ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΜΕΣΟΛΟΓΓΙΟΥ

ΠΑΡΑΡΤΗΜΑ ΝΑΥΠΑΚΤΟΥ

ΤΜΗΜΑ ΤΗΛΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΔΙΚΤΥΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Ανάπτυξη εφαρμογής για κινητά τηλέφωνα προκειμένου να εμφανίζει στατιστικά και να διενεργεί αναλύσεις σε δείγμα data feed από τα public streams που παρέχει το Twitter

Συνοδινού Η. Αγγελική

Αριθμός Μητρώου: 0862

Επιβλέποντες καθηγητές:

Αλεφραγκής Παναγιώτης – Βώρος Νικόλαος

Ναύπακτος, 2013

«Ανάπτυξη εφαρμογής για κινητά τηλέφωνα προκειμένου να εμφανίζει στατιστικά και να διενεργεί αναλύσεις σε δείγμα data feed από τα public streams που παρέχει το Twitter»

Αγγελική Η. Συνοδινου

Ευχαριστίες

Η ολοκλήρωση αυτής της πτυχιακής υλοποιήθηκε με την υποστήριξη ενός αριθμού ανθρώπων στους οποίους θα ήθελα να εκφράσω τις θερμότερες ευχαριστίες μου.

Πρώτα από όλους θα ήθελα να ευχαριστήσω τους επιβλέποντες καθηγητές μου κ. Νικόλαο Βώρο και κ. Παναγιώτη Αλεφραγκή, οι οποίοι μου έδωσαν την ευκαιρία να εκπονήσω την παρούσα πτυχιακή εργασία.

Επίσης θα ήθελα να ευχαριστήσω θερμά τον κ. Ανδρέα Λάλο για την πολύτιμη καθοδήγησή του η οποία συνέβαλε τα μέγιστα στην ολοκλήρωσή της εργασίας.

Τέλος θα ήθελα να ευχαριστήσω τους γονείς μου για την πίστη τους στο πρόσωπό μου, τις αδερφές μου Άννα και Ελευθερία που κάνουν τη ζωή μου ομορφότερη, καθώς επίσης και τους φίλους μου Κωνσταντίνα, Λένια, Άννα και Μπάμπη που με κάνουν να θυμάμαι ότι τα ομορφότερα πράγματα στη ζωή δεν είναι καν πράγματα!

Αγγελική Η. Συνοδινού

Πίνακας περιεχομένων

Περιεχόμενα

Πίνακας Εικόνων

Εισαγωγή

Η παρούσα πτυχιακή εργασία αποτελεί τη συρραφή τριών φαινομενικά ετερόκλητων θεμάτων. Συγκεκριμένα η θεματολογία της είναι η εξής:

- Το εργαλείο αναζήτησης και ανάλυσης δεδομένων Splunk
- Το κοινωνικό δίκτυο Twitter
- Το λειτουργικό σύστημα Android

Ο τελικός στόχος του εν λόγω εγχειρήματος είναι η ανάπτυξη μιας εφαρμογής η οποία θα επικοινωνεί με μια πλατφόρμα συλλογής και ανάλυσης δεδομένων προσφέροντας στους χρήστες κινητών συσκευών με λειτουργικό σύστημα Android τη δυνατότητα να λαμβάνουν στατιστικά και αναλύσεις, σχετικά με τα public streams που παρέχει το κοινωνικό δίκτυο Twitter. Ωστόσο πέραν αυτού, στο θεωρητικό κομμάτι της εργασίας αναλύονται έννοιες που αφορούν τα προαναφερθέντα θέματα, οι οποίες αποτελούν το θεμέλιο λίθος αυτής της εργασίας.

Τα συστήματα πληροφορικής παράγουν δεδομένα κάθε δευτερόλεπτο της ημέρας. Τα μηχανικά αυτά δεδομένα περιέχουν εγγραφές σχετικά με τις συμπεριφορές των χρηστών, τα επίπεδα ασφαλείας, κινδύνους στον κυβερνοχώρο, ενέργειες απάτης και πολλά άλλα. Την ανάγκη ταχείας συλλογής, ανάλυσης και οπτικοποίησης αυτών των δεδομένων έρχεται να καλύψει το εργαλείο Splunk, το οποίο παρέχει οργάνωση και εξαγωγή πληροφοριών σε πραγματικό χρόνο, μέσα από τεράστιο όγκο δεδομένων μηχανής, προερχόμενα από διαφορετικές πηγές.

Η ραγδαία αύξηση χρήσης των κοινωνικών δικτύων αποτελεί σημαντικό παράγοντα, με ισχυρή επίδραση πέρα από τον τομέα της ψυχαγωγίας, στις κοινωνικές και τεχνολογικές εξελίξεις. Αυτή η εργασία επικεντρώνεται σε ένα από τα μεγαλύτερα κοινωνικά δίκτυα, το Twitter, που λόγω των ιδιαίτερων χαρακτηριστικών και του μεγάλου όγκου πληροφοριών που προσφέρει αποτελεί μια σημαντική πηγή συλλογής και ανάλυσης δεδομένων με σκοπό την εξαγωγή διάφορων χρήσιμων συμπερασμάτων.

Από την άλλη πλευρά, η δυναμική είσοδος του Android στην αγορά και ο μεγάλος αριθμός του αγοραστικού κοινού του, αποτελεί πρόκληση για κάθε προγραμματιστή να αναπτύξει καινοτόμες και χρήσιμες εφαρμογές, καλύπτοντας τις ανάγκες ακόμα και του πιο απαιτητικού χρήστη.

Η παρούσα εργασία οργανώνεται ως εξής:

- Στο κεφάλαιο 1 παρουσιάζεται το λογισμικό αναζήτησης Splunk. Καταγράφονται τα βασικά χαρακτηριστικά και οι λειτουργίες του σε θεωρητικό και πρακτικό επίπεδο. Μέσω παραδειγμάτων εξηγείται συνοπτικά ο τρόπος χρήσης του.

- Στο κεφάλαιο 2 γίνεται μια συνοπτική αναφορά στην έννοια των κοινωνικών δικτύων. Τονίζεται η σημασία τους και παρουσιάζεται το Twitter και οι δυνατότητες παροχών του στο χρήστη.

- Στο κεφάλαιο 3 γίνεται μία ολοκληρωμένη παρουσίαση του λειτουργικού συστήματος Android. Καταγράφεται η εξέλιξη του όπως αποτυπώνεται από τις διάφορες εκδόσεις του και γίνεται αναφορά σε θέματα ασφαλείας και προστασίας προσωπικών δεδομένων .

- Στο κεφάλαιο 4 γίνεται παρουσίαση της εφαρμογής που αναπτύχθηκε στα πλαίσια της παρούσας πτυχιακής εργασίας. Αναλύεται ο τρόπος δημιουργίας της καθώς και ο τρόπος χρήσης της.

- Στο κεφάλαιο 5 αναφέρονται τα συμπεράσματα που εξάγονται από αυτή την προσπάθεια και γίνονται προτάσεις για μελλοντική έρευνα και ανάπτυξη πάνω στο παρόν θέμα.

Κεφάλαιο 1

Splunk

Επισκόπηση του Splunk

Το Splunk είναι ένα ισχυρό και ευέλικτο λογισμικό αναζήτησης που χρησιμεύει στην εξερεύνηση τεράστιου όγκου δεδομένων σε πολύ μικρό χρόνο. Αξιοποιεί το σύνολο των δεδομένων και εξάγει χρήσιμες πληροφορίες, δίνοντας στο χρήστη τη δυνατότητα να εντοπίσει μοτίβα, συσχετίσεις και ευκαιρίες για περαιτέρω ανάλυση με εύκολο και γρήγορο τρόπο χωρίς να χρειάζεται να χρησιμοποιήσει περίπλοκες βάσεις δεδομένων και ειδικές μονάδες ελέγχου και ανάλυσης. Το μόνο που απαιτείται είναι ένα πρόγραμμα περιήγησης στο διαδίκτυο κι όλα τα υπόλοιπα τα αναλαμβάνει το Splunk!

Για να γίνει πιο κατανοητή η έννοια του Splunk παρακάτω παρουσιάζονται μερικές από τις λειτουργίες που προσφέρει:

- Διαρκής καταχώρηση του συνόλου των δεδομένων σε πραγματικό χρόνο.
- Αυτόματη ανακάλυψη των χρήσιμων πληροφοριών που βρίσκονται ενσωματωμένες στα δεδομένα, γλιτώνοντας το χρήστη από τον κόπο να χρειαστεί να τα ανακαλύψει χειροκίνητα μέσω χρονοβόρων διαδικασιών και περίπλοκων εργαλείων.
- Αναζήτηση στη φυσική και εικονική υποδομή των πληροφοριακών δεδομένων για οτιδήποτε ενδιαφέρον, φέρνοντας αποτελέσματα σε λίγα μόλις δευτερόλεπτα.
- Αποθήκευση αναζητήσεων και προσθήκη ετικετών σε σημαντικές πληροφορίες καθιστώντας το σύστημα πιο έξυπνο.
- Ρύθμιση τακτικών και αυτοματοποιημένων ελέγχων συστήματος (ή δικτύου) για παρακολούθηση συγκεκριμένων και επαναλαμβανόμενων γεγονότων.

- Δημιουργία αναλυτικών αναφορών με τη μορφή διαδραστικών γραφημάτων και πινάκων.
- Κοινοποίηση αποθηκευμένων αναζητήσεων και αναφορών μέσω ηλεκτρονικού ταχυδρομείου, σε συναδέλφους και άλλους χρήστες του Splunk για ομαδική γνωστοποίηση και μελέτη των αποτελεσμάτων.
- Εξέταση κατάστασης πληροφοριακού συστήματος με σκοπό την αποτροπή διακοπών λειτουργίας των διακομιστών καθώς και του εντοπισμού συμβάντων που αποτελούν απειλή για το σύστημα.
- Σχεδιασμός εξειδικευμένων, πλούσιων σε πληροφορίες γραφημάτων και πινάκων (dashboards) που ανταποκρίνονται στις μοναδικές ανάγκες και απαιτήσεις του κάθε χρήστη ή επιχείρησης.

Σε ποιους απευθύνεται το Splunk

Το Splunk είναι ένα ευπροσάρμοστο εργαλείο το οποίο μπορεί να χρησιμοποιηθεί με ποικίλους τρόπους από ένα μεγάλο εύρος χρηστών διαφορετικών ειδικοτήτων και κλάδων. Διαχειριστές συστήματος (system administrators), αναλυτές ασφαλείας (security analysts), προσωπικό υποστήριξης δικτύου (network support staff) , μηχανικοί (service desk), διαχειριστές εταιρειών (managers), καθώς και το προσωπικό ανάπτυξης εφαρμογών (application support staff) Αυτές λοιπόν είναι μόνο λίγες από τις οι κατηγορίες χρηστών που χρησιμοποιούν το Splunk για να φέρουν εις πέρας την εργασία τους, αξιοποιώντας το ο καθένας με διαφορετικό τρόπο.

Παρακάτω θα εξετάσουμε με μεγαλύτερη λεπτομέρεια το τι προσφέρει το Splunk σε κάθε χρήστη ξεχωριστά, ανάλογα με την επαγγελματική του ιδιότητα.

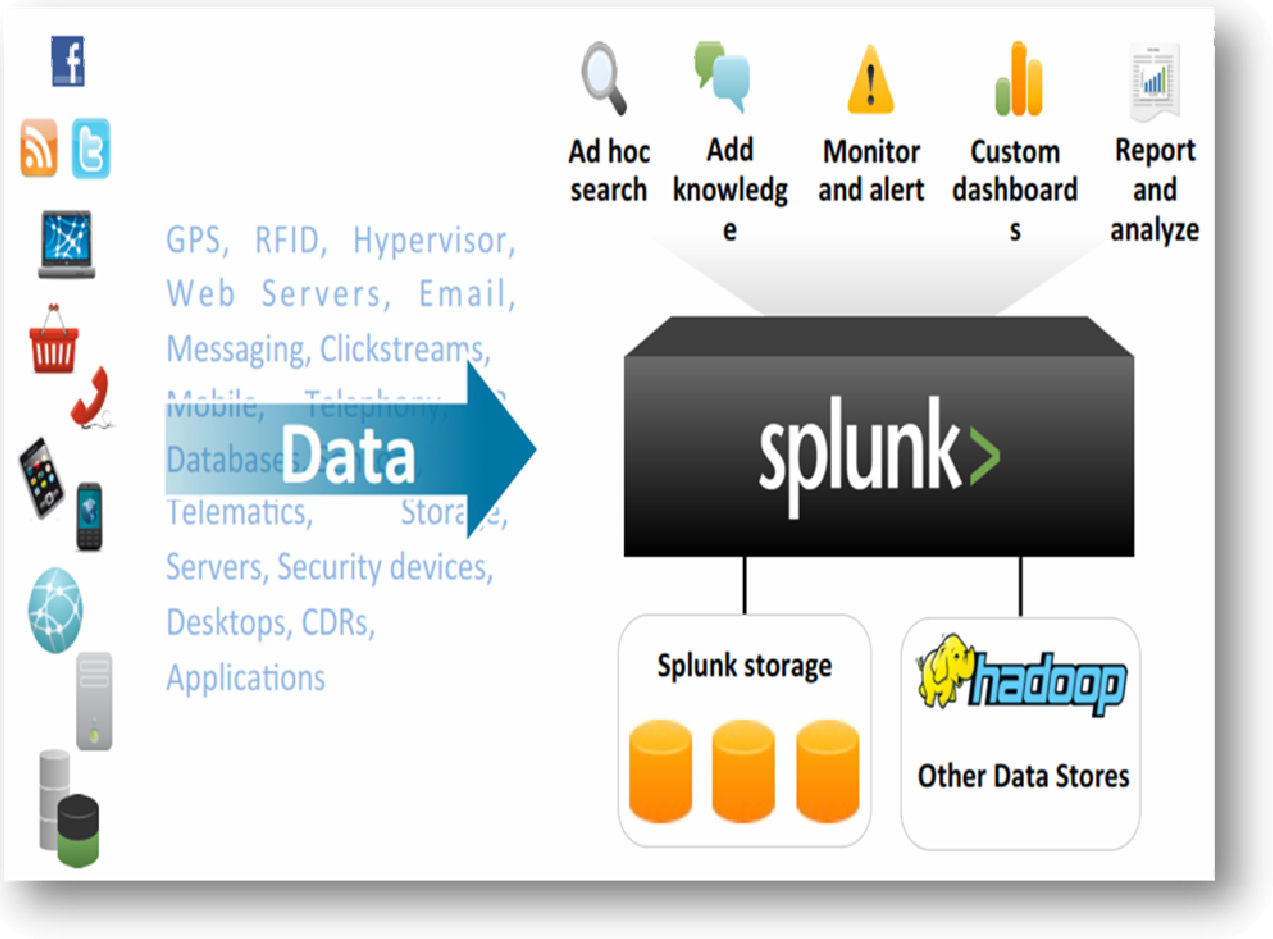
- Οι διαχειριστές του συστήματος (system administrators) και το προσωπικό (IT staff) μπορούν να χρησιμοποιήσουν το Splunk για να διερευνήσουν

