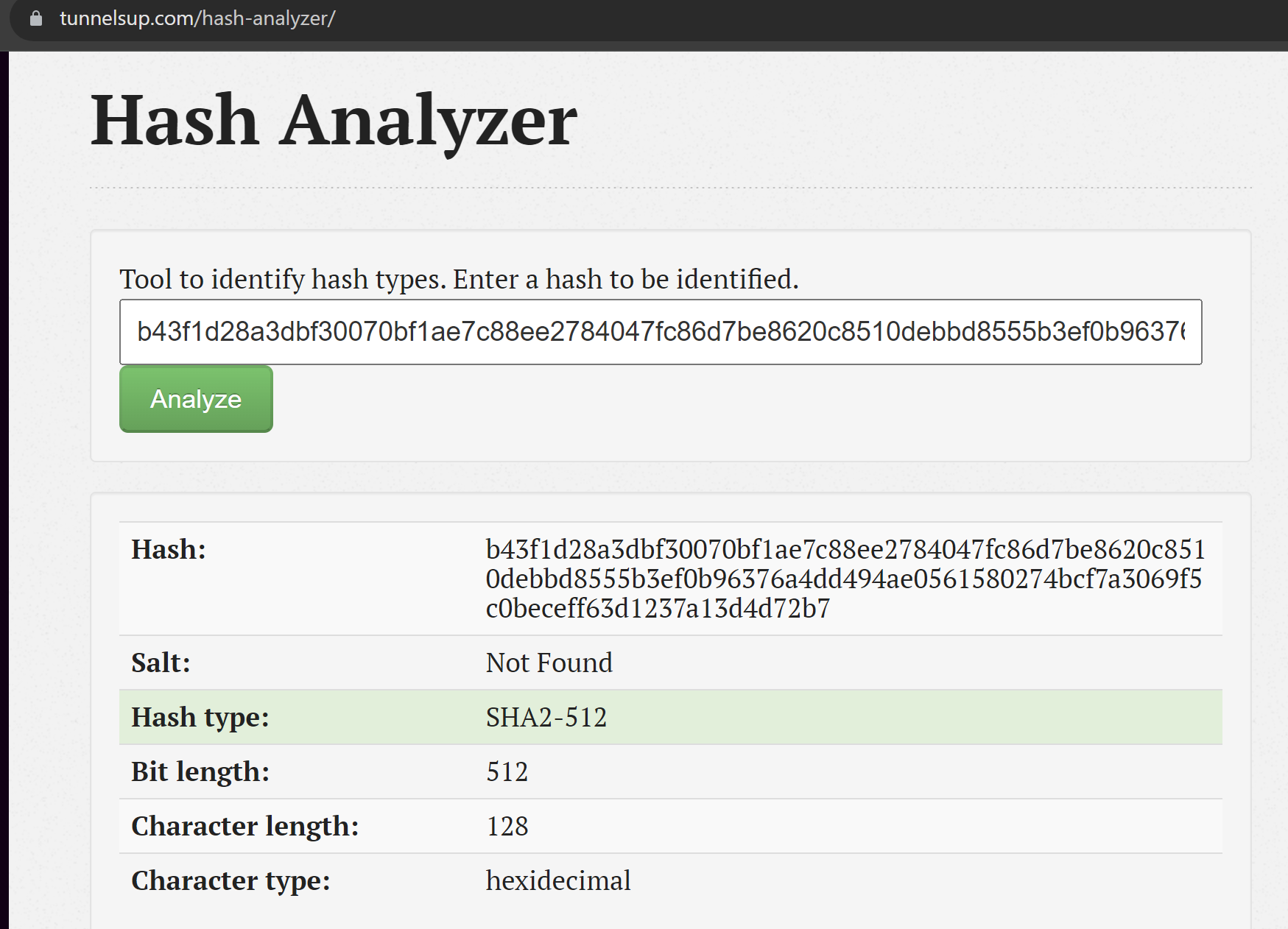


**В нашем случае — 1700.**

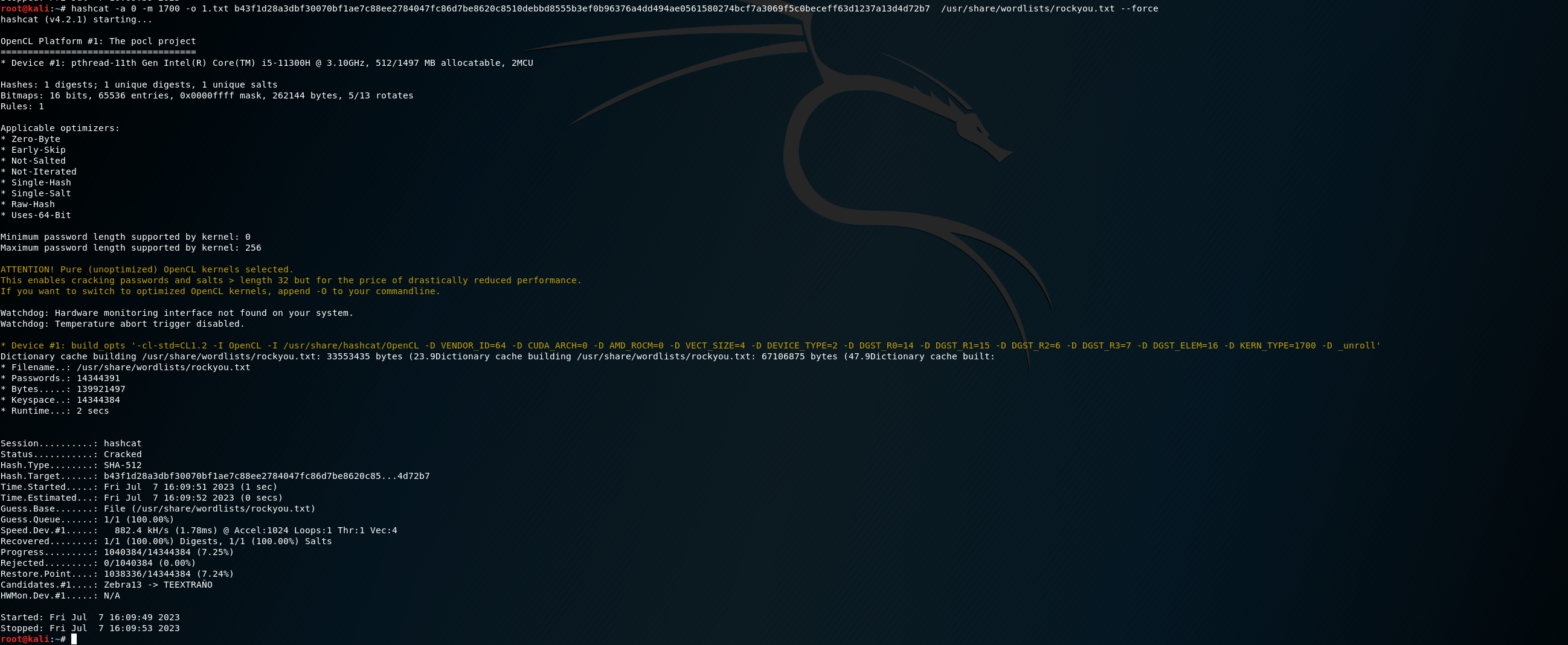
**Введем команду и получим пароль в нужном файле:**

