
Ασφάλεια Πληροφοριακών & Επικοινωνιακών Συστημάτων

3η Ομαδική Εργασία

Αυλακιώτης Χρήστος – 321/2012015
Κατσιβέλης Κων/νος – 321/2011063
Φιωτάκης Γιώργος – 321/2013220

A) Απαντήσεις Ερωτήσεων

- Ποιος ο λόγος της χρήσης του salt για την παραγωγή της σύνοψης ενός συνθηματικού;
- Η συνόψεις δημιουργούνται με τη τεχνική του κατακερματισμού, αυτό σημαίνει πως η συνάρτηση κατακερματισμού παίρνει ως είσοδο ένα κείμενο και επιστρέφει μια διαφορετική έξοδο η οποία αποτελεί την αναπαράσταση του κειμένου εισόδου βάση της αλγορίθμου που χρησιμοποίησε η συνάρτηση. Άρα πάντα ένα κείμενο θα έχει την ίδια αναπαράσταση όταν περάσει από την συνάρτηση κατακερματισμού με χρήση του ιδίου αλγορίθμου. Η συναρτήσεις αυτές απαιτούν πολύ λίγο χρόνο για την εκτέλεση τους και είναι εύκολο κάποιος να βρει η να δημιουργήσει μια λίστα με συνδυασμούς φράσεων. Άρα άμα κάποιος υποκλέψει τη σύνοψη του κωδικού μας και δημιουργήσει συνόψεις από παρά πολλούς συνδυασμούς φράσεων, γραμμάτων, αριθμών, χαρακτήρων κλπ, και τις συγκρίνει με την σύνοψη του κωδικού μας είναι πολύ πιθανό να βρει το κωδικό μας. Γιατί το λόγο για μεγαλύτερη ασφάλεια θα πρέπει να δημιουργούμε τη σύνοψη του κωδικού μας μαζί με κάποια τυχαία σειρά αλφαριθμητικών ώστε να μην είναι πλέον εύκολο να βρεθεί ο κωδικός μας με τη παραπάνω διαδικασία.
- Ποιες είναι κατά την γνώμη σας οι αδυναμίες του συστήματος; Περιγράψτε σύντομα τι ευπάθειες μπορεί να εκμεταλλευτεί ένας επιτιθέμενος. Προτείνετε μηχανισμούς που κατά τη γνώμη σας μπορούν να βελτιώσουν την ασφάλεια που παρέχει η εφαρμογή.
- Μια από τις ευπάθειες που μπορεί να εκμεταλλευτεί κάποιος είναι ότι πολλά σημαντικά δεδομένα όπως συμμετρικά και ασύμμετρα κλειδιά, κωδικοί κλπ, κατά την εκτέλεση του προγράμματος βρίσκονται αποθηκευμένα σε Strings. Αυτό σημαίνει πως αυτές οι συμβολοσειρές βρίσκονται διασκορπισα στην μνήμη του υπολογιστή. Έτσι άμα υπήρχε κρυμμένο στον υπολογιστή μας κάποιο πρόγραμμα – ληστής θα μπορούσε να προσπελάσει αυτά τα δεδομένα και να ανακτήσει της πολύτιμες αυτές συμβολοσειρές με τα προσωπικά μας δεδομένα και τα δεδομένα που χρησιμοποιεί η εφαρμογή. Για να το αποτρέψουμε αυτό θα έπρεπε να

αποθηκεύουμε όλα αυτά τα δεδομένα σε πίνακες χαρακτήρων ή bytes (στο συγκεκριμένο πρόγραμμα το χουμε κάνει για τους κωδικούς των χρηστών) για να μη μπορούσε να τα ανακτήσει ο επιτιθέμενος αλλά και επίσης να ελέγχουμε τον υπολογιστή μας συχνά για κακόβουλο λογισμικό. Επίσης άμα το ιδιωτικό κλειδί της εφαρμογής ήταν και αυτό αποθηκευμένο σε κάποιο αρχείο θα την πολύ εύκολο να το πάρει κάποιος και έπειτα να μπορεί να αποκρυπτογραφήσει τα δεδομένα μας. Γιατί πρέπει το ιδιωτικό κλειδί της εφαρμογής να βρίσκεται δηλωμένο στο κώδικα. Τέλος τα δεδομένα των χρηστών βρίσκονται άπλα αποθηκευμένα σε φακέλους στο φάκελο της εφαρμογής και θα την πολύ εύκολο κάποιος να τα σβήσει και να τα χάσουμε. Γιατί το λόγο θα τα ωφέλιμο να γίνονταν backup και σε άλλα μέρη του υπολογιστή και σε κρυφά αρχεία.

B) Λίγα λόγια για την υλοποίηση.

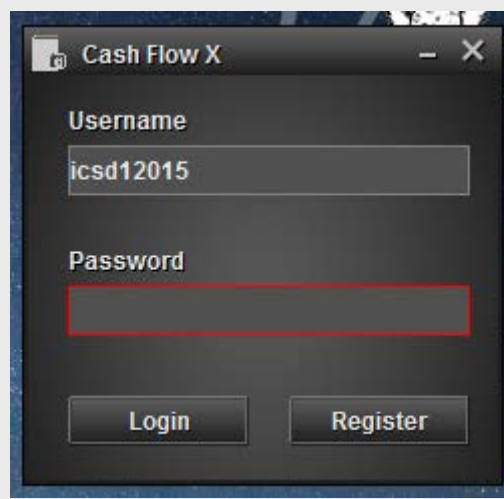
Έγινε προσπάθεια να βγει ο κώδικας άπλα δομημένος, κατανοητός αλλά και επαναχρησιμοποιήσιμος χωρίς να υστερεί σε λειτουργίες. Τα σχολία είναι αρκετα πιστευω ώστε να είναι ευκολο στην κατανοηση του τι γίνεται. Μόνο στην κλάση των γραφικών δεν υπάρχουν πολλά καθώς είναι πολύ μεγάλη και όλες τις σημαντικές λειτουργίες τις εκτελεί από τη Main. Για τα γραφικά χρησιμοποιήθηκε μια άλλη εμφάνιση το LookAndFeel των γραφικών στοιχείων μέσω μιας βιβλιοθήκης η όποια βρίσκεται στο φάκελο lib του project. Αν δεν την προσθέσετε στο project, θα χρησιμοποιηθεί η εμφάνιση του λειτουργικού συστήματος αλλά σίγουρα δε θα φαίνονται καλά τα γραφικά καθώς σχεδιάστηκαν για αυτήν την εμφάνιση και δε χρησιμοποιήθηκε layout για ευκολία. Επίσης έχουν γίνει παντού έλεγχοι για σφάλματα στις εισαγωγές στοιχείων, με ενημερωτικά παράθυρα και σε άλλες περιπτώσεις εκτός σφαλμάτων για ευκολία του χρηστή. Ξέρω πως αυτό δεν ήταν το ζητούμενο αλλά επειδή αρέσει να ασχολούμαι με το design το κάνα. Τώρα όσο αναφορά τις βασικές λειτουργίες του προγράμματος υλοποιούνται όλες στη Main και ενώ οι διαδικασίες κρυπτογράφησης είναι σε ξεχωριστές κλάσης η κάθε μια οι όποιες περιέχουν τα πάντα για την υλοποίηση της κρυπτογράφησης που απευθύνονται. Για την εγγραφή των κλειδιών σε αρχεία χρησιμοποιήθηκε κωδικοποίηση σε Base64 για να γίνουν String από byte arrays καθώς δεν βρίσκαμε άλλο τρόπο να το κάνουμε αυτό (παρακαλούμε αν υπάρχει άλλος τρόπος να μας τον πείτε στην εξέταση). Ως εξτρά μετρά ασφάλειας μπήκε προϋπόθεση για τους κωδικούς να αποτελούνται από το λιγότερο 8 χαρακτήρες, να χουν ένα τουλάχιστον ψηφίο, σύμβολο, πεζό και κεφάλαιο γράμμα. Επίσης οι κωδικοί αποθηκεύονται μονό σε char arrays ώστε να μην μενού ως συμβολοσειρές στη μνήμη και το ιδιωτικό κλειδί είναι δηλωμένο στο κώδικα της εφαρμογής όπως και το δημόσιο σε περίπτωση που χαθεί. Βγήκε λίγο μεγάλη λήγω όλων αυτών των ελέγχων και γραφικών αλλά ελπίζουμε να μην δύσκολο στη διόρθωση λήγω της δομής του. Ελπίζουμε να την

