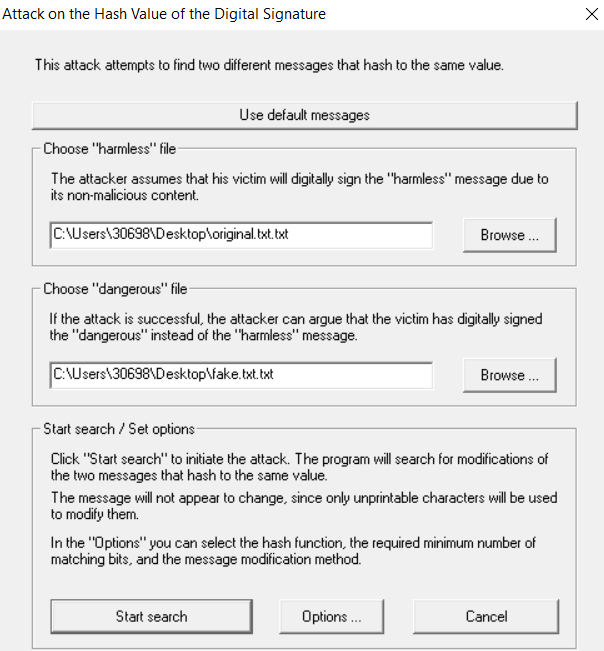
1.5 Στο συγκεκριμένο ερώτημα καλούμαστε, με βάση τα κείμενα που δημιουργήσαμε στο παραπάνω βήμα, να βρούμε ένα «επικίνδυνο» μήνυμα το οποίο μοιάζει στο fake.txt και να έχει την ίδια τιμή hash με το original.txt για τις παρακάτω περιπτώσεις:

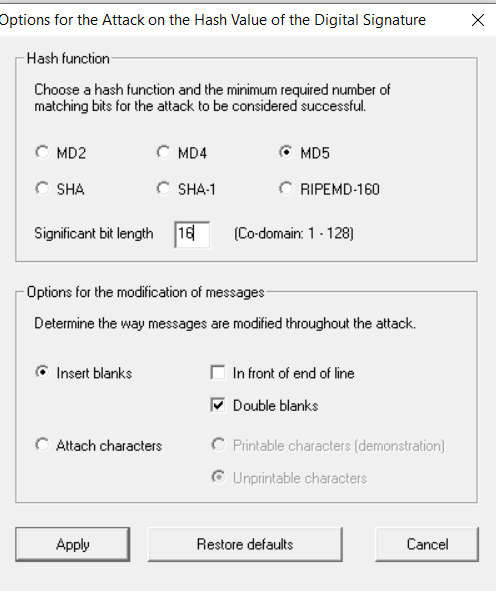
* Για τον αλγόριθμο MD5 και τα πρώτα 16 bit της τιμής hash.
* Για τον αλγόριθμο MD5 και τα πρώτα 50 bit της τιμής hash.
* Για τον αλγόριθμο SHA1 και τα πρώτα 80 bit της τιμής hash.
* Για τον αλγόριθμο SHA1 και όλα (160) τα bit της τιμής hash.

Η διαδικασία που θα ακολουθήσουμε είναι η εξής. Αρχικά θα μετακινηθούμε μέσω του μενού σε Analysis 🡪 Hash 🡪 Attack on the hash value of the digital signature. Ύστερα στο βοηθητικό παράθυρο θα επιλέξουμε τον αλγόριθμο και τα αρχεία που επιθυμούμε (στην περίπτωσή μας πάντα τα original.txt και fake.txt).