προβλήματα στο Server, να κατανοήσουν τις διαμορφώσεις του συστήματος και να παρακολουθήσουν τη δραστηριότητα των χρηστών. Στη συνέχεια μετατρέπουν τις αναζητήσεις σε δυναμικές ειδοποιήσεις (alerts) οι οποίες τρέχουν στο παρασκήνιο και βρίσκονται σε επιφυλακή για τυχόν εντοπισμό κακής απόδοσης του συστήματος, λάθη και πιθανή υπερφόρτωση του

- Οι ανώτεροι μηχανικοί δικτύων (senior network engineers) χρησιμοποιούν το Splunk για τον προσδιορισμό γεγονότων και σεναρίων που συνήθως αποτελούν λόγους εμφάνισης προβλημάτων, όπως εσφαλμένες ρυθμίσεις δρομολογητών επιτρέποντας τους να αναγνωρίζουν και επιλύουν τεχνικά προβλήματα άμεσα, με ελάχιστο φόρτο ενασχόλησης περιορίζοντας όποιες δυσλειτουργίες αυτών και επιλύοντας τες έγκαιρα προτού υπάρξουν σημαντικές επίπτωση στους χρήστες και τις υπηρεσίες που υποστηρίζουν.
- Οι αναλυτές ασφαλείας (security analysts) και οι μηχανικοί ασφάλειας (security engineers) χρησιμοποιούν το Splunk για την παρακολούθηση συγκεκριμένων ομάδων χρηστών (tagged users) οι οποίοι έχουν πρόσβαση σε ευαίσθητα δεδομένα. Το Splunk καταγράφει και ελέγχει αυτόματα για κακόβουλες ροές δεδομένων και χρησιμοποιεί εξελιγμένους συσχετισμούς μέσω αναζήτησης για να εντοπίσει γνωστά μοτίβα κινδύνου όπως διαρροή δεδομένων, επιθέσεις, ακόμα και ενέργειες σε επίπεδο απάτης
- Οι διαχειριστές (managers) σε όλους τους τομείς κάνουν χρήση του Splunk για να δημιουργήσουν αναφορές και να έχουν πρόσβαση σε πίνακες εργαλείων (dashboards) που καταγράφουν την εύρυθμη λειτουργία, παρουσιάζουν δείκτες απόδοσης, μοτίβα εργασιών και αλληλεπιδράσεων εντός ή εκτός προκαθορισμένων ορίων των πληροφοριακών συστημάτων μιας επιχείρησης ή οργανισμού.
- Το προσωπικό ανάπτυξης εφαρμογών (application support staff) χρησιμοποιεί το Splunk για έρευνα και αποκατάσταση του περιβάλλοντος της εφαρμογής απ' άκρη σ' άκρη δημιουργώντας ειδοποιήσεις και πίνακες εργαλείων που παρακολουθούν ενεργά την απόδοση και διαθεσιμότητα των πόρων μιας ολόκληρης υπηρεσίας σε μια επιχείρηση διαχωρίζοντας τους χρήστες σε ομάδες με σκοπό κάθε ομάδα να έχει πρόσβαση σε συγκεκριμένα δεδομένα χωρίς να διακυβεύεται η ασφάλεια ευαίσθητων πληροφοριών από μη εξουσιοδοτημένους χρήστες.

Εισαγωγή δεδομένων στο Splunk

Το Splunk είναι μια εφαρμογή σχεδιασμένη να βοηθήσει το χρήστη να πάρει μια γενική εικόνα του τι συμβαίνει σε ένα πληροφοριακό σύστημα. Το Splunk λαμβάνει τα δεδομένα από σχεδόν οποιαδήποτε πηγή σε διαφορετικές μορφές. Τα δεδομένα αυτά μπορεί να προέρχονται από διακομιστές, βάσεις δεδομένων, δίκτυα, εικονικές μηχανές, εφαρμογές, κοινωνικά δίκτυα ακόμα και τηλεφωνικές επικοινωνίες. Τα εισάγει στο ευρετήριο, το οποίο είναι ουσιαστικά μια αποθήκη δεδομένων, με τη μορφή γεγονότων και τα καθιστά αναζητήσιμα. Τα ανεπεξέργαστα δεδομένα (raw data) μετατρέπονται σε γεγονότα (events) και αποθηκεύονται σε indexes. Το Splunk στη συνέχεια τακτοποιεί τα events με κριτήριο το χρόνο που συνέβησαν. Τα περισσότερα δεδομένα τοποθετούνται στα indexes αυτόματα, υπάρχουν όμως και δεδομένα τα οποία χρίζουν κάποιας επεξεργασίας προτού μετακινηθούν λόγω της μορφής τους.



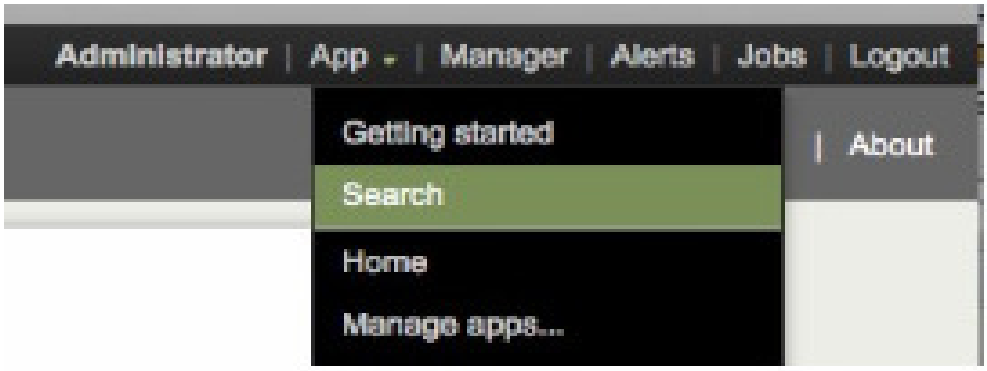
Εικόνα 1 Εισαγωγή δεδομένων στο Index

Ταμπλό αναζήτησης- Search app

Σε αυτή την ενότητα θα παρουσιαστεί με τη βοήθεια παραδείγματος το ταμπλό αναζήτησης του Splunk, ή αλλιώς το Search app, το οποίο αποτελεί την προεπιλεγμένη μηχανή για αναζήτηση στο interface του Splunk.

Ας υποθέσουμε ότι εργαζόμαστε στην ομάδα εξυπηρέτησης πελατών στο διαδικτυακό κατάστημα ***«Flowers & Gifts Shop».***

Για πρόσβαση στο ταμπλό αναζήτησης πηγαίνουμε στο μενού Apps στην γραμμή πλοήγησης του Splunk στην πάνω δεξιά γωνία της σελίδας και επιλέγουμε το υπομενού Search όπως φαίνεται στην εικόνα:

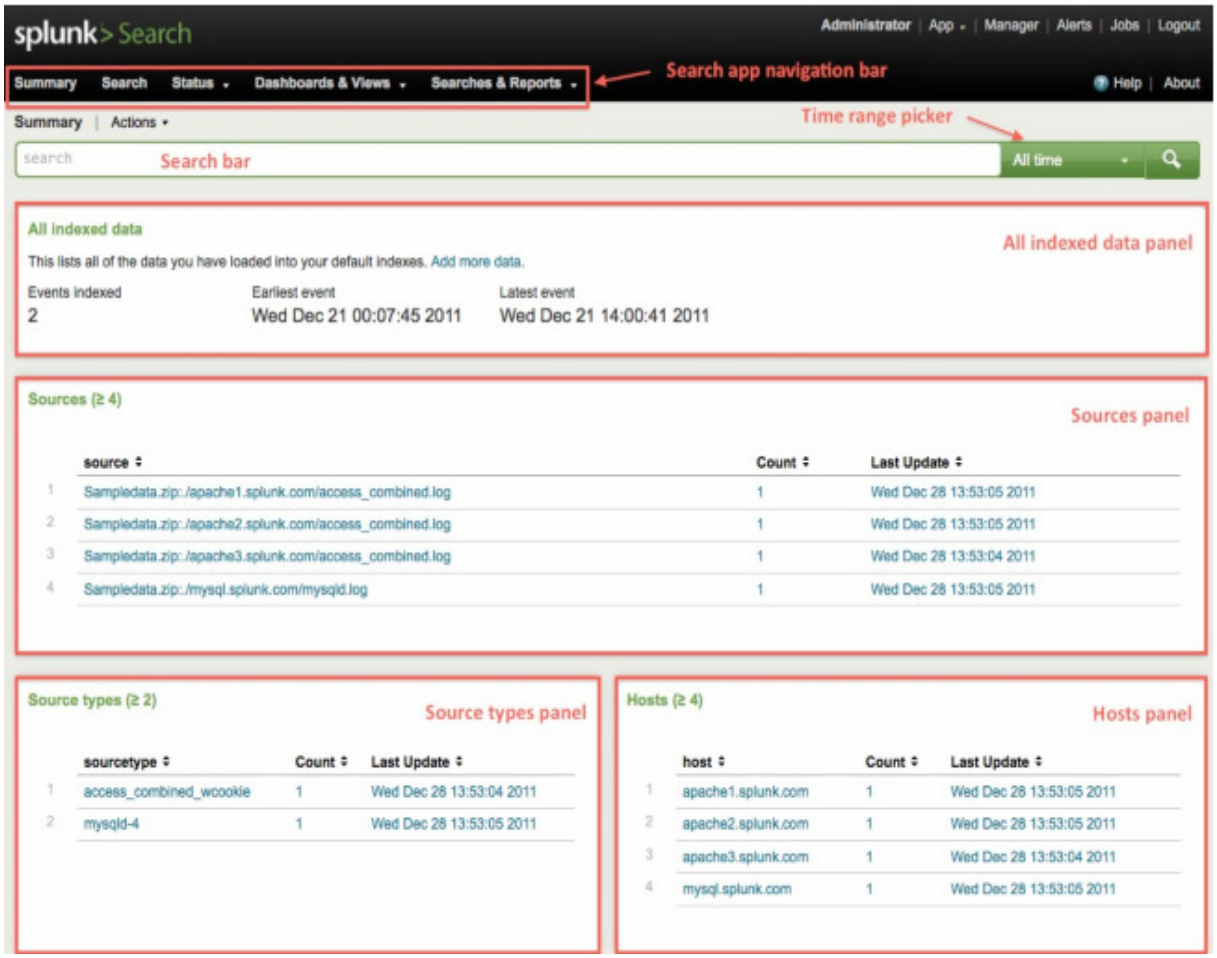


Το dashboard αναζήτησης (Summary dashboard) δίνει διάφορες επιλογές περιήγησης ανάμεσα στα υπάρχοντα στη μπάρα επιλογών dashboards. Εμφανίζει πληροφορίες σχετικά με τα δεδομένα που βρίσκονται στο Index και δίνει τα απαιτούμενα μέσα για την αναζήτηση αυτών των δεδομένων. Παρακάτω εξηγούνται συνοπτικά τα στοιχεία του μενού διεπαφής του χρήστη στο Summary όπως αυτά παρουσιάζονται στην εικόνα:

- **Searches & Reports**: περιέχει τη λίστα όλων των αποθηκευμένων αναζητήσεων και εκθέσεων δεδομένων που έχει οριστεί από το χρήστη.
- **Search bar and Time range picker:** η γραμμή στην οποία ο χρήστης έχει τη δυνατότητα να πληκτρολογήσει αναζητήσεις, οι οποίες αφορούν διαφορετικό χρονικό εύρος ανάκτησης δεδομένων κάθε φορά.

- **All indexed data panel:** παρουσιάζει πληροφορίες σχετικά με όλα τα δεδομένα που βρίσκονται στο Index, οι οποίες αφορούν τον αριθμό των events και τη χρονική περίοδο που εισήχθη το πιο πρόσφατο καθώς και το παλαιότερο event.
- **Sources panel:** παρουσιάζει τις δημοφιλέστερες πηγές από τις οποίες προέρχονται τα δεδομένα όπως π.χ syslog-ng, Files and directories, Windows Event Log data, Performance monitoring data κλπ.
- **Sourcetypes panel:** παρουσιάζει τους πιο δημοφιλείς τύπους των ροών δεδομένων που αρχειοθετεί σύμφωνα με την γραμμογράφηση και την πηγή των δεδομένων όπως π.χ apache_error για σφάλματα που συγκεντρώνονται από το error log του Apache web server ή asterisk_cdr για call detail records του Asterisk IP PBX

- **Hosts:** παρουσιάζει τα συστήματα (hosts) όπως διακομιστές και δικτυακές συσκευές , από όπου προέρχονται οι ροές δεδομένων. Από κάθε host μπορεί να εισρέουν δεδομένα από διαφορετικά sources με διαφορετικά sourcertypes.