τρέξετε κιόλας και να τη δείτε λίγα λεπτά εκτός από τα ακρινούς για να δείτε ότι όντως είναι καλοφτιαγμένη και ο κώδικας δεν είναι τσάμπα μεγάλος σε έκταση. Γενικά υπήρχαν αρκετα bugs άλλα όλα διορθωθήκαν και τώρα δεν υπάρχει κάποιο που να χουμε εντοπίσει

Γ) Οθόνες Εκτέλεσης Εφαρμογής

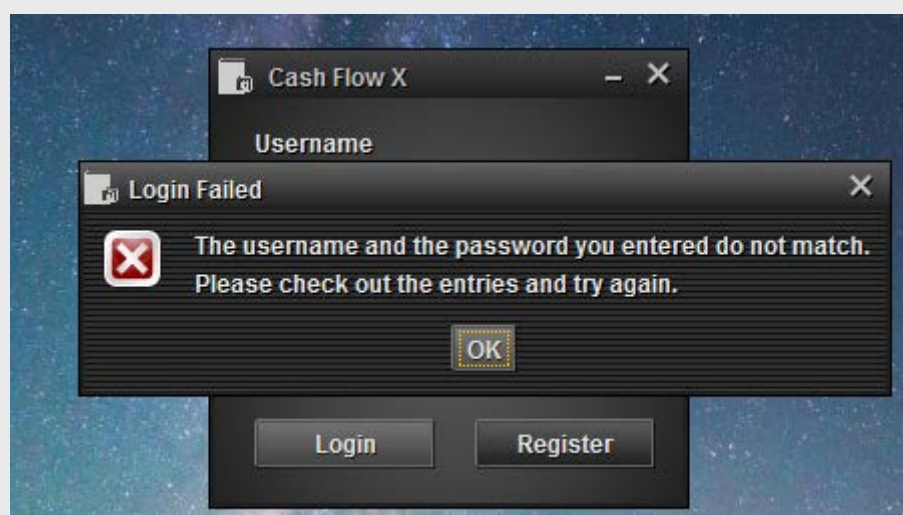
Αυτή είναι πρώτη οθόνη της αρμογής οπου γίνεται η σύνδεση του χρηστή. Στη συγκεκριμένη περίπτωση έχουμε πατήσει login χωρίς να βάλουμε κωδικό και έτσι κοκκινίζει το JPasswordField του κωδικού

Γενικά αυτής της μορφής ο έλεγχος και ειδοποίηση υπάρχει σε όλες τις φόρμες του προγράμματος

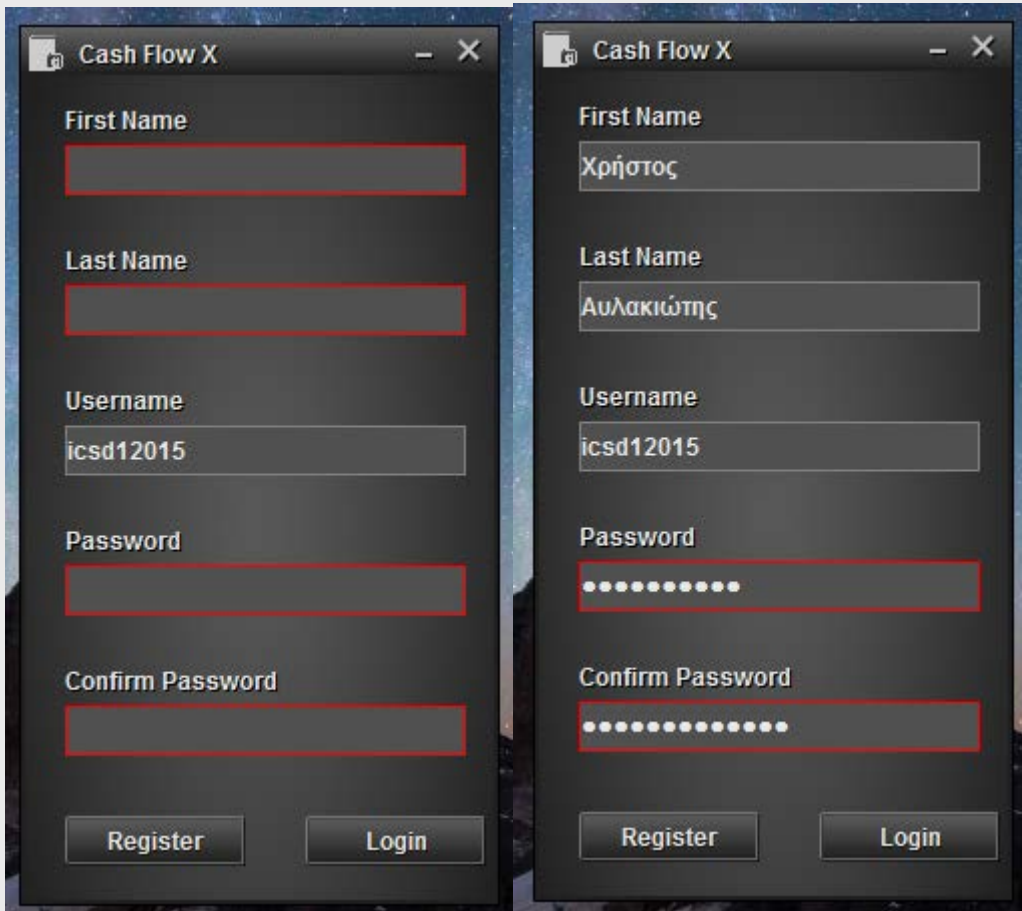


Εδώ έχουμε βάλει λάθος κωδικό ή/και λάθος όνομα χρηστή οποτε μας εμφανίζει αυτό το Message Dialog για να μας ενημερώσει.