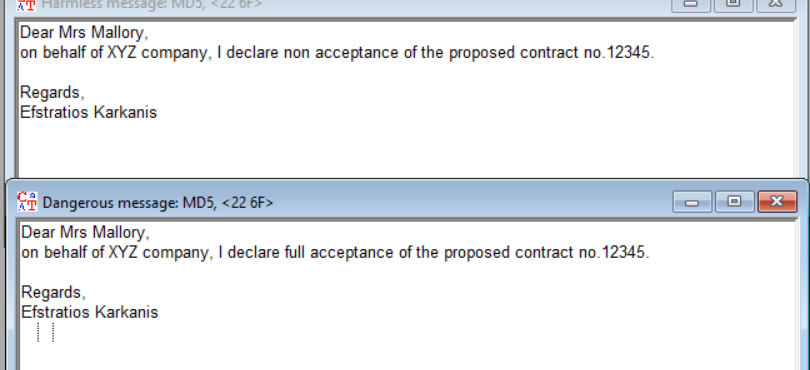
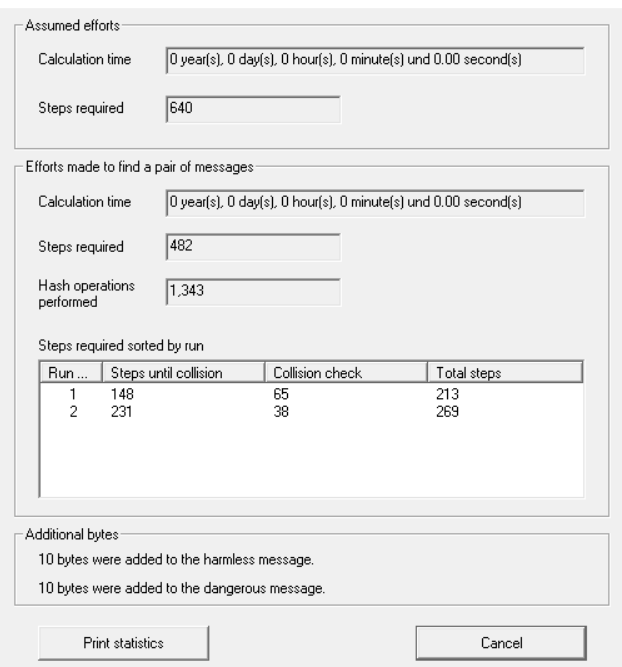
1. **Για τον αλγόριθμο MD5 και τα πρώτα 16 bit της τιμής hash.**

Αφού βάλουμε τις απαραίτητες παραμέτρους.



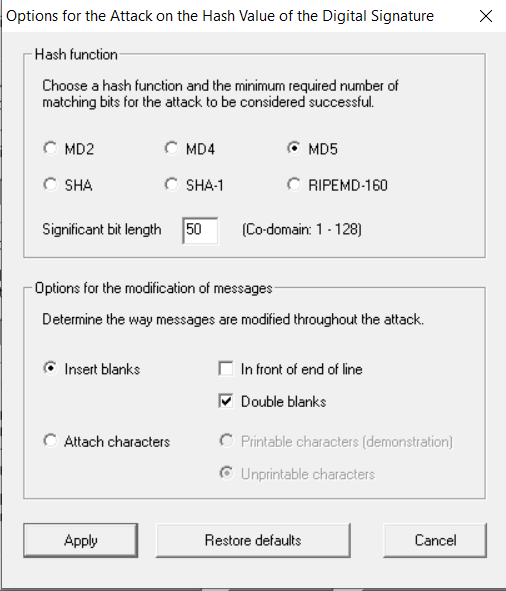


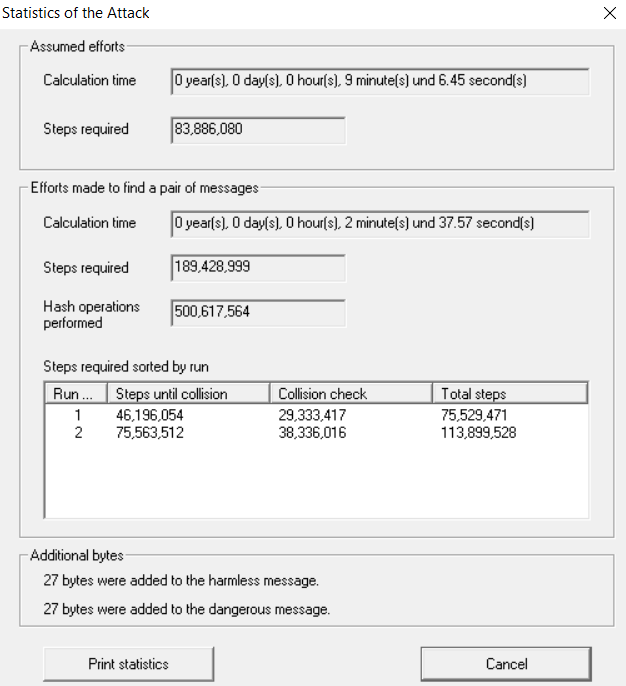
Πραγματοποιούμε την επίθεση. Ο χρόνος είναι σχεδόν μηδενικός.