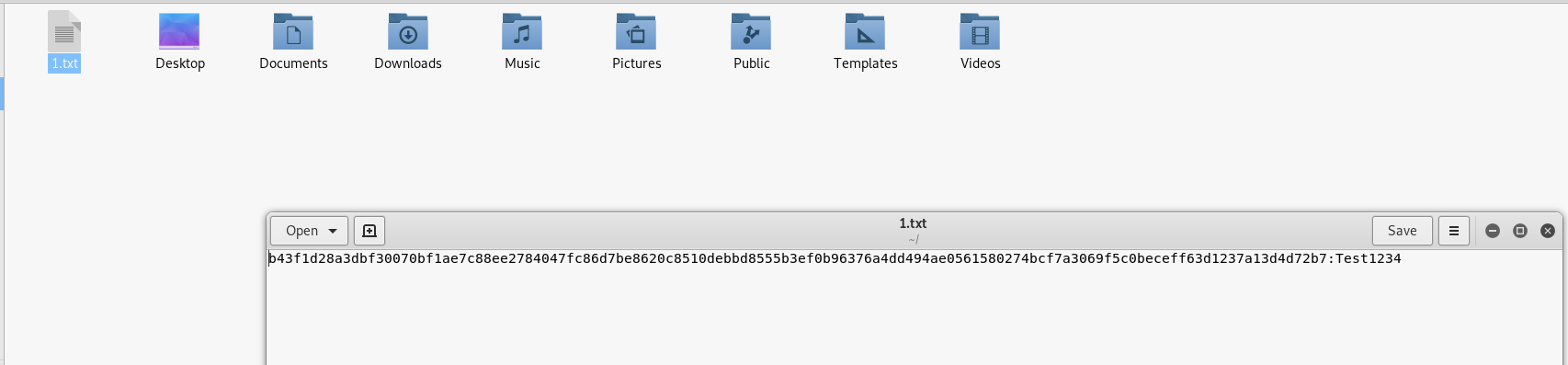


****2)**** b43f1d28a3dbf30070bf1ae7c88ee2784047fc86d7be8620c8510debbd8555b3ef0b96376a4dd494ae0561580274bcf7a3069f5c0beceff63d1237a13d4d72b7