Επίσης γενικά σε όλα τα σφάλματα χρηστή άλλα και exceptions που μπορεί να προκύψουν υπάρχουν αντίστοιχοι διάλογοι ενημέρωσης.



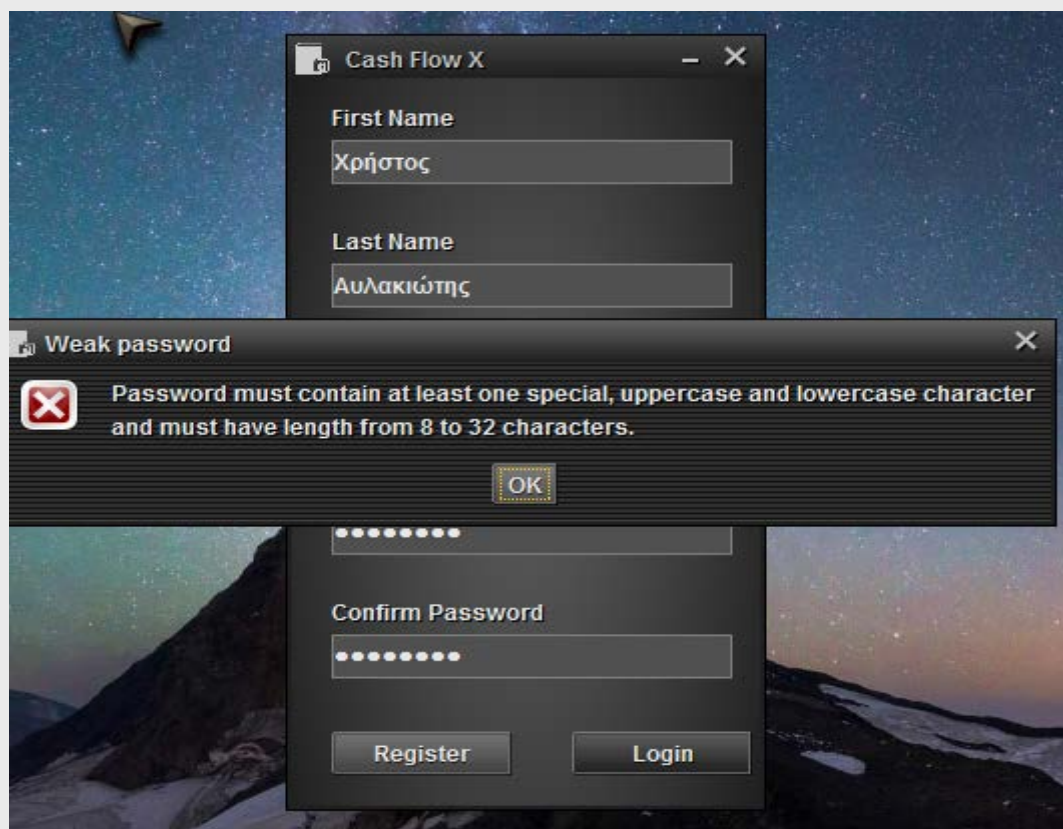
Αυτό είναι το παράθυρο εγγραφής νέου χρηστή. (το όνομα υπάρχει γιατί είχαμε προσπαθήσει προηγουμένως να κάνουμε σύνδεση με αυτό χωρίς να υπάρχει)



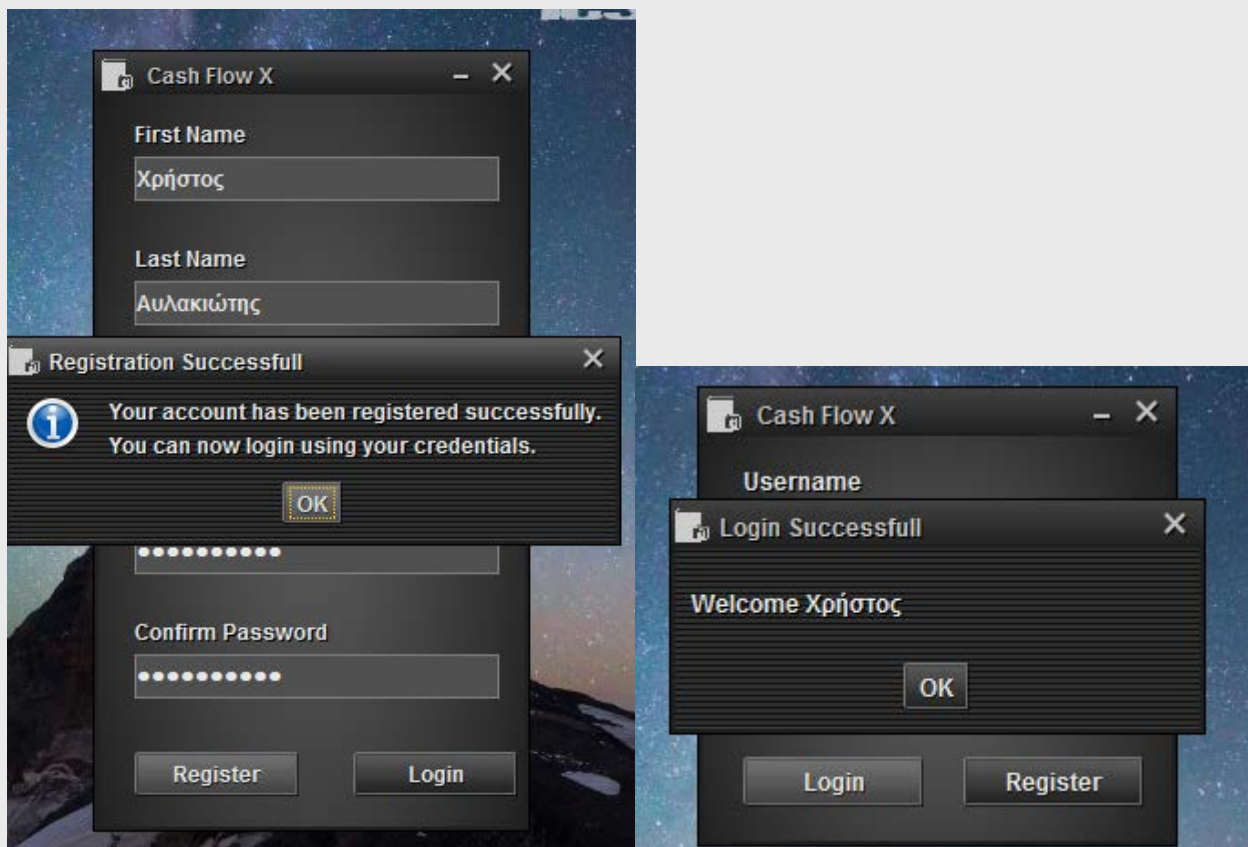
The image displays two side-by-side screenshots of a software window titled "Cash Flow X". The window contains a registration form with the following fields: "First Name", "Last Name", "Username", "Password", and "Confirm Password". At the bottom of the window are two buttons: "Register" and "Login".