Εικόνα 2 Splunk Summary Dashbord

Αναζήτηση και Διερεύνηση Δεδομένων

Αφού εισαχθούν τα δεδομένα του συστήματος στο Splunk μπορεί να ξεκινήσει η πανίσχυρη διαδικασία αναζήτησης για οτιδήποτε και όχι απλά έναν πεπερασμένο αριθμό προκαθορισμένων αποτελεσμάτων. Στις αναζητήσεις συνδυάζεται ο χρόνος με διάφορους όρους και περιορισμούς που θέτει ο χρήστης. Ακόμα και αν ένα σύστημα αποτελείται από terabytes στοιχείων το Splunk επιτρέπει την ακριβή και ταχεία αναζήτηση δεδομένων, δίνοντας τη δυνατότητα εξέτασης και εντοπισμού ή και πρόληψης τυχόν αποτυχίας του συστήματος παρουσιάζοντας τα συμβάντα λίγα δευτερόλεπτα πριν από αυτό για να αναζητηθούν τα αίτια και να γίνουν διορθώσεις.

Όταν πραγματοποιείται μια αναζήτηση στο Splunk, γίνεται ουσιαστικά μια αντιστοίχηση των όρων της αναζήτησης με τα τμήματα των δεδομένων ενός event. Τα events αποτελούν από μόνα τους μια εγγραφή δραστηριότητας. Το Splunk ξεχωρίζει τα events μεταξύ τους ανάλογα με τη χρονική στιγμή που συνέβησαν.

Εδώ είναι ένα δείγμα event:

172.26.34.223 - - [01/Jul/2005:12:05:27 -0700] "GET /trade/app?action=logout

HTTP/1.1" 200 2953

Τα events περιέχουν κομμάτια πληροφορίας ή πεδία. Όταν εισάγονται στοιχεία στο index, το Splunk εξάγει αυτόματα κάποια χρήσιμα στοιχεία, όπως για παράδειγμα την πηγή από την οποία προήλθε ένα event, τη μορφή του καθώς και το χρόνο που πραγματοποιήθηκε. Ο χρήστης έχει τη δυνατότητα να χρησιμοποιήσει ονόματα πεδίων (τα οποία συνήθως δηλώνουν τα χαρακτηριστικά του) είτε λέξεις κλειδιά για να τρέξει μια αναζήτηση η οποία θα επιστρέψει περιορισμένα αποτελέσματα που σχετίζονται άμεσα με τα στοιχεία που αναζητά εκείνη τη στιγμή.

Καθώς πραγματοποιείται μια αναζήτηση ο χρήστης αρχίζει να αναγνωρίζει μοτίβα και να προσδιορίσει περισσότερες πληροφορίες που θα μπορούσαν να φανούν χρήσιμες, όπως νέα αναζητήσιμα πεδία. Το Splunk μπορεί να ρυθμιστεί έτσι ώστε να

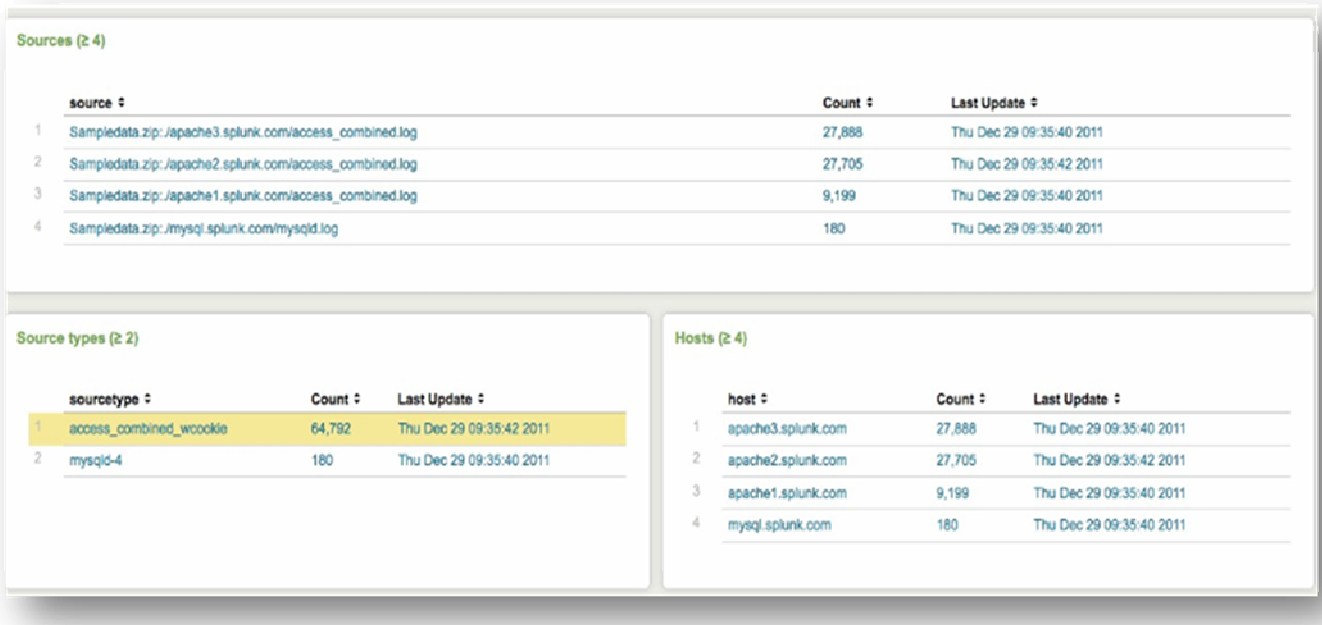
αναγνωρίζει αυτά τα πεδία κάθε φορά που θα εισέρχονται στο index νέα δεδομένα. Επίσης υπάρχει η δυνατότητα δημιουργίας νέων πεδίων κατά τη διάρκεια της αναζήτησης, τα οποία μπορούν να χρησιμοποιηθούν και να αξιοποιήσουν διαφορετικά τα αποτελέσματα της ανάλυσης των δεδομένων. Οι νέες πληροφορίες που προσφέρονται βοηθούν στην καλύτερη και αποτελεσματικότερη κατασκευή αναζητήσεων οδηγώντας στην οικοδόμηση λεπτομερών εκθέσεων.

Ξεκινώντας μία αναζήτηση

Τα βήματα που πρέπει να ακολουθήσει ο χρήστης προκειμένου να εκκινήσει τη διαδικασία αναζήτησης είναι τα ακόλουθα:

1. Με μια προσεκτική ματιά στο Sources panel του Summary dashboard βλέπουμε τρία αρχεία καταγραφής του διακομιστή Apache και ένα αρχείο καταγραφής βάσης δεδομένων mySQL για το ηλεκτρονικό κατάστημα **«Flowers & Gifts Shop»**

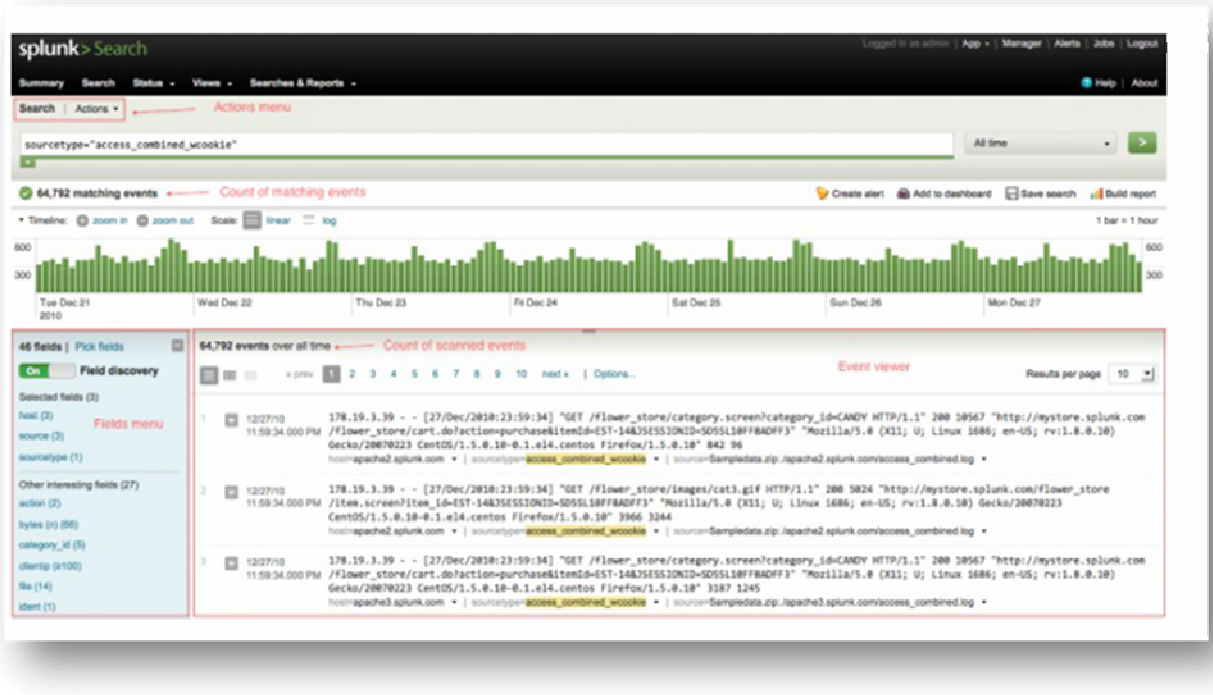
Οι εξοικειωμένοι χρήστες με τα αρχεία καταγραφής Apache θα αναγνωρίσουν στο source type panel τον τύπο *access_combined_wcookie* ως μια από τις μορφές



Εικόνα 3 Summary Dashboard (Λεπτομέρειες)

Η αναζήτηση στο Splunk είναι μια διαφραστική διαδικασία, όπου ο χρήστης μπορεί να πραγματοποιεί αναζητήσεις χωρίς να είναι απαραίτητο να γράφει εντολές αναζήτησης στην μπάρα αναζήτησης. Όλες οι πληροφορίες που υπάρχουν στους πίνακες sources, sourcetypes και hosts αποτελούν συνδέσμους(links) τους οποίους μπορεί να επιλέξει με ένα κλικ του ποντικιού και να πάρει χρήσιμα αποτελέσματα.

2. Στο *Sourcetypes* panel, επιλέγουμε τον τύπο access_combined_wcookie. Το Splunk μας οδηγεί στο dashboard της αναζήτησης εκεί όπου εμφανίζονται όλα τα αποτελέσματα.



Εικόνα 4 Προβολή αποτελεσμάτων αναζήτησης

Απόκτηση γνώσης

Η ελεύθερης μορφής αναζήτηση σε ανεπεξέργαστα δεδομένα (raw data) είναι μόνο η αρχή! Ο χρήστης προσθέτοντας τις δικές του γνώσεις πάνω στα πεδία και συμβάντα εμπλουτίζει αυτά τα δεδομένα και βελτιώνει το επίκεντρο των

αναζητήσεων του. Δίνοντας ετικέτα (tag) υψηλής προτεραιότητας σχολιάζει events σύμφωνα με τη λειτουργικότητα τους ή την απαίτηση τους για έλεγχο. Το Splunk ξεπερνά τις παραδοσιακές προσεγγίσεις στη διαχείριση αρχείων, χαρτογραφώντας τη γνώση που αποκτά κατά τη διάρκεια μιας αναζήτησης. Επιτρέπει το διαμοιρασμό των αναζητήσεων, αναφορών και των διαφόρων πινάκων εργαλείων (dashboards) σε όλο το φάσμα εφαρμογών που χρησιμοποιούνται από μια επιχείρηση ή οργανισμό.

Αυτοματοποιημένος έλεγχος

Κάθε αναζήτηση μπορεί να προγραμματιστεί να τρέχει σε κάποια συγκεκριμένα χρονικά διαστήματα και να ρυθμιστεί να επιστρέφει ειδοποιήσεις σχετικά με την κατάσταση ενός δικτύου ή περιβάλλοντος, όταν συναντά πληροφορίες οι οποίες πρέπει να γνωστοποιηθούν στο χρήστη. Αυτή η αυτοματοποιημένη λειτουργία ειδοποιήσεων μπορεί να χρησιμοποιηθεί σε ένα μεγάλο εύρος λειτουργιών και στοιχείων μιας IT υποδομής. Το Splunk παρέχει ειδοποιήσεις μέσω ηλεκτρονικού ταχυδρομείου ή μέσω SNMP (πρωτόκολλο ανταλλαγής πληροφοριών διαχείρισης μεταξύ των συσκευών ενός δικτύου) σε άλλες κονσόλες διαχείρισης. Ο χρήστης μπορεί να μεριμνήσει να λαμβάνει ειδοποιήσεις που αφορούν διάφορες αλλαγές πάνω στην ομαλή λειτουργία του συστήματος, όπως για παράδειγμα τη διακοπή λειτουργίας ενός server, καθώς και τη λήψη πληροφοριών για τυχόν διαρροή δεδομένων από το δίκτυο ή επιθέσεων που προέρχονται από εξωτερικούς παράγοντες.

Ανάλυση και έκθεση αποτελεσμάτων - Analyze and Report

Η δυνατότητα του Splunk να αναλύει γρήγορα τεράστιες ποσότητες δεδομένων επιτρέπει στο χρήστη να συνοψίζει τα αποτελέσματα από όλες τις αναζητήσεις με τη μορφή διαδραστικών πινάκων, γραφημάτων και διαγραμμάτων. Οι αναφορές χρησιμοποιούν στατιστικές εντολές για τη μέτρηση των «τάσεων» (trends)

που επικρατούν στον κόσμο των δεδομένων, συγκρίνουν τις ανώτατες τιμές τους και προχωρούν στην έκθεση των πιο διαδεδομένων από αυτά σε διάφορες μορφές διαγραμμάτων.