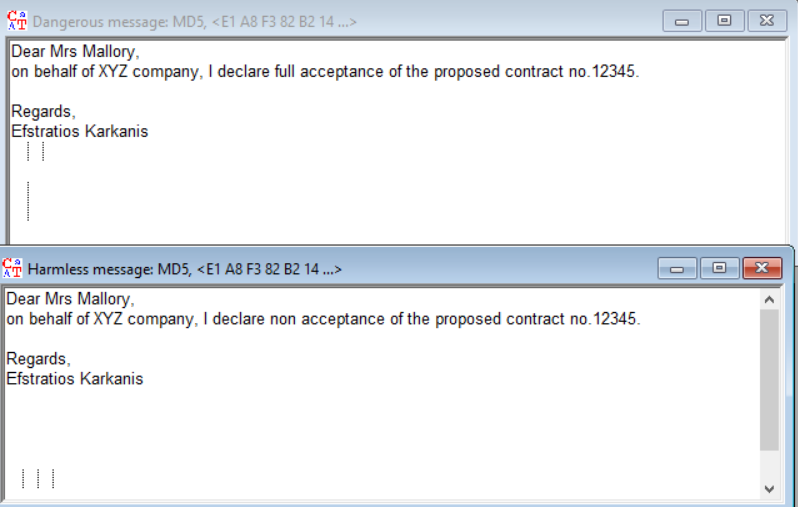


1. **Για τον αλγόριθμο MD5 και τα πρώτα 50 bit της τιμής hash.**

Φορτώνουμε και πάλι τα δεδομένα, και αφού κάνουμε τις απαραίτητες αλλαγές, πραγματοποιούμε την επίθεση. Ο χρόνος ολοκλήρωσης ήταν περίπου 3 λεπτά.

