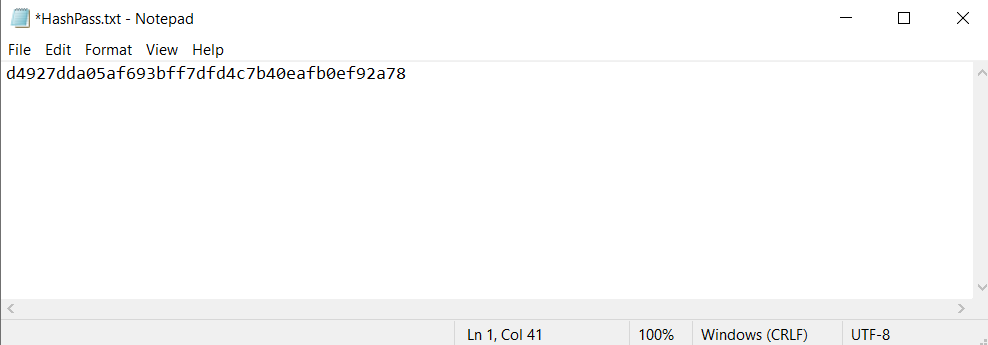
**Ερώτημα\_1**

Στο πρώτο ερώτημα της εργασίας καλούμαστε, με βάση τα χαρακτηριστικά του «hash value», να βρούμε ποια συνάρτηση έχει χρησιμοποιηθεί και να εφαρμόσουμε την καταλληλότερη επίθεση με κάποιο «password cracker». Για να βρούμε τη συνάρτηση θα χρησιμοποιήσουμε ένα hash-identifier (<https://sourceforge.net/projects/hashidentifier/>) και για την επίθεση θα χρησιμοποιήσουμε το JohnTheRipper. Αναλυτικότερα:

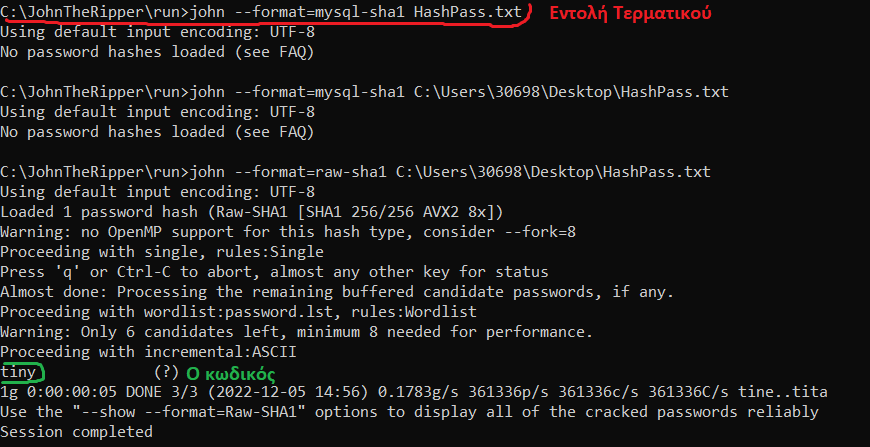
* Θα βάλω το συνθηματικό (**d4927dda05af693bff7dfd4c7b40eafb0ef92a78**) στο hash-identifier και θα πάρω τη συνάρτηση που χρησιμοποιήθηκε για να παραχθεί.



* Αποθηκεύω το συνθηματικό σε ένα αρχείο



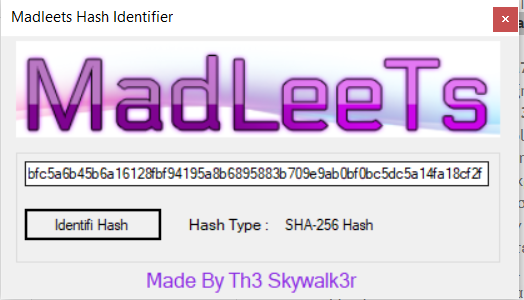
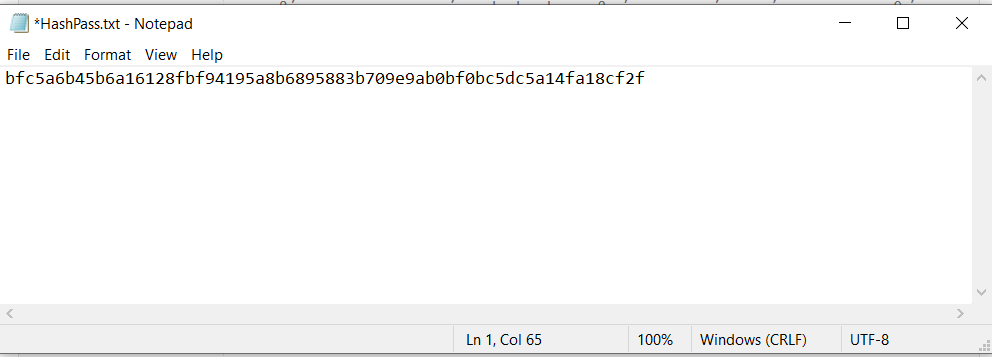
* Ύστερα θα κατευθυνθώ από το τερματικό μου στο φάκελο όπου έχω το JohnTheRipper και θα πραγματοποιήσω την επίθεση ορίζοντάς του και το είδος του Hash που χρησιμοποίησα, αφού το βρήκα στο προηγούμενο βήμα.

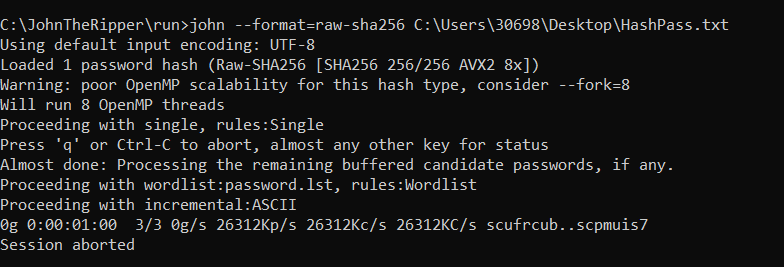


* Όπως φαίνεται από τα αποτελέσματα ο κωδικός είναι «tiny» και ο χρόνος που χρειάστηκε ήταν ελάχιστος όπως φαίνεται και στο τερματικό.

**Ερώτημα\_2**

Σε αυτό το ερώτημα θα επαναλάβουμε την παραπάνω διαδικασία για ένα διαφορετικό Hash. Θα βρούμε την συνάρτηση που χρησιμοποιήθηκε και πάλι και θα βάλουμε το φάκελο στο JohnTheRipper ώστε να κάνει την πιο αποδοτική επίθεση.





* Παρατηρώ ότι με τον απλό τρόπο παίρνει πάρα πολύ χρόνο καθώς δεν είναι εύκολο να σπάσω το Hash λόγο του sha-256. Αφού ξέρω όμως το μέγεθος του Password θα το περάσω ως όρισμα στον JohnTheRipper και θα ξαναδοκιμάσω. Αλλά και πάλι παίρνει μεγάλο χρόνο για να ολοκληρωθεί.