Το Splunk προσφέρει μια ποικιλία τρόπων για κοινή χρήση των αναφορών μεταξύ των μελών μιας ομάδας ή των συμμετεχόντων ενός έργου. Μπορούν να ρυθμίσουν το Splunk να πραγματοποιεί προγραμματισμένες αναφορές και τα αποτελέσματα αυτών να αποστέλλονται μέσω ηλεκτρονικού ταχυδρομείου όπως έχει προαναφερθεί στις προηγούμενες ενότητες, να εκτυπώνονται, να αποθηκεύονται σε συλλογές εκθέσεων της κοινότητας (συνήθως κοινότητα αποτελεί μια επιχείρηση) και να προστίθενται σε εξειδικευμένα dashboards για γρήγορη αναφορά.

Παράδειγμα χρήσης του Splunk

Κάνοντας χρήση του παραδείγματος του διαδικτυακού καταστήματος που προαναφέρθηκε, μέσω μιας σειράς απλών αναζητήσεων στο Search Interface θα γίνει πιο κατανοητή η λειτουργία του εργαλείου Splunk.

Το διαδικτυακό κατάστημα ***«Flowers & Gifts Shop»*:**

Είναι η πρώτη ημέρα εργασίας μας στην ομάδα υποστήριξης πελατών του ηλεκτρονικού καταστήματος «***Flowers & Gifts Shop»*** και μόλις έχουμε ξεκινήσει να εξερευνούμε τα access logs(τα δεδομένα που προκύπτουν από την κίνηση των πελατών στο κατάστημα), όταν ξαφνικά λαμβάνουμε κλήση από ένα πελάτη ο οποίος διαμαρτύρεται ότι κατά την ολοκλήρωση της παραγγελίας του λαμβάνει μήνυμα σφάλματος από το server με αποτέλεσμα να ακυρώνεται όλη η διαδικασία και μας δίνει την IP διεύθυνση του η οποία είναι 10.2.1.44.

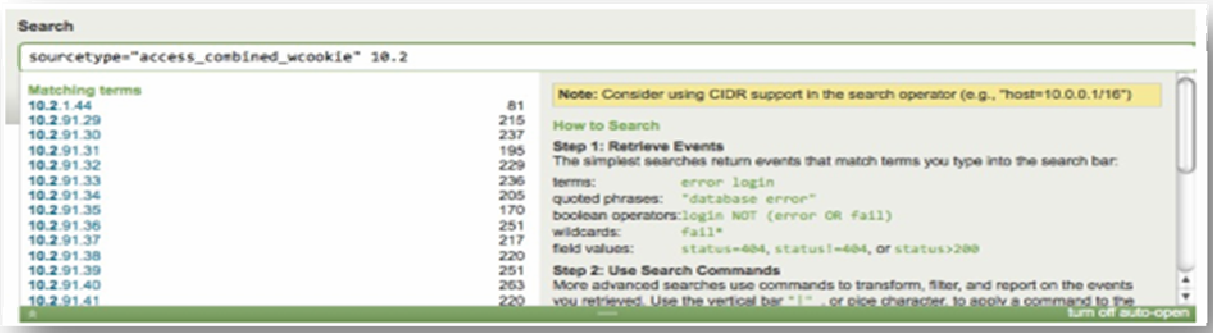
Τα πάντα στο Splunk είναι διαθέσιμα προς αναζήτηση. . Δεν χρειάζεται κάποιος να είναι εξοικειωμένος με τις πληροφορίες που δίνουν τα δεδομένα διότι η αναζήτηση είναι απλή, φτάνει να πληκτρολογήσουμε τις κατάλληλες λέξεις κλειδιά στη γραμμή αναζήτησης και να πατήσουμε το Enter (ή το πράσινο βέλος στο τέλος της γραμμής αναζήτησης). Σε προηγούμενο παράδειγμα τρέξαμε μια αναζήτηση κάνοντας κλικ στο web access source type (access_combined_wcookie) η οποία αφορούσε όλα τα δεδομένα που έχουν σχέση με την πρόσβαση των πελατών στο

ηλεκτρονικό κατάστημα. Θα κάνουμε χρήση της ίδιας εντολής με σκοπό τη μελέτη του ιστορικό πρόσβασης του συγκεκριμένου πελάτη.

1. Πληκτρολογούμε την Ip διεύθυνση του πελάτη στη γραμμή αναζήτησης:

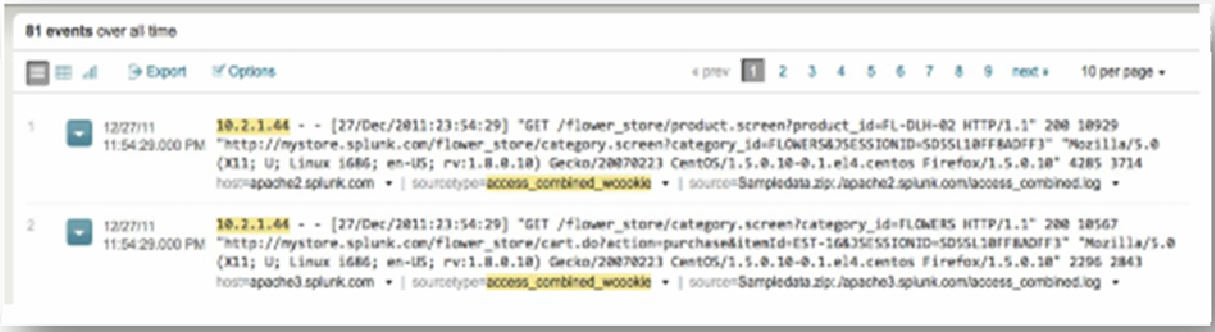
sourcetype=access_combined_wcookie 10.2.1.44

Καθώς πληκτρολογούμε την αναζήτηση ο βοηθός αναζήτησης του Splunk ανοίγει.



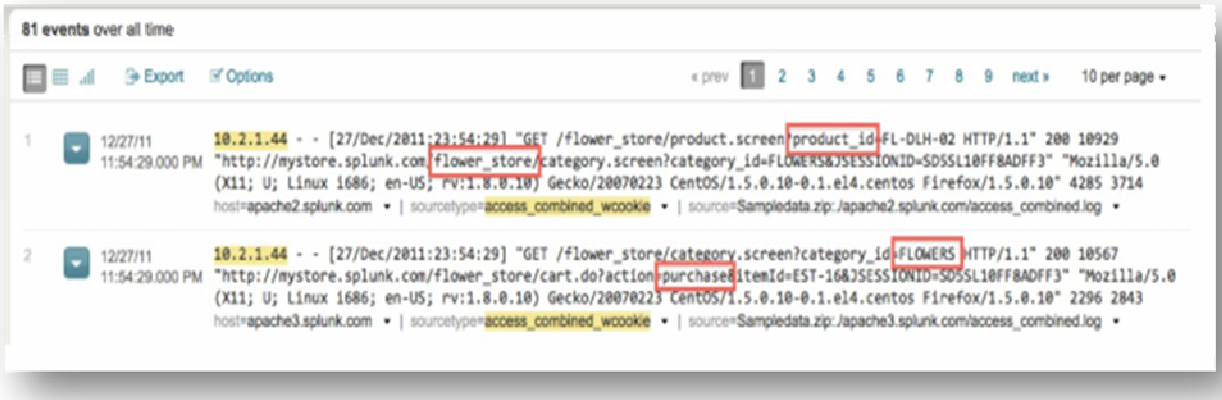
Ο οδηγός δείχνει αυτό που πληκτρολογούμε καθώς και προτεινόμενες Ip διευθύνσεις και παρόμοιες προτεινόμενες εντολές σύμφωνα με τις λέξεις κλειδιά που χρησιμοποιήσαμε. Επίσης παρουσιάζει τον αριθμό των αποτελεσμάτων που ταιριάζουν με τη δική μας αναζήτηση ώστε να γνωρίζουμε εξαρχής πόσα αποτελέσματα θα επιστρέψει το Splunk. Εάν αυτή η αναζήτηση δεν υπάρχει στα δεδομένα μας τότε ο βοηθός αναζήτησης δε θα κάνει κάποια από τις παραπάνω ενέργειες.

2. Πατάμε Enter στην αναζήτηση της Ip του πελάτη και το Splunk φέρνει το ιστορικό πρόσβασης του στο online κατάστημα.



Το Splunk κάθε φορά που εκτελούμε μια αναζήτηση δίνει έμφαση στα αποτελέσματα που αφορούν την εντολή που πληκτρολογήσαμε στη γραμμή αναζήτησης όπως βλέπουμε και στην εικόνα.

3. Σε αυτό το σημείο θα εξετάσουμε τα αποτελέσματα της αναζήτησης. Θα πρέπει να αναγνωρίσουμε λέξεις-κλειδιά και φράσεις ανάμεσα στα events που σχετίζονται με το ηλεκτρονικό κατάστημα (λουλούδια, είδη δώρων, αγορές κλπ.).

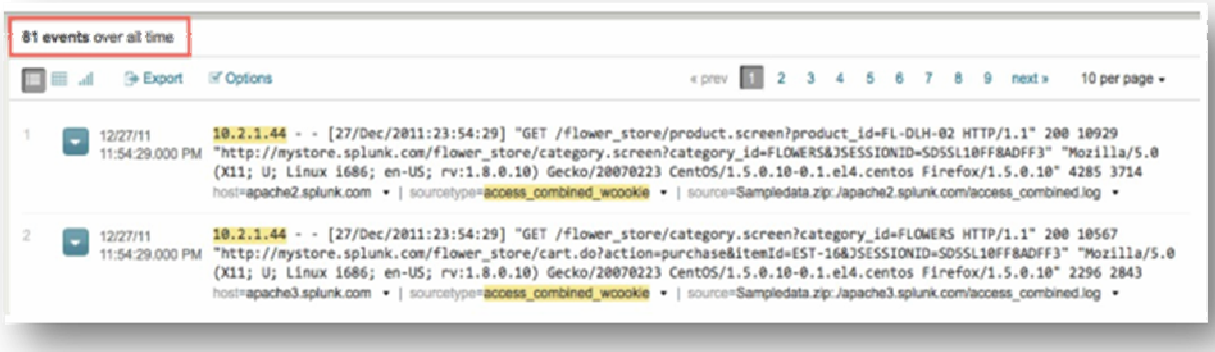


Ο πελάτης ανέφερε ότι βρισκόταν στη διαδικασία αγοράς δώρου, άρα η νέα μας αναζήτηση θα πρέπει να βασίζεται στη λέξη-κλειδί αγορά (purchase) .

4. Πληκτρολογούμε τη λέξη αγορά (purchase) στη μπάρα της αναζήτησης:

sourcetype=access_combined_wcookie 10.2.1.44 purchase

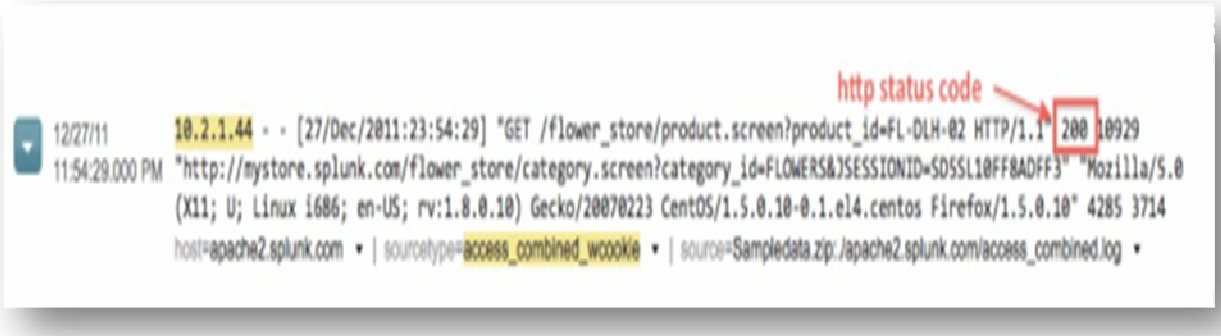
Όταν πραγματοποιείται μια αναζήτηση το Splunk δεν διακρίνει κεφαλαίους ή πεζούς χαρακτήρες και κάνει ανάκτηση των γεγονότων που περιέχουν τις λέξεις-κλειδιά οπουδήποτε μέσα στο ακατέργαστο κείμενο (raw data) των events.



Ανάμεσα στα αποτελέσματα που φέρνει το Splunk υπάρχουν events που δείχνουν κάθε φορά που ο πελάτης προσπάθησε να πραγματοποιήσει μια αγορά από το ηλεκτρονικό κατάστημα.

Χρήση Τελεστών Απόφασης

Με την αναζήτηση *access_combined* που πραγματοποιήσαμε παρατηρούμε ότι τα περισσότερα από τα αποτελέσματα περιέχουν την κατάσταση (status) HTTP 200 ή Successful(επιτυχής). Αυτό το status αναφέρεται στο Server του συστήματος. Τα αποτελέσματα που ψάχνουμε δεν αφορούν επιτυχή κατάσταση αύτη τη στιγμή αφού ο πελάτης ανέφερε πρόβλημα.