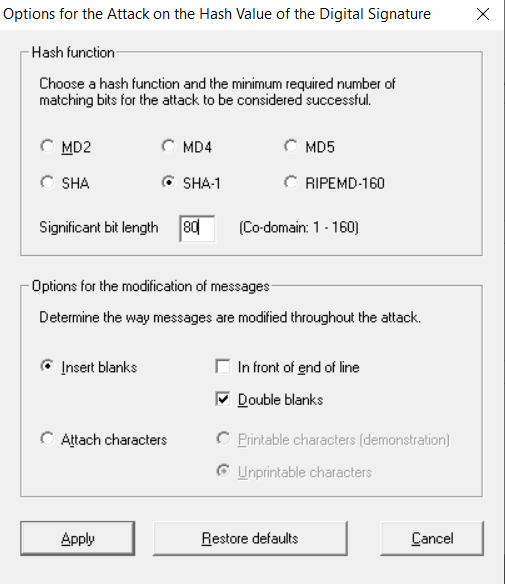


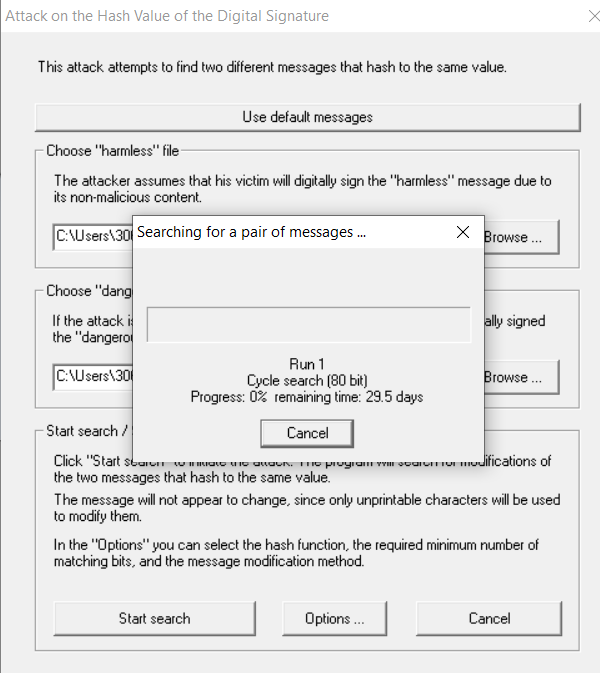




1. **Για τον αλγόριθμο SHA1 και τα πρώτα 80 bit της τιμής hash.**

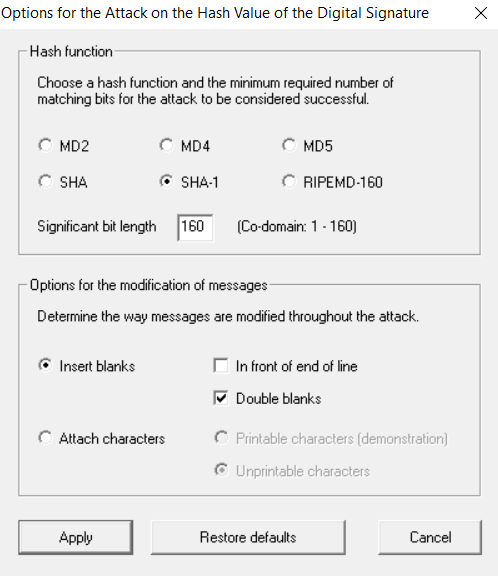
Φορτώνουμε και πάλι τα δεδομένα μας και αφού κάνουμε τις απαραίτητες αλλαγές εκτελούμε την επίθεσή μας, ο χρόνος ολοκλήρωσης ήταν περίπου 30 ημέρες.

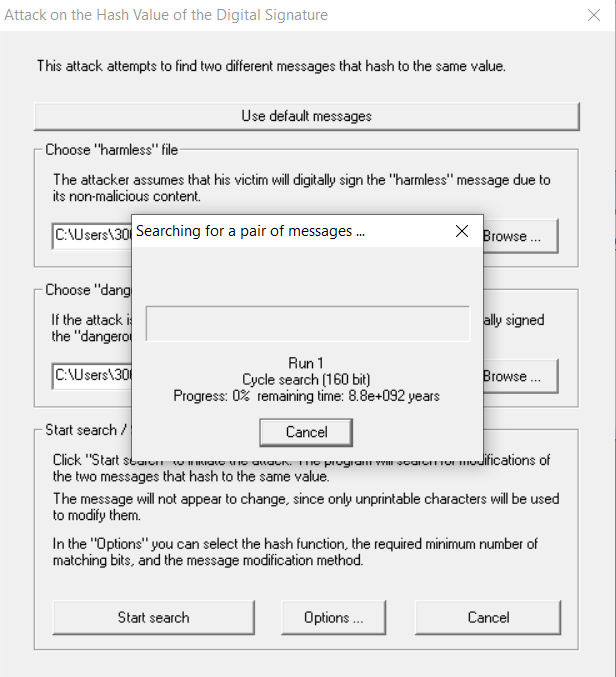




1. **Για τον αλγόριθμο SHA1 και όλα (160) τα bit της τιμής hash.**

Φορτώνουμε και πάλι τα δεδομένα μας, και αφού κάνουμε τις απαραίτητες αλλαγές στον αλγόριθμο, εκτελούμε την επίθεσή μας. Ο χρόνος ολοκλήρωσης ήταν υπερβολικά μεγάλος.





Σχόλια:

* Μπορούμε να καταλάβουμε μέσω αυτού του ερωτήματος την τεράστια διαφορά στην ασφάλεια των δύο αλγορίθμων.
* Προφανώς δεν ολοκληρώσαμε τα δύο τελευταία παραδείγματα καθώς δεν ήταν χρονικά βιώσιμα.
* Στις αλλαγές των αρχείων με το ίδιο hash-value(κατηγορία 1 και 2) οι διαφορές είναι είτε σε χαρακτήρες που δεν φαίνονται, είτε σε μικρούς χαρακτήρες κ.λπ., όπως αναγράφεται και στην εφαρμογή.

1.6 Προφανώς μία τέτοια επίθεση όπως περιγράφουμε και εκτελούμε στο 1.5 θα ήταν καταστροφική για την ασφάλεια μίας ψηφιακής υπογραφής, καθώς αν καταφέρει κάποιος να πετύχει ένα collision-attack στη συνάρτηση Hash θα του δοθεί η δυνατότητα να υπογράφει ο ίδιος με το όνομα και τα στοιχεία ενός άλλου. Κάτι τέτοιο θα μπορούσε να φανεί ιδιαίτερα ζημιογόνο σε ατομικό επίπεδο και πόσο μάλλον σε επίπεδο ενός οργανισμού.