In the left screenshot, all input fields are empty. In the right screenshot, the fields are filled with the following text: "First Name" is "Χρήστος", "Last Name" is "Αυλακιώτης", "Username" is "icsd12015", "Password" is masked with dots, and "Confirm Password" is also masked with dots.

Στη συνέχεια βλέπουμε το παράθυρο για ενημέρωση πως ο κωδικός δε πληρή τις προϋποθέσεις ασφάλειας τις οποίες αναφέρει



The image shows the "Cash Flow X" registration window with a "Weak password" error dialog box overlaid. The dialog box has a red "X" icon and the following text: "Password must contain at least one special, uppercase and lowercase character and must have length from 8 to 32 characters." Below the text is an "OK" button. The registration form is partially visible behind the dialog box, showing the "First Name" field filled with "Χρήστος", the "Last Name" field filled with "Αυλακιώτης", and the "Password" and "Confirm Password" fields masked with dots. The "Register" and "Login" buttons are also visible at the bottom of the registration form.



Η εναλλαγή των λειτουργιών του προγράμματος γίνεται μέσω ενός JTabbedPane.

Αυτή είναι η καρτέλα για την καταχώρηση νέας συναλλαγής. Το document του JTextField για το πόσο το κάνω implement και φτιάχνει τη μορφή του αριθμού με κόμματα ανά χιλιάδες και παίρνει μόνο νούμερα (22 max)

Στην επομένη οθόνη φαίνεται το παράθυρο για την επιλογή ημερομηνίας.

The screenshot shows the 'Cash Flow X' application window. The 'Transaction Details' section is visible, with the 'Ammount' field set to '123,456,789.99' and the currency set to 'EUR'. A 'Pick date' calendar overlay is displayed, showing the month of May 2016. The calendar has a grid of days from Sunday to Saturday. The date '01/05/2016' is highlighted in the calendar. Below the calendar, there is a 'Type' dropdown menu with a downward arrow. At the bottom of the application window, there are 'Save' and 'Clear' buttons.

Sun	Mon	Tue	Wed	Thur	Fri	Sat
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	

<< 01/05/2016 >>

Type: ...

Save Clear

The screenshot shows the 'Cash Flow X' application window. The 'Transaction Details' section is visible, with the 'Ammount' field set to '123,456,789.99' and the currency set to 'EUR'. A 'Description' field is present. A 'Transaction Entry Created' message overlay is displayed, stating 'Your transaction entry added successfully.' with an 'OK' button. Below the message, the 'Date' field is set to '27/05/2016' and the 'Type' dropdown menu is set to 'Profit'. At the bottom of the application window, there are 'Save' and 'Clear' buttons.

Transaction Entry Created

Your transaction entry added successfully.

OK

Date: 27/05/2016

Type: Profit

Save Clear

The screenshot shows the 'Cash Flow X' application window. The 'Transaction Details' section is visible, with the 'Ammount' field set to '123,456,789.99' and the currency set to 'EUR'. A 'Description' field is present. An 'Entry not saved' warning overlay is displayed, stating 'You haven't saved the new transaction entry. Are you sure you want to leave this tab?' with 'Yes' and 'No' buttons. Below the warning, the 'Date' field is empty and the 'Type' dropdown menu is set to '...'. At the bottom of the application window, there are 'Save' and 'Clear' buttons.

Entry not saved

You haven't saved the new transaction entry. Are you sure you want to leave this tab?

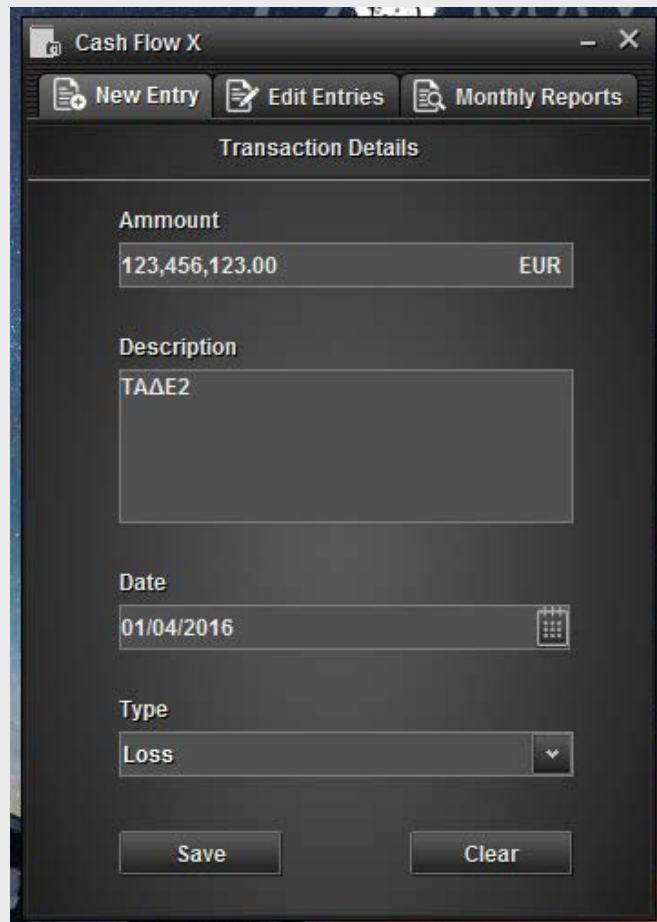
Yes No

Date:

Type: ...