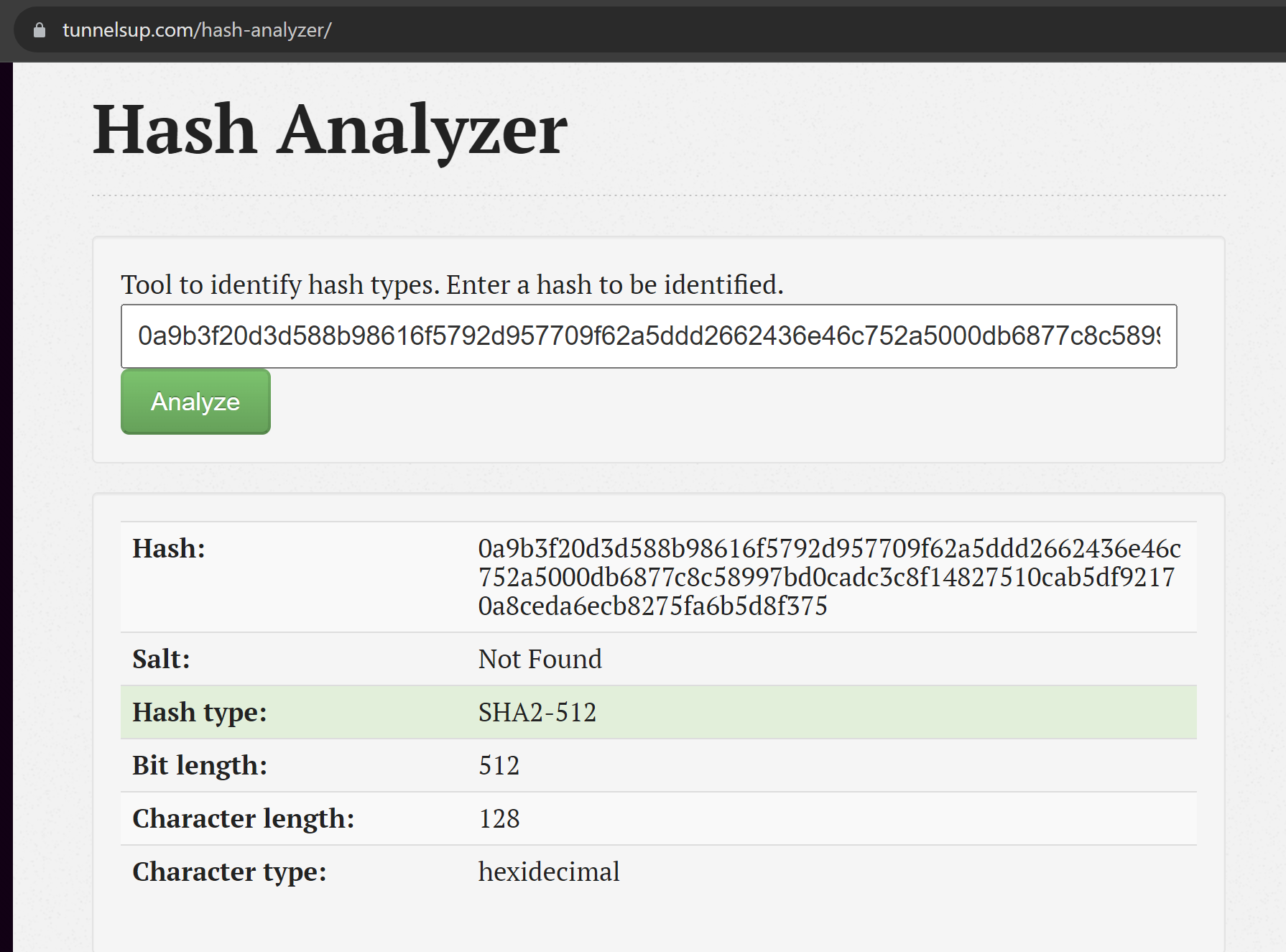


****код 1700, значит введу команду hashcat -a 0 -m 1700 -o 1.txt b43f1d28a3dbf30070bf1ae7c88ee2784047fc86d7be8620c8510debbd8555b3ef0b96376a4dd494ae0561580274bcf7a3069f5c0beceff63d1237a13d4d72b7 /usr/share/wordlists/rockyou.txt --force****





****3)**** 0a9b3f20d3d588b98616f5792d957709f62a5ddd2662436e46c752a5000db6877c8c58997bd0cadc3c8f14827510cab5df92170a8ceda6ecb8275fa6b5d8f375



код 1700. ****значит введу команду hashcat -a 0 -m 1700 -o 2.txt**** 0a9b3f20d3d588b98616f5792d957709f62a5ddd2662436e46c752a5000db6877c8c58997bd0cadc3c8f14827510cab5df92170a8ceda6ecb8275fa6b5d8f375  ****/usr/share/wordlists/rockyou.txt --force****