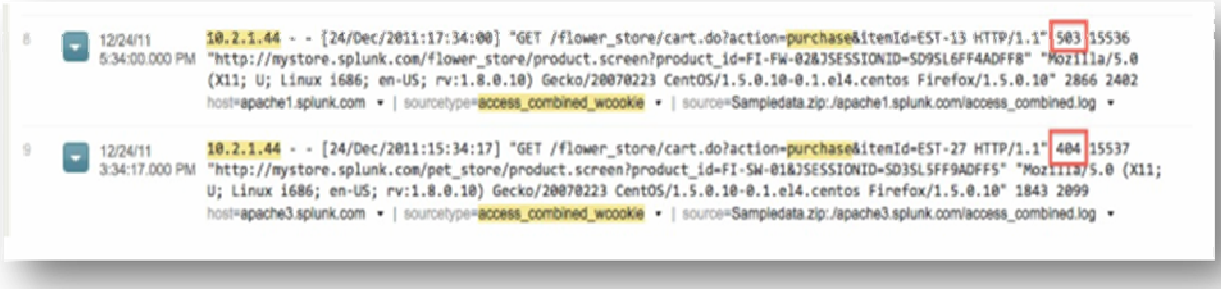


1. Εδώ μπορούμε να κάνουμε χρήση του τελεστή απόφασης NOT για να αφαιρεθούν οι επιτυχείς ενέργειες του πελάτη από τα αποτελέσματα.

   Πληκτρολογούμε λοιπόν:

   sourcetype=access_combined_wcookie 10.2.1.44 purchase NOT 200

Στα νέα αποτελέσματα παρατηρούμε ότι ο πελάτης λαμβάνει σφάλματα HTTP server(503) και client(404).

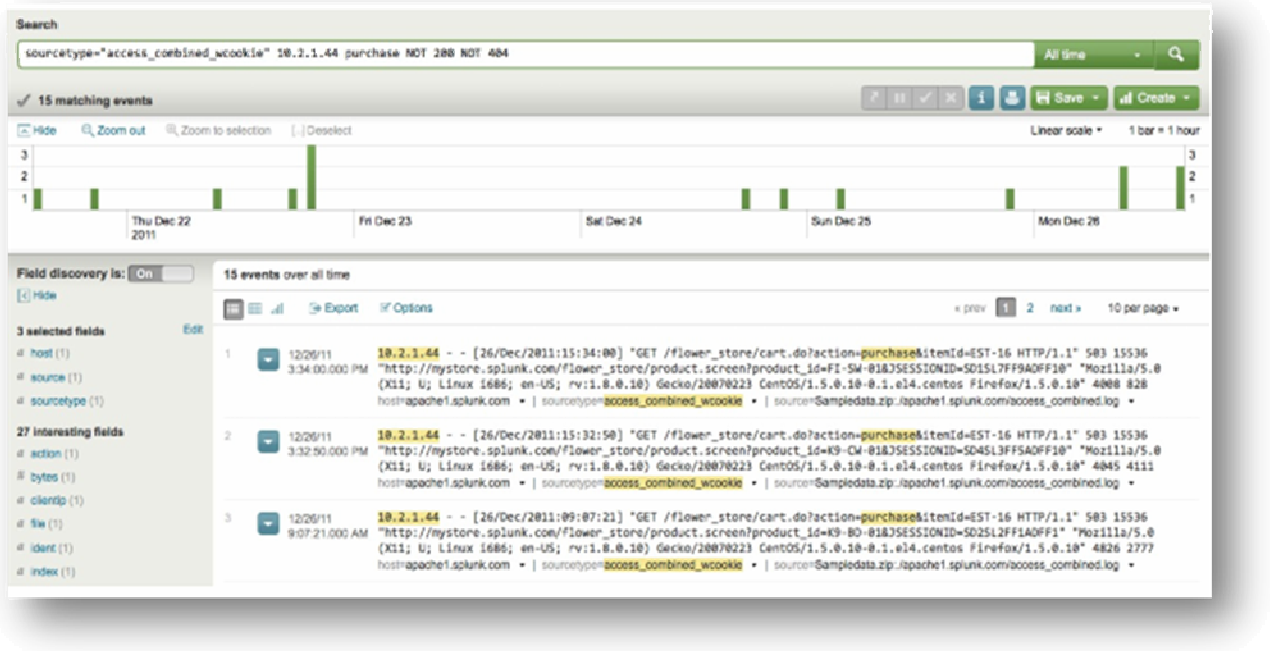


Συγκεκριμένα ανέφερε ότι λαμβάνει σφάλμα από το server επομένως μπορούμε να αφαιρέσουμε γρήγορα τα άσχετα με αυτό γεγονότα.

Ένας ακόμα τρόπος να χρησιμοποιήσουμε τελεστές απόφασης είναι να χρησιμοποιήσουμε τα ίδια τα αποτελέσματα της αναζήτησης.

2. Τοποθετούμε τον κέρσορα πάνω στο 404 στα αποτελέσματα και πατάμε Alt-click (για Windows ctrl-click). Αυτό διαμορφώνει την αναζήτηση σε :

sourcetype=access_combined_wcookie 10.2.1.44 purchase NOT 200 NOT 404



Από τα νέα αποτελέσματα που προκύπτουν βλέπουμε την ανεπιτυχή προσπάθεια του πελάτη να ολοκληρώσει την αγορά.Τώρα που επιβεβαιώθηκε ότι η αιτία ήταν όντως σφάλμα από το server μένει να ανακαλύψουμε τι ήταν αυτό που την προκάλεσε.

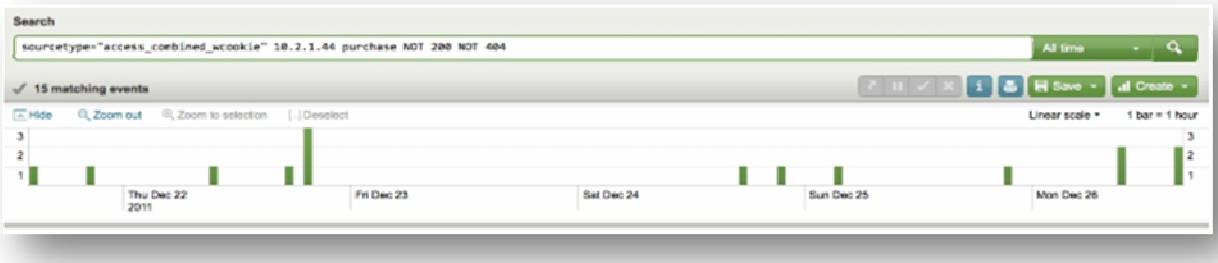
Ερεύνηση σφάλματος - Χρήση Timeline

Συνεχίζοντας με την προηγούμενη αναζήτηση που μας έδειξε την αποτυχή ολοκλήρωση αγοράς του πελάτη θα δούμε με ποιο τρόπο μπορούμε να

χρησιμοποιήσουμε το χρονολόγιο(Timeline) του Splunk για να πάρουμε περισσότερες πληροφορίες σχετικά με το συμβάν.

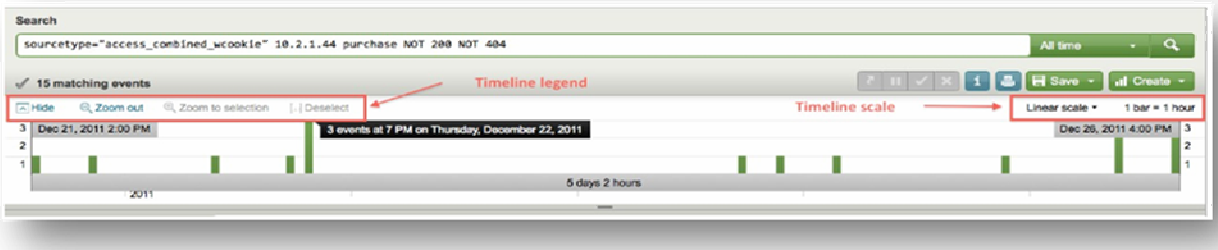
1. Επιστρέφουμε στην αναζήτηση:

sourcetype=access_combined_wcookie 10.2.1.44 purchase NOT 200 NOT 404



Η κάθε μπάρα αντιστοιχεί σε ένα event που αφορά την παρούσα αναζήτηση. Εάν δεν εμφανίζονται μπάρες τότε σημαίνει ότι δεν βρέθηκαν σχετικά γεγονότα.

2. Τοποθετούμε τον κέρσορα πάνω σε κάποια από τις μπάρες, ένα tooltip εμφανίζεται το οποίο παρουσιάζει τον αριθμό των events που βρήκε το Splunk τη συγκεκριμένη χρονική στιγμή (1 μπάρα= 1 ώρα).

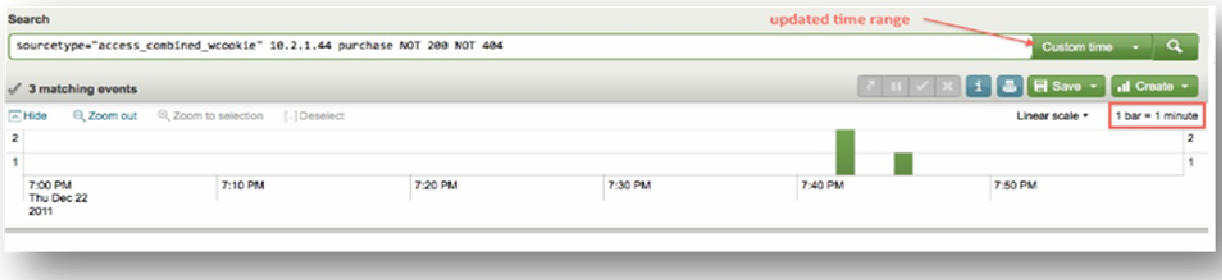


Όσο μεγαλύτερη εμφανίζεται η μπάρα τόσο περισσότερα events προέκυψαν εκείνη την ώρα.

3. Επιλέγουμε την υψηλότερη μπάρα αύτη τη φορά και κάνουμε κλικ πάνω σε αυτή. Αυτό ανανεώνει την αναζήτηση και εμφανίζει τα αποτελέσματα εμφανίζοντας μόνο αυτά που αφορούν το επιλεγμένο χρονικό εύρος. Το Splunk σε αυτή την περίπτωση δεν πραγματοποιεί νέα αναζήτηση απλά εμφανίζει τα αποτελέσματα με περισσότερες λεπτομέρειες.

4. Κάνουμε διπλό κλικ πάνω στην ίδια μπάρα.

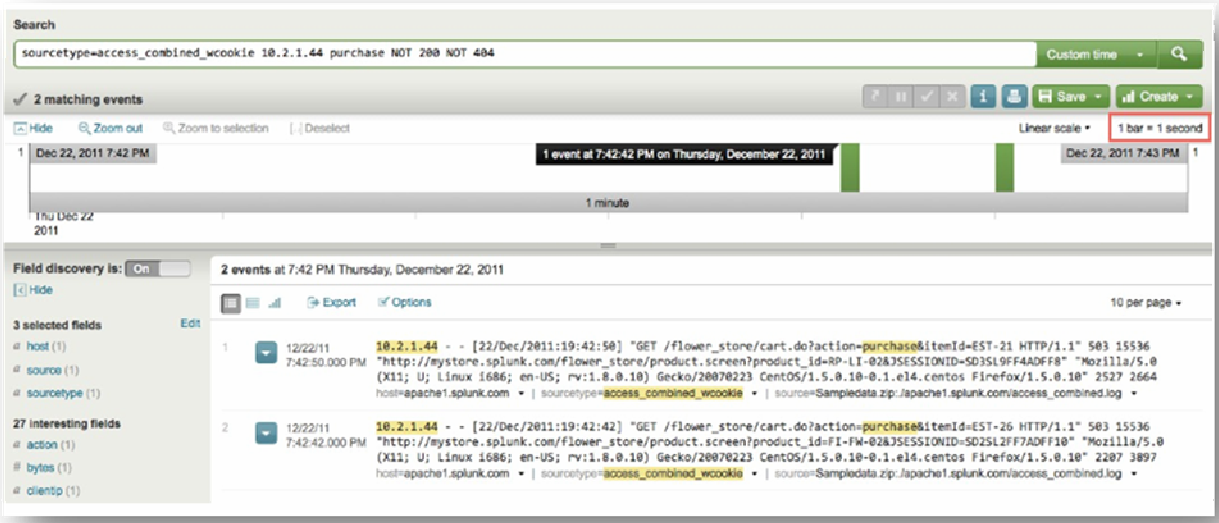
Το Splunk τρέχει νέα αναζήτηση και φέρνει μόνο τα αποτελέσματα για την ώρα που επιλέξαμε.



Τα αποτελέσματα της αναζήτησης είναι τα ίδια αλλά παρατηρούμε ότι ο χρόνος στη μπάρα αναζήτησης είναι custom. Κάθε μπάρα πλέον αντιπροσωπεύει ένα λεπτό της ώρας.