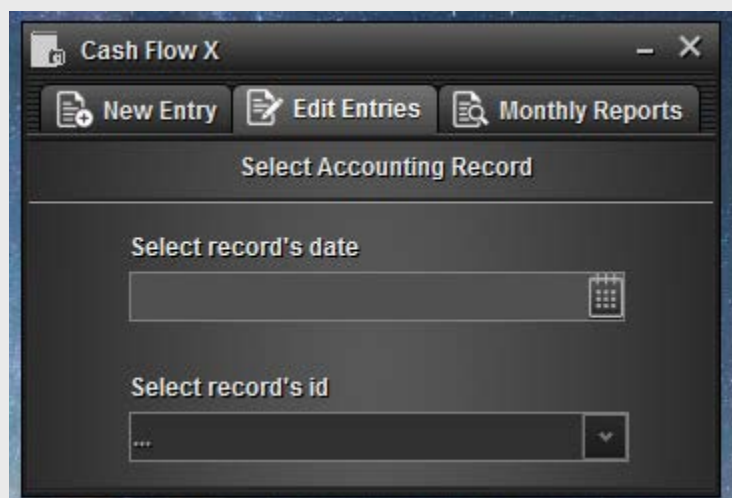
Save Clear

Επίσης βάλαμε άλλη μια εγγραφή ώστε να εμφανίσουμε μετά μια μικρή αναφορά. Βέβαια αυτή μπήκε σε άλλο μηνά αλλά αμέσως τώρα πάμε να αλλάξουμε τη προηγούμενη και να τις βάλουμε στον ίδιο.

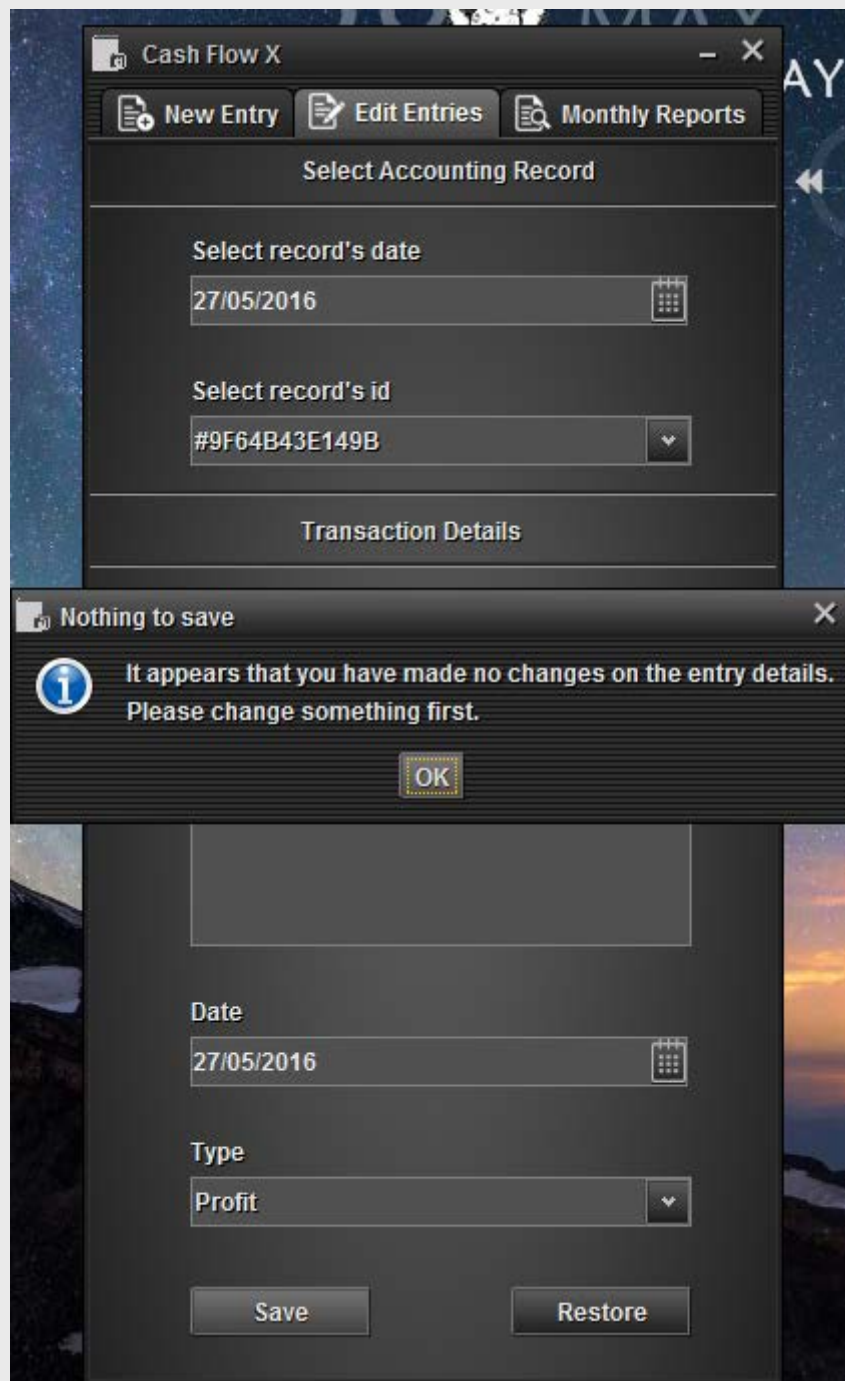
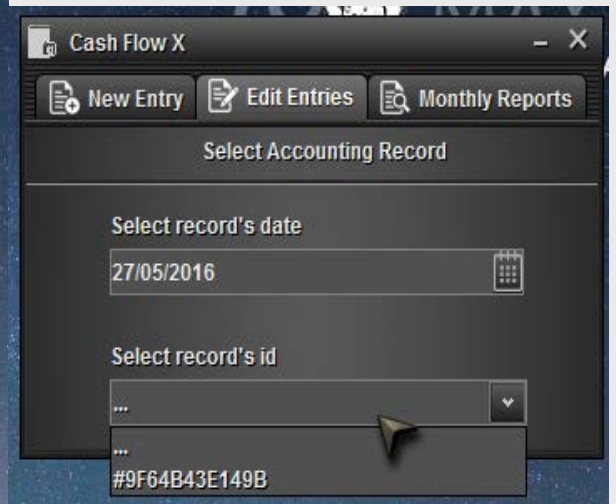
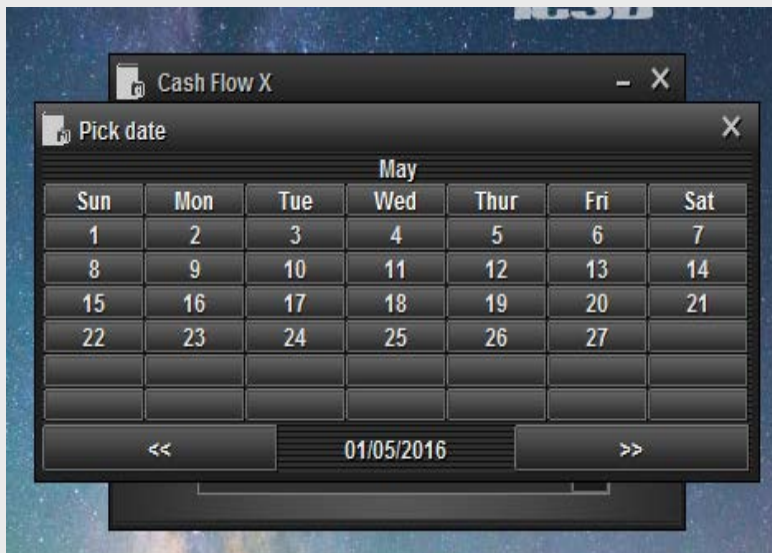


The screenshot shows the 'Cash Flow X' application window. At the top, there are three buttons: 'New Entry', 'Edit Entries', and 'Monthly Reports'. Below these is a section titled 'Transaction Details'. Inside this section, there are four input fields: 'Ammount' (with the value '123,456,123.00' and a currency dropdown set to 'EUR'), 'Description' (with the value 'ΤΑΔΕ2'), 'Date' (with the value '01/04/2016' and a calendar icon), and 'Type' (with a dropdown menu showing 'Loss'). At the bottom of the form are two buttons: 'Save' and 'Clear'.

Αυτή είναι η καρτέλα για επεξεργασία κάποιας εγγραφής αρχικά ο χρήστης επιλέγει την ημερομηνία και έπειτα η λίστα γεμίζει με τους κωδικούς των εγγράφων που χουν γίνει για την ημερομηνία αυτή και μπορεί από κει να επιλέξει κάποια και να την αλλάξει.



The screenshot shows the 'Cash Flow X' application window. At the top, there are three buttons: 'New Entry', 'Edit Entries', and 'Monthly Reports'. Below these is a section titled 'Select Accounting Record'. Inside this section, there are two input fields: 'Select record's date' (with a calendar icon) and 'Select record's id' (with a dropdown menu showing '...').



Εδώ αλλάξαμε λίγο την περιγραφή της εγγραφής και την ημερομηνία.