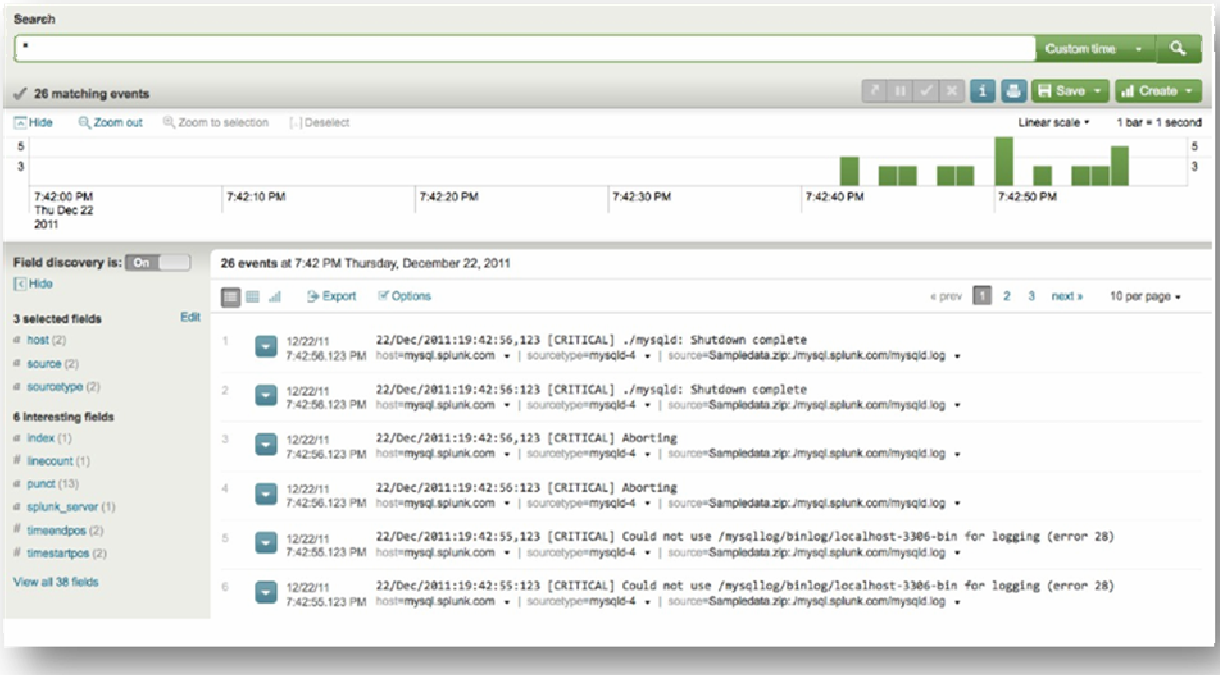
5. Κάνουμε διπλό κλικ πάνω σε κάποια άλλη μπάρα.

Το Splunk ανανεώνει την αναζήτηση. Κάθε μπάρα αντιπροσωπεύει τον αριθμό των γεγονότων που συνέβησαν κάθε δευτερόλεπτο του χρόνου.



6. Χωρίς να αλλάξουμε το χρόνο αντικαθιστούμε την προηγούμενη αναζήτηση με «*». Με αυτόν τον τρόπο θα δούμε τα γεγονότα που συνέβησαν το συγκεκριμένο λεπτό.

Ο αστερίσκος (*) στο Splunk φέρνει όλα τα αποτελέσματα που βασίζονται στις λέξεις-κλειδιά της αναζήτησης μας. Σε αυτή την περίπτωση ψάχνουμε για web access logs.



Η αναζήτηση αυτή φέρνει τελικά SQL database errors. Αυτά τα σφάλματα λοιπόν ήταν η αιτία που εμπόδιζε τον πελάτη να ολοκληρώσει την παραγγελία του. Το επόμενο βήμα είναι να αναφέρουμε το σφάλμα στους υπεύθυνους IT(IT operations team) για να επιληφθούν του θέματος.

Αλλαγή του χρονικού εύρους αναζήτησης

Υποθέτοντας ότι είμαστε πλέον αρκετά εξοικειωμένοι με το να τρέχουμε απλές αναζητήσεις, παρακάτω θα συνεχίσουμε να ασχολούμαστε με το παράδειγμα

του διαδικτυακού καταστήματος και θα εξετάσουμε πώς μπορούμε να περιορίσουμε τις αναζητήσεις μας επεμβαίνοντας στο πεδίο του χρόνου.

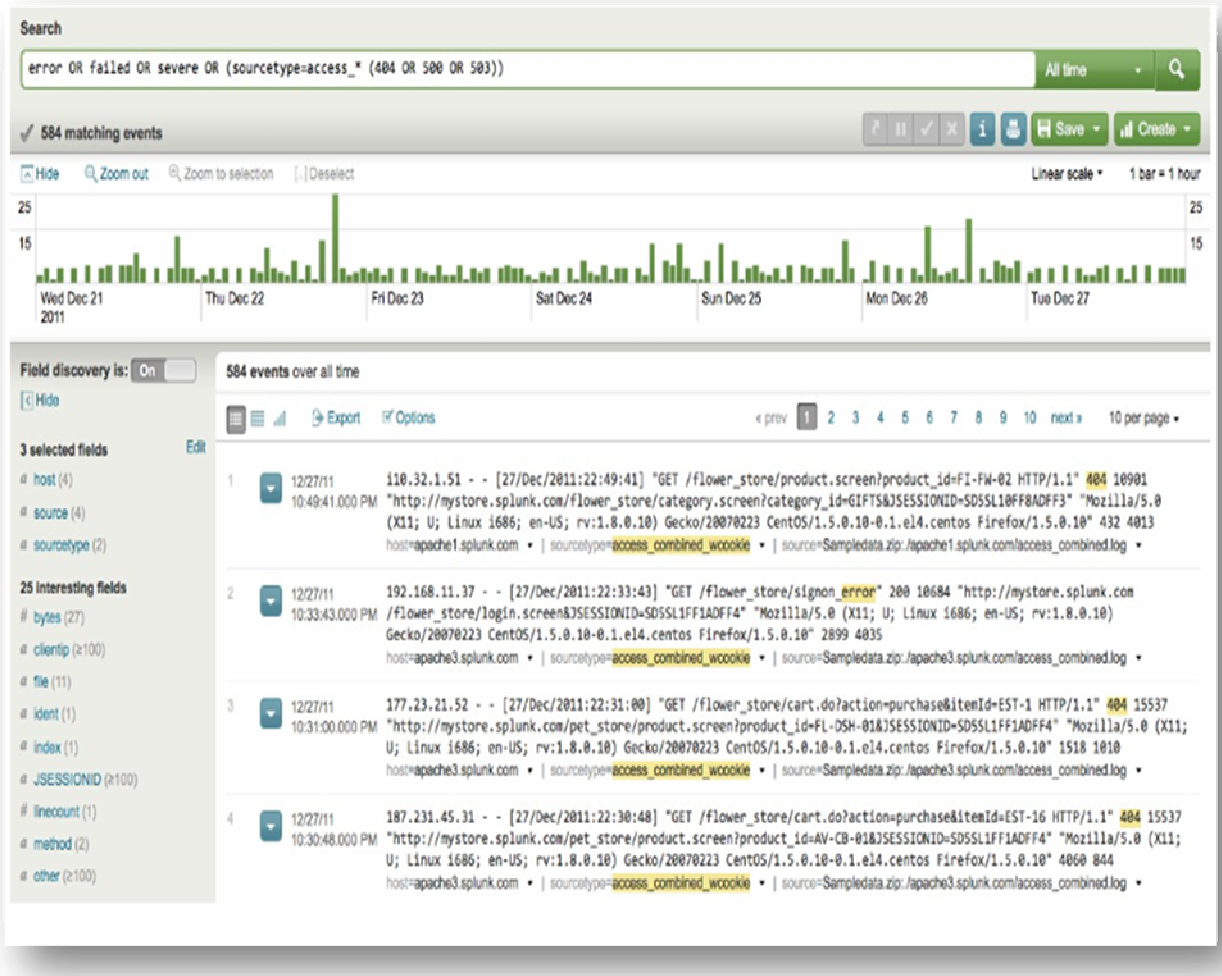
Βρισκόμαστε στη δεύτερη μέρα εργασίας μας στο ηλεκτρονικό κατάστημα ***«Flowers & Gifts Shop»*** «και αποφασίζουμε να τρέξουμε μια γρήγορη αναζήτηση ώστε να δούμε μήπως υπάρχουν πρόσφατα ζητήματα στην ομαλή λειτουργία του συστήματος για τα οποία θα πρέπει να είμαστε ενήμεροι.

1. Επιστρέφουμε στη γραμμή αναζήτησης και τρέχουμε την αναζήτηση:

error OR failed OR severe OR (sourcetype=access_* (404 OR 500 OR 503))

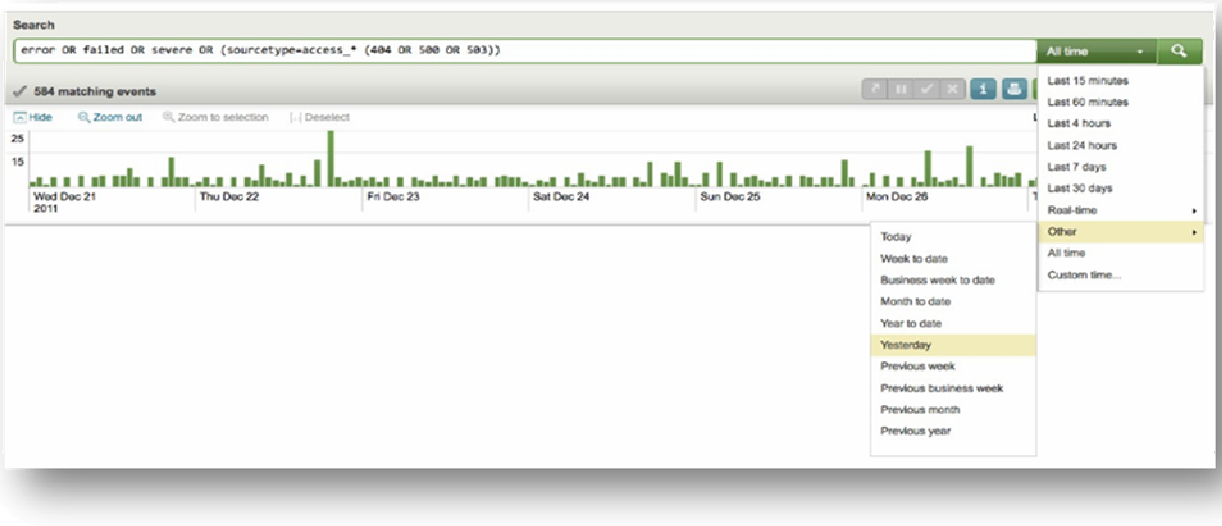
για το χρονικό εύρος All Time.

Αυτή η αναζήτηση χρησιμεύει στον εντοπισμό γενικών λαθών ανάμεσα στα events και επιστρέφει αποτελέσματα που περιέχουν τις λέξεις κλειδιά που εισάγαμε , οι οποίες φανερώνουν κάποιο γενικό σφάλμα ή κάποιο σφάλμα παρόμοιο με αυτό που αντιμετωπίσαμε παραπάνω, την προηγούμενη ημέρα σχετικά με τη συνεχή αποτυχία ολοκλήρωσης μια αγοράς λόγω σφάλματος που παρουσίαζε ο server.

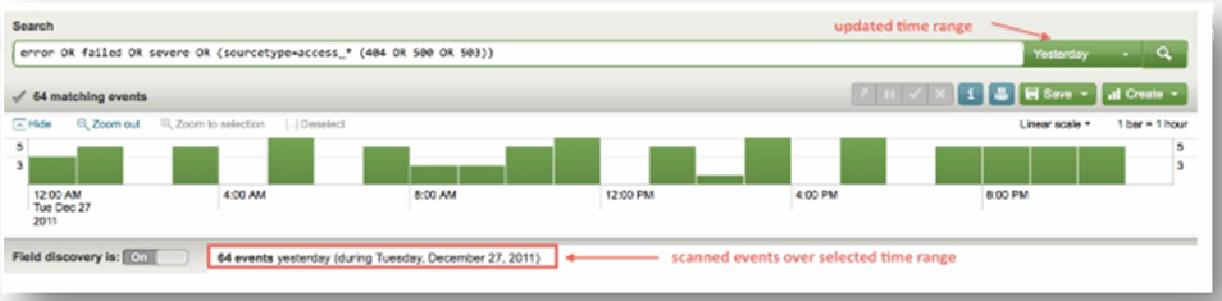


Είναι η δεύτερη ημέρα απασχόλησης μας άρα τα γεγονότα για τα οποία είμαστε υπεύθυνοι ξεκινούν από χθες.

2. Στη γραμμή αναζήτησης αλλάζουμε το χρόνο κάνοντας κλικ στο All Time→Other→Yesterday



**Το Splunk ψάχνει και αναλύει όλα τα δεδομένα του συστήματος με προεπιλογή χρόνου All time. Σε περίπτωση που ο όγκος των δεδομένων είναι πολύ μεγάλος και γίνει επιλογή μελέτης δεδομένων για τα τελευταία 15 λεπτά,την προηγούμενη ώρα, ημέρα ή εβδομάδα τότε υπάρχει πιθανότητα καθυστέρησης ανακτησης αποτελεσμάτων από τη μηχανή αναζήτησης*



3. Μετά την επιλογή ενός χρονικού εύρους από αυτή τη λίστα τότε η αναζήτηση τρέχει αυτόματα. Σε αντίθετη περίπτωση πατάμε το Enter.

Με αυτή την αναζήτηση παρατηρείται επιστροφή γενικών σφαλμάτων, όχι μόνο Web access logs που συνέβησαν την προηγούμενη ημέρα. Το επόμενο βήμα είναι να

ειδοποιηθεί το υπεύθυνο τμήμα επίλυσης σφαλμάτων ώστε να προχωρήσουν στη διόρθωσή τους.

Χρήση πεδίων

Συνεχίζοντας με το παράδειγμα του online καταστήματος σε αυτή την ενότητα θα εξηγηθεί τι είναι τα πεδία(fields) και πώς μπορούν να χρησιμοποιηθούν για να προσφέρουν χρήσιμες πληροφορίες σχετικά με τα διάφορα συμβάντα σε ένα σύστημα.

Τα πεδία είναι αναζητήσιμες τιμές και ονόματα ανάμεσα στα events τα οποία αναζητούνται μέσω του ονόματος τους. Παραδείγματα πεδίων αποτελούν το όνομα ενός server, το όνομα ή ο τύπος ενός αρχείου, κατηγορίες χρηστών κλπ.

Τα πεδία βοηθούν στο να ξεχωρίζουν τα events μεταξύ τους, επειδή διαφέρουν ανά περίπτωση και στο όνομα και στην τιμή. Δίνουν τη δυνατότητα προσαρμοσμένων αναζητήσεων, αποκλειστικά για τα δεδομένα την ανάκτηση των οποίων επιθυμεί ο χρήστης εκείνη τη στιγμή. Του επιτρέπουν να επωφεληθεί στο έπακρο από τη γλώσσα αναζήτησης του Splunk και τα προσφερόμενα γραφήματα, διαγράμματα, πίνακες και αναφορές.