Cash Flow X

New Entry Edit Entries Monthly Reports

Select Accounting Record

Select record's date

27/05/2016

Select record's id

#9F64B43E149B

Transaction Details

Ammount

123,456,789.00 EUR

Description

ΤΑΔΑΙ

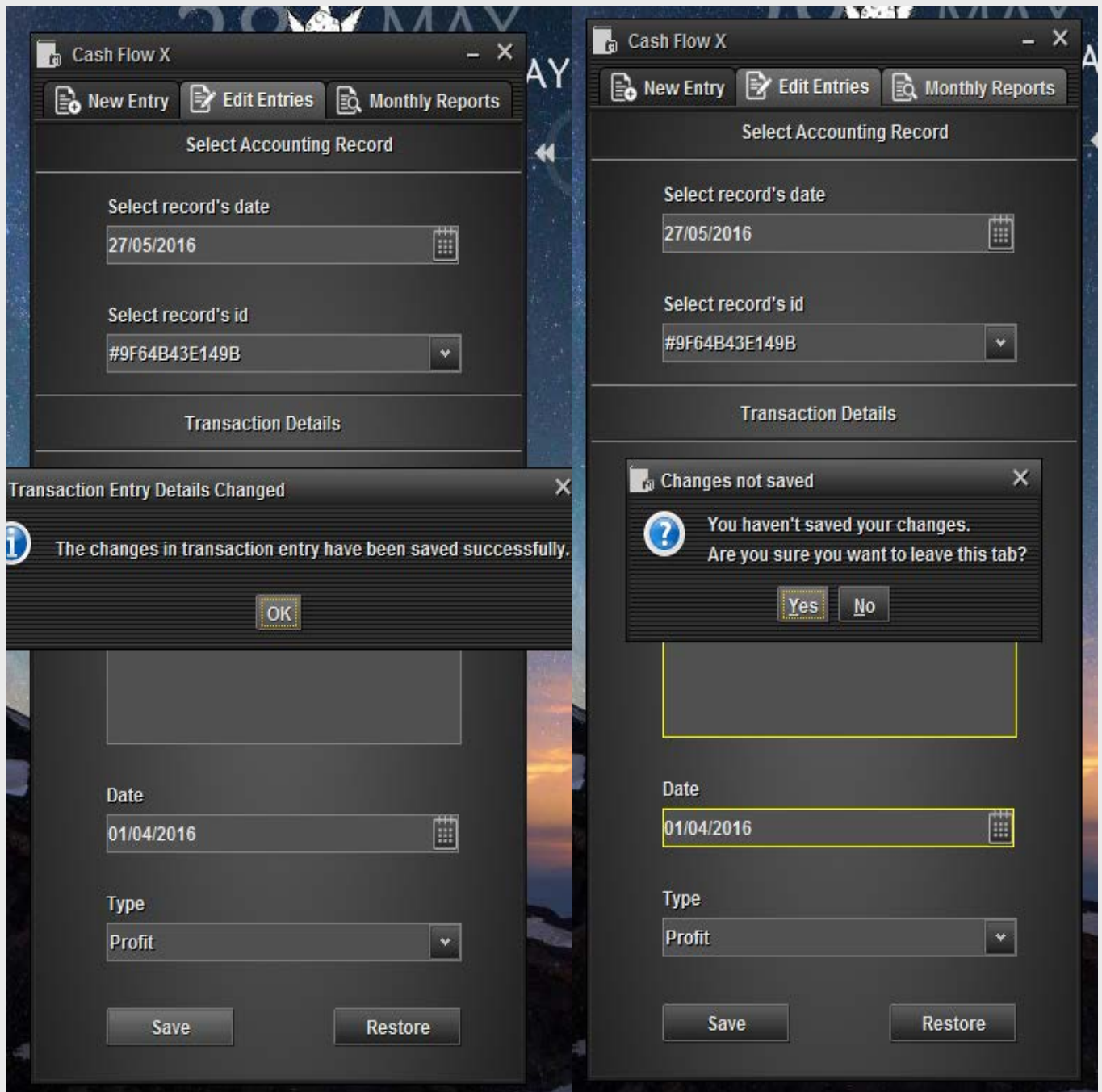
Date

01/04/2016

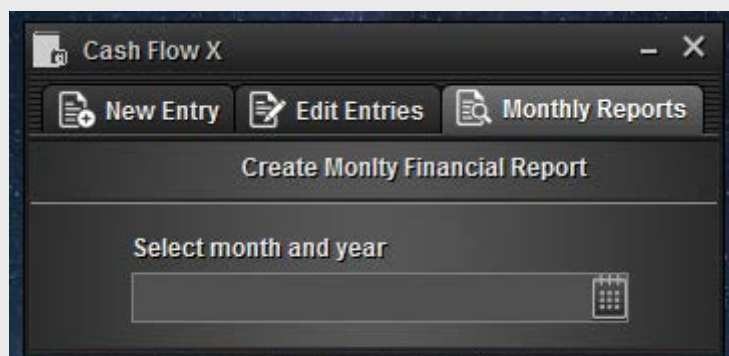
Type

Profit

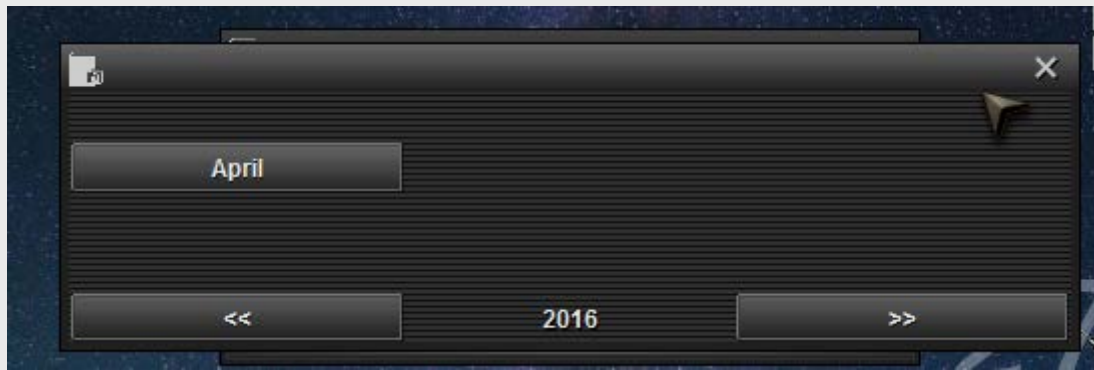
Save Restore



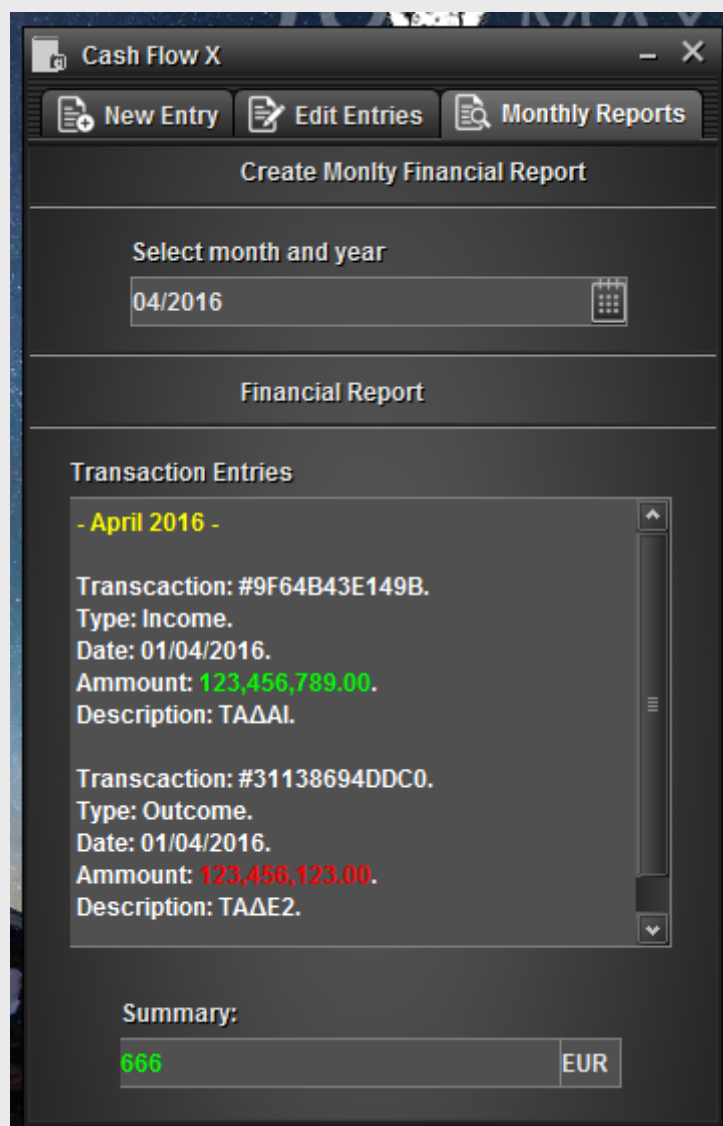
Και αυτή είναι η καρτέλα για δημιουργία οικονομικής αναφορά για κάποιον μηνά. Εδώ ο χρήστης πάλι μέσω ενός παράθυρου επιλεγεί τον μηνά που θέλει και εμφανίζεται η αφορά



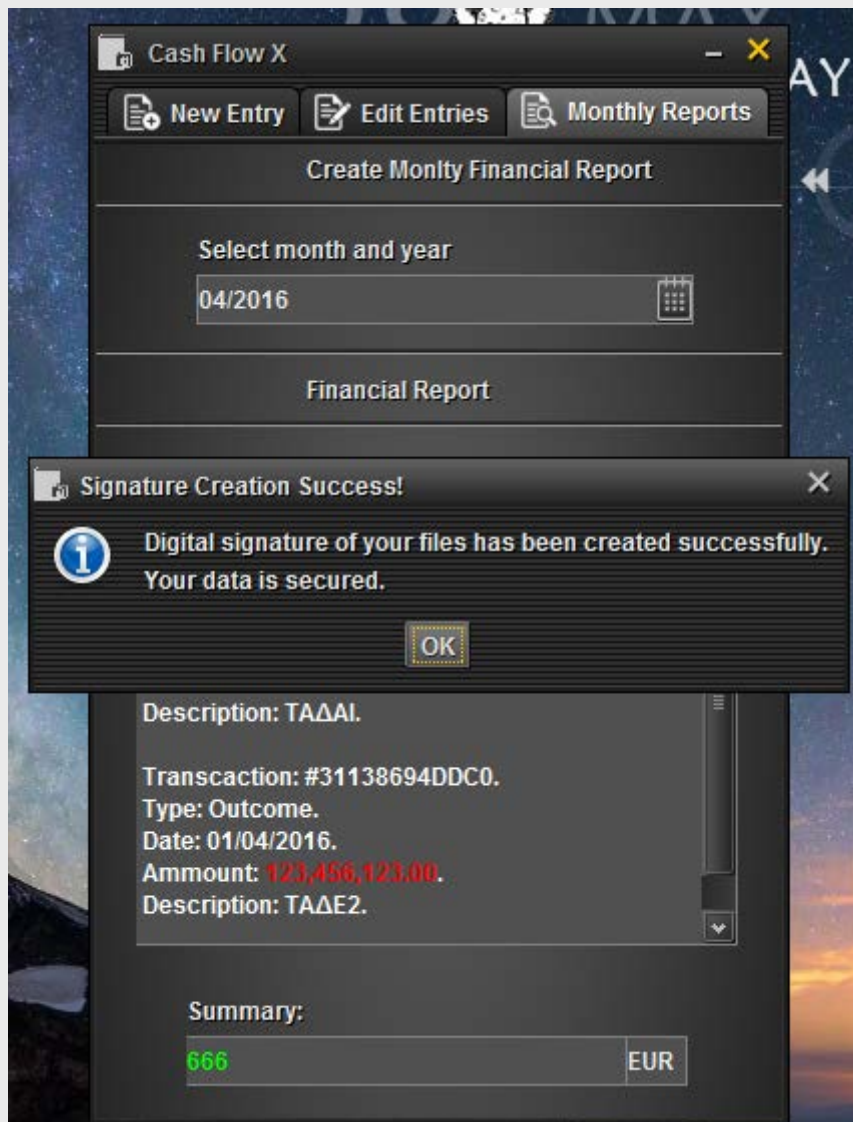
(Εμφανίζεται μονό ο Απρίλιος διότι μονό σε αυτόν τον μηνά έχουμε καταχωρήσει έγγραφες)