Τα περισσότερα πεδία μέσα στα δεδομένα έχουν μοναδικές τιμές και ονόματα, μερικά πεδία όμως συναντώνται παραπάνω από μία φορές σε ένα event έχοντας διαφορετικές τιμές αλλά ίδιο όνομα. Χαρακτηριστικό παράδειγμα αποτελούν τα πεδία ηλεκτρονικού ταχυδρομείου τα οποία έχουν ως τιμές το όνομα του αποστολέα και του παραλήπτη ή πολλαπλών παραληπτών.

I. Η πλαϊνή γραμμή πεδίων

1. Πίσω στη γραμμή αναζήτησης. Επιλέγουμε Yesterday στο χρόνο και πληκτρολογούμε αναζήτηση για να γίνει έλεγχος προσβάσεων στο server:

sourcetype="access_*"

Πατάμε Enter

2. Στα αποτελέσματα αναζήτησης διακρίνουμε:

- Την ip διεύθυνση των χρηστών που χρησιμοποιούν το ηλεκτρονικό κατάστημα
- Κωδικούς κατάστασης HTTP για κάθε αίτηση σελίδας
- URIs και urls για την αίτηση σελίδας και για την αναφερόμενη σελίδα
- Μεθόδους αίτησης σελίδας

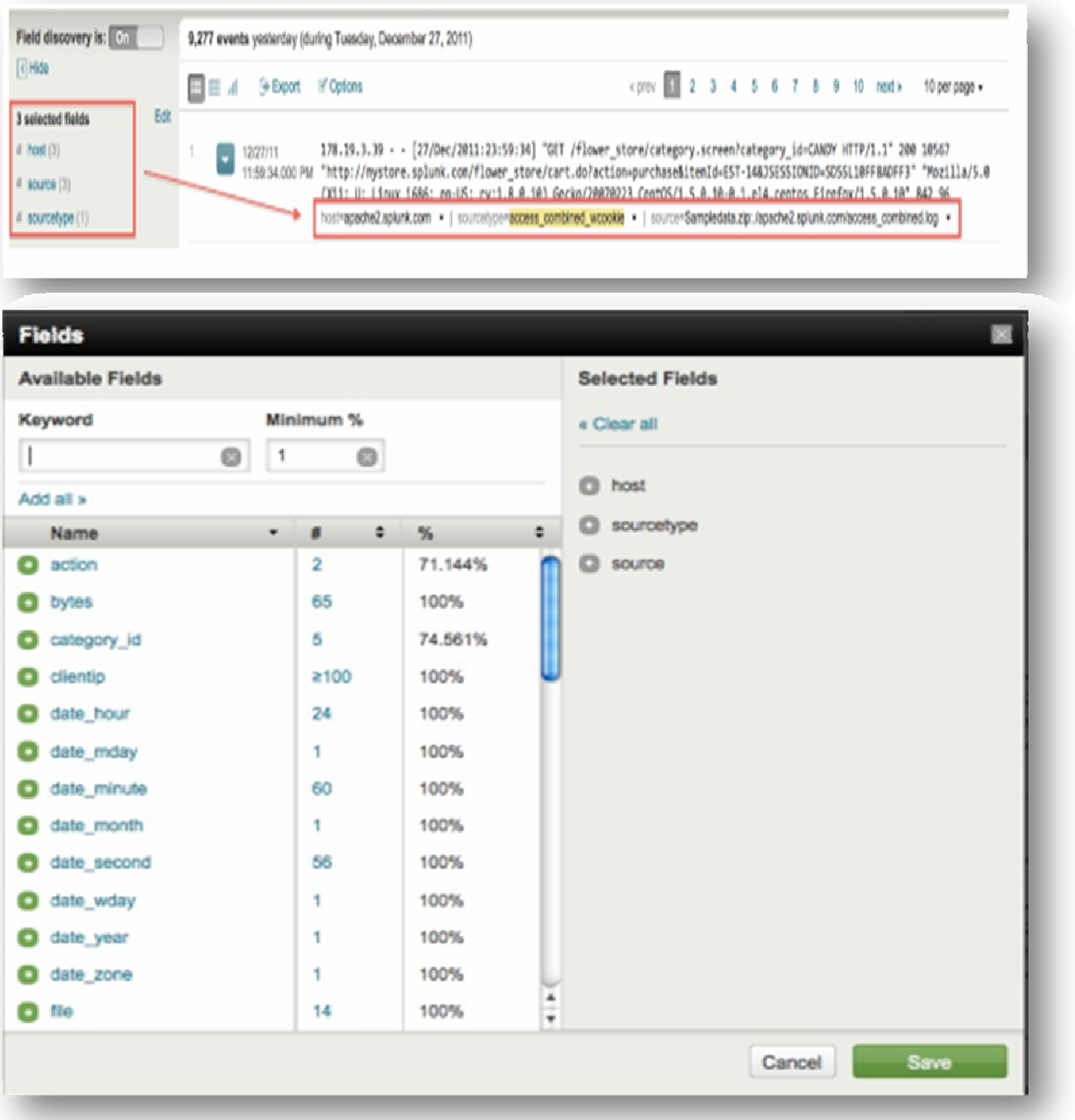
Καθώς το Splunk ανακτά τα νέα δεδομένα, εξάγει από αυτά πεδία, με τα οποία ενημερώνει την πλαϊνή μπάρα πεδίων στα αριστερά του Search Interface dashboard.

II. Αυτόματη εξαγωγή και προεπιλεγμένα πεδία

Το Splunk εξάγει πεδία δύο φορές. Πρώτα γίνεται η εξαγωγή των προεπιλεγμένων (default) πεδίων και έπειτα των άλλων τα οποία προέκυψαν από τα δεδομένα μέσα στο index. Τα default fields είναι τα εξής:

- Το πεδίο host
- Το πεδίο source

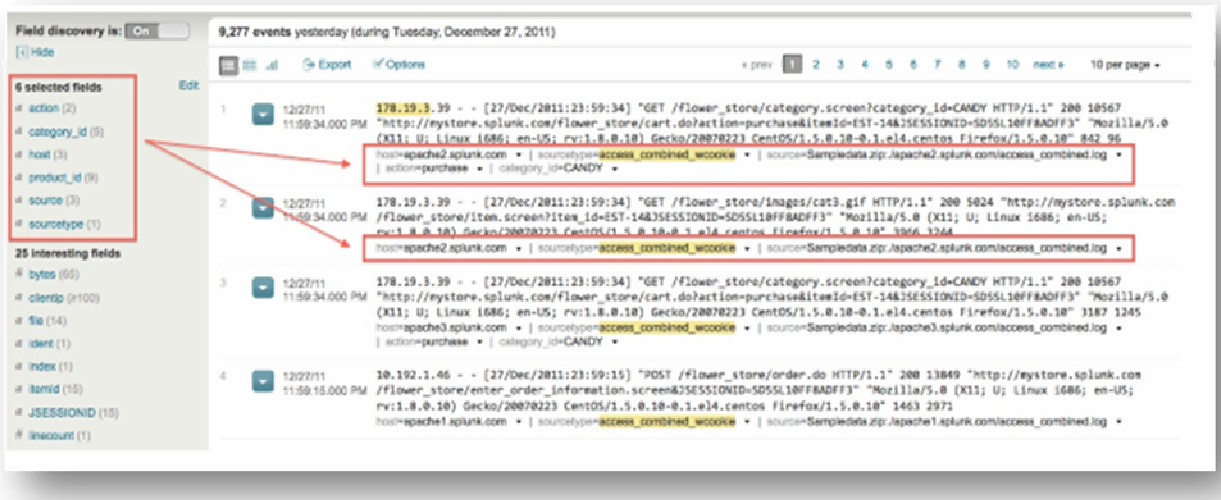
- Το πεδίο sourcetype



1. Χρησιμοποιώντας την επιλογή edit στην πλαϊνή γραμμή πεδίων ανοίγει ένα παράθυρο, στα αριστερά του οποίου εμφανίζονται όλα τα διαθέσιμα πεδία (available fields) και στα δεξιά τα επιλεγμένα πεδία (selected fields) στα δεξιά. Διαθέσιμα είναι τα πεδία τα οποία εξήγαγε το Splunk από όλα τα events και επιλεγμένα αυτά που έχουν επιλεχθεί να φαίνονται στο dashboard της αναζήτησης(τα πεδία host, source και sourcetype είναι ήδη προεπιλεγμένα) .

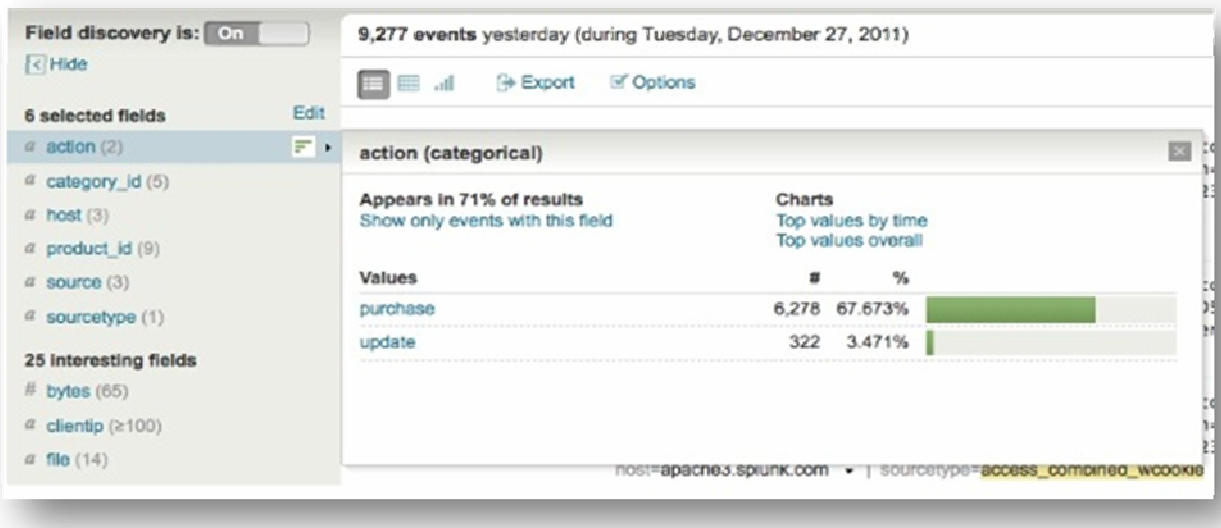
Αν περιηγηθούμε ανάμεσα στα Available fields παρατηρούμε fields τα οποία αφορούν το διαδικτυακό κατάστημα του παραδείγματος μας, όπως το action που αναφέρεται στις ενέργειες των πελατών , το category_id που δείχνει τον τύπο του προϊόντος και το product_id που είναι ο κωδικός του προϊόντος που πρόκειται να αγοράσει ο πελάτης.

2. Επιλέγοντας αυτά τα τρία πεδία τα τοποθετούμε στη λίστα Selected, πατάμε αποθήκευση (save) και όταν επιστρέψουμε στην αναζήτηση αυτά θα περιλαμβάνονται μέσα στα αποτελέσματα της αναζήτησης.



Οι αριθμοί δίπλα στο όνομα των Selected fields δηλώνουν πόσες τιμές υπάρχουν διαθέσιμες για το κάθε πεδίο ξεχωριστά.

3. Πατάμε πάνω στο πεδίο action



Ανοίγει ένα νέο παράθυρο με πληροφορίες για το πεδίο αυτό. Οι δύο τιμές που αντιστοιχούν σε αυτό το πεδίο είναι η τιμή purchase (αγορά) και η τιμή update(ανανέωση). Επίσης μας δίνεται η πληροφορία ότι το πεδίο action εμφανίζεται στο 71% του συνόλου των αποτελεσμάτων αναζήτησης. Αυτό σημαίνει ότι τα ¾ των events αφορούν την αγορά ενός προϊόντος ή την ανανέωση του (στο καλάθι αγορών).