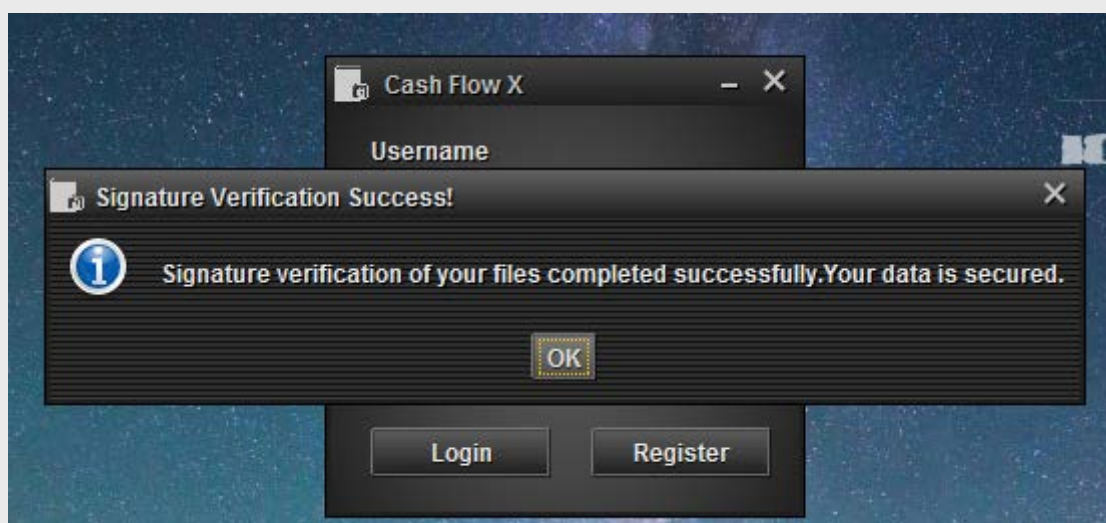
Και έτσι εμφανίζεται η οικονομική αναφορά. Αναλόγως αν είναι χασούρα η κέρδος μπαίνει και ανάλογο χρώμα στη γραμματοσειρά.



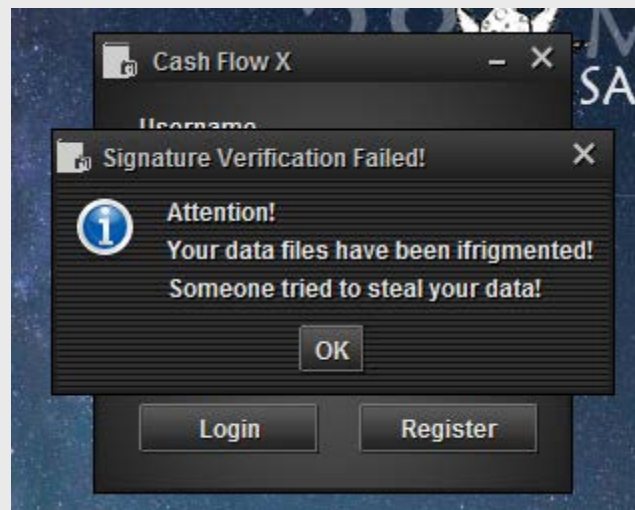
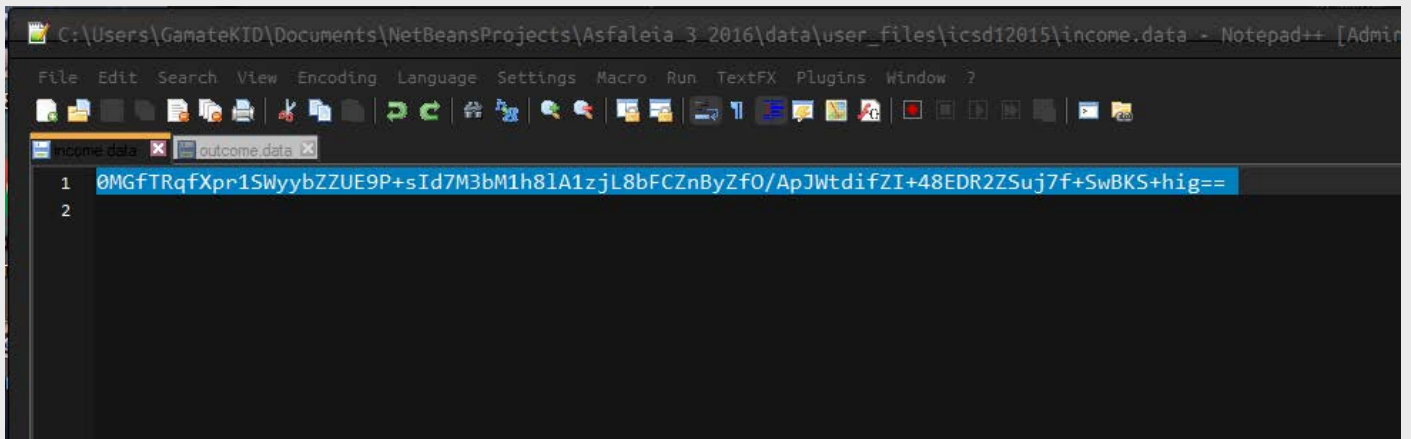
Κατά την έξοδο από την εφαρμογή ενεργοποιείται ο μηχανισμός ακεραιότητας και εμφανίζεται αντίστοιχο μήνυμα.



Όπως και στην έναρξη της εφαρμογής



Τώρα αν πειράξουμε κάποιο αρχείο δεδομένων για παράδειγμα άμα σβήσουμε τη μια από τις δυο έγγραφες η εφαρμογή θα το καταλάβει και θα μας ενημερώσει.



Σημείωση: τα γραφικά διορθωθήκαν λίγο μετά τα screenshots.