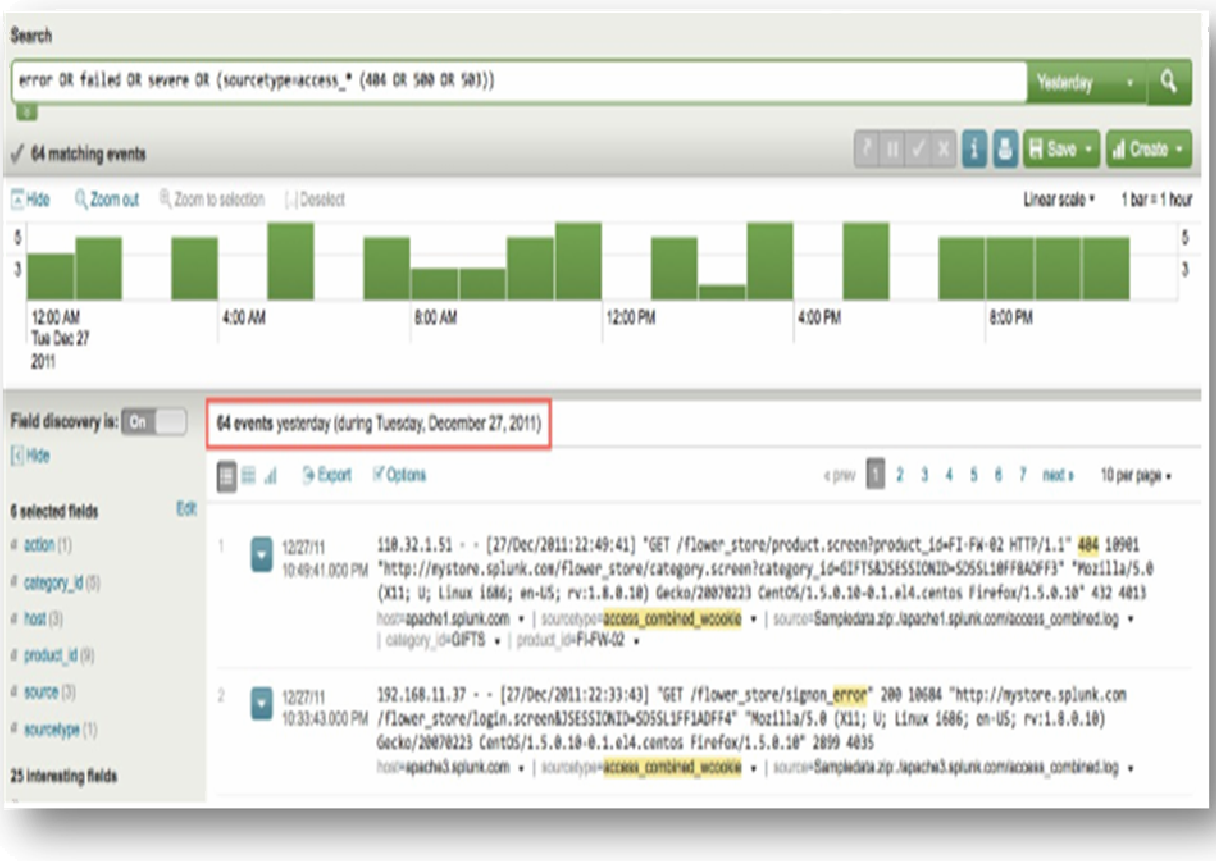
III. Χρήση πεδίων για στοχευμένες αναζητήσεις

Τα επόμενα δύο παραδείγματα απεικονίζουν τη διαφορά ανάμεσα στην αναζήτηση με λέξεις-κλειδιά και την αναζήτηση με πεδία.

Παράδειγμα *1.*

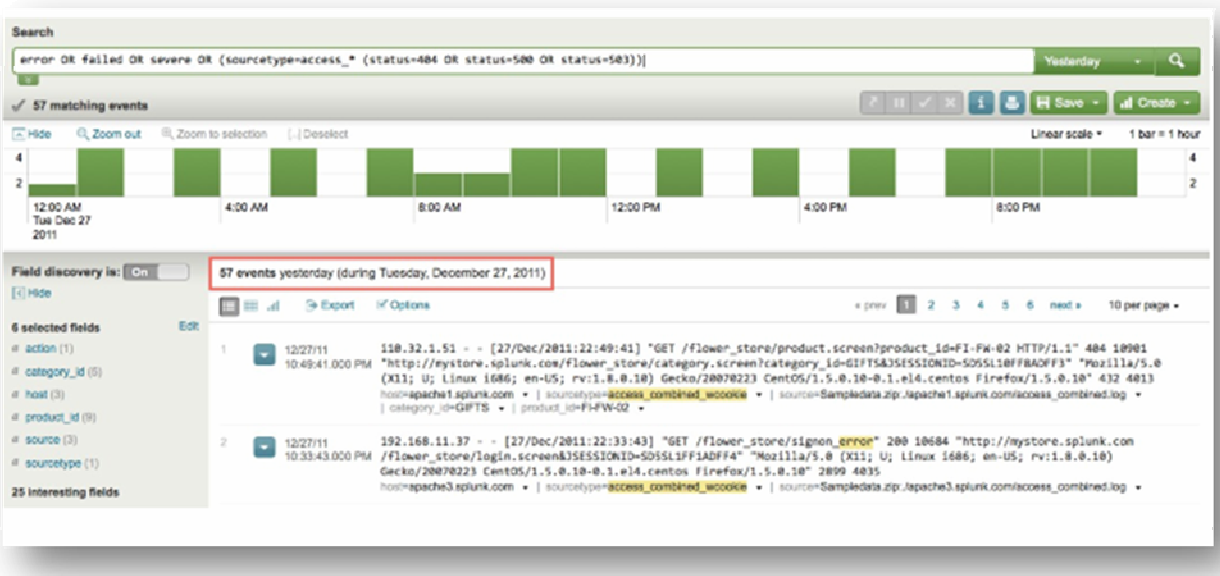
Επιστρέφουμε στην αναζήτηση που τρέξαμε για να ελέγξουμε εάν υπάρχουν σφάλματα μέσα στα δεδομένα μας:

error OR failed OR severe OR (sourcetype=access_* (404 OR 500 OR 503))



Αυτή τη φορά θα κάνουμε χρήση πεδίων στην αναζήτηση.

Τα HTTP errors ανήκουν στο πεδίο status, επομένως σύμφωνα με τον κανόνα αναζήτησης στο Splunk οπού fieldname=fieldvalue, το search string διαμορφώνεται ως εξής :



error OR failed OR severe OR (sourcetype=access_* (status=404 OR status=500 OR status=503))

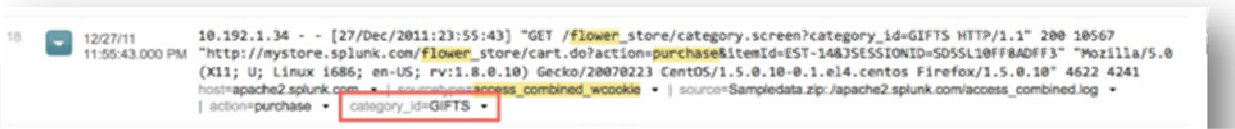
Παρατηρείται ότι στη δεύτερη αναζήτηση με τη χρήση πεδίων, ο αριθμός αποτελεσμάτων μειώθηκε στα 57 και αυτό επειδή το Splunk αναζήτησε μόνο events που περιέχουν αυτά τα συγκεκριμένα πεδία/τιμές.

Παράδειγμα 2.

Έστω ότι θέλουμε να κάνουμε την απλή αναζήτηση:

sourcetype=access_* purchase flower*

για να παρακολουθήσουμε τις αγορές λουλουδιών στο διαδικτυακό κατάστημα. Ενώ πληκτρολογούμε τη λέξη flower ο βοηθός αναζήτησης μας εμφανίζει τη λέξη flower αλλά και flowers και επειδή δεν γνωρίζουμε ποια από τις δύο λέξεις αντιπροσωπεύει

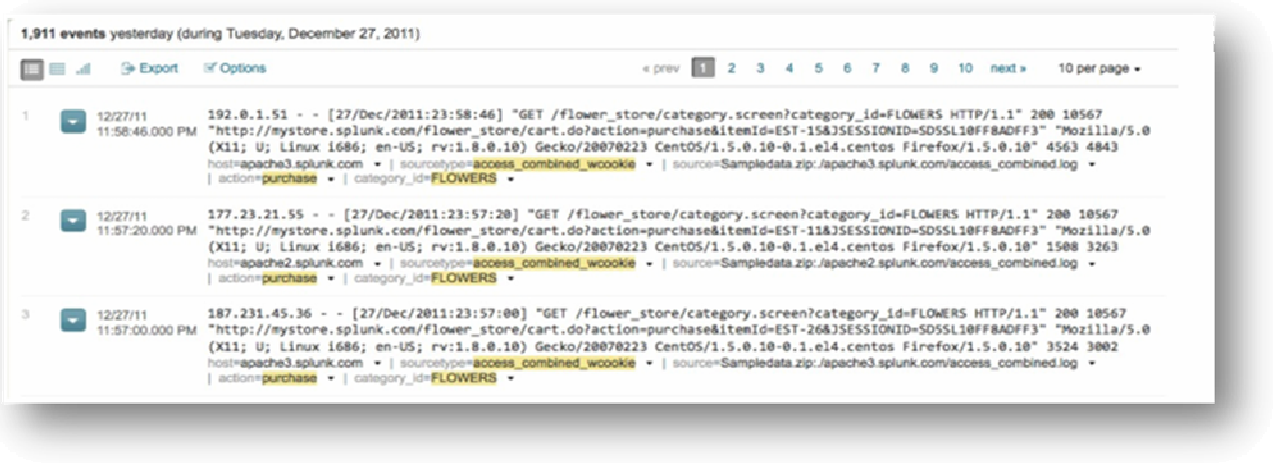


το προϊόν flower θα χρησιμοποιήσουμε τον αστερίσκο για να περιλάβουμε και τις δύο λέξεις στην αναζήτηση.

Τα αποτελέσματα που επιστρέφει το Splunk δεν είναι κατατοπιστικά σε αυτή την περίπτωση και αυτό επειδή η λέξη-κλειδί flower υπάρχει παντού μέσα στα events.

Προσαρμόζουμε λοιπόν πάλι το search string χρησιμοποιώντας το field category_id:

sourcetype=access_* action=purchase category_id=flower*



Στη δεύτερη αναζήτηση έχουμε λιγότερα αποτελέσματα και υπάρχει μόνο μια τιμή για το πεδίο category_id, η τιμή flowers.

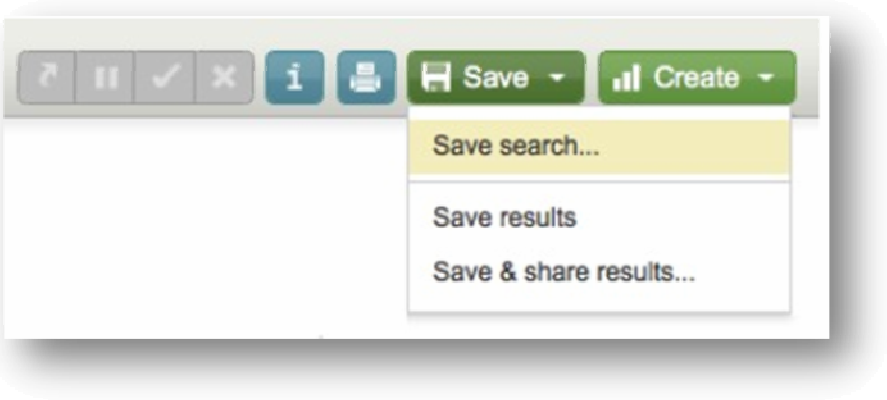
Αποθήκευση μιας Αναζήτησης

Σε αυτή την ενότητα θα εξεταστεί ο τρόπος αποθήκευσης μιας αναζήτησης και πώς μπορεί να χρησιμοποιηθεί ξανά αργότερα.

Πίσω στο διαδικτυακό κατάστημα. Η τελευταία αναζήτηση που τρέξαμε αφορούσε σφάλματα στο server την προηγούμενη ημέρα. Μια αναζήτηση που για ευνόητους λόγους θα πρέπει να τρέχουμε κάθε πρωί, επομένως για να αποφύγουμε την πληκτρολόγηση του ίδιου search string καθημερινά, δημιουργούμε ένα μια αποθηκευμένη αναζήτηση(saved search).

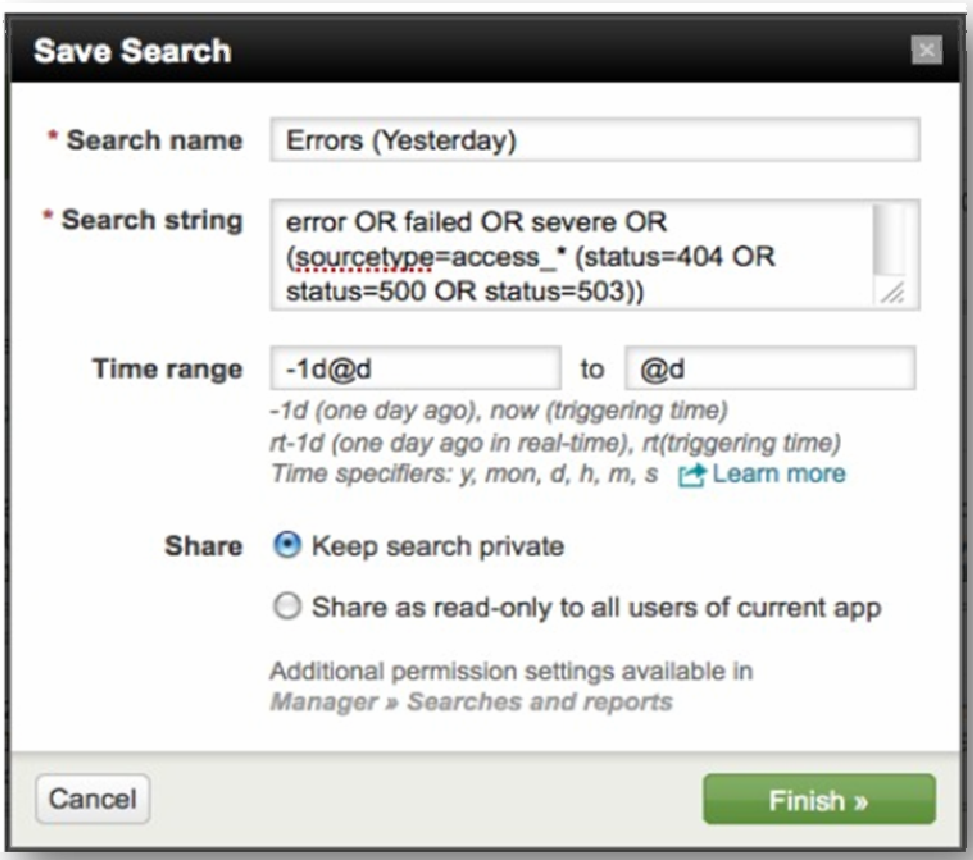
1. Τρέχουμε ξανά την αναζήτηση για την προηγούμενη ημέρα και επιλέγουμε Save κάτω από τη γραμμή αναζήτησης.

Αυτό μας επιτρέπει την αποθήκευση των αποτελεσμάτων της αναζήτησης και μας δίνει τη δυνατότητα να τα μοιραστούμε με την ομάδα μας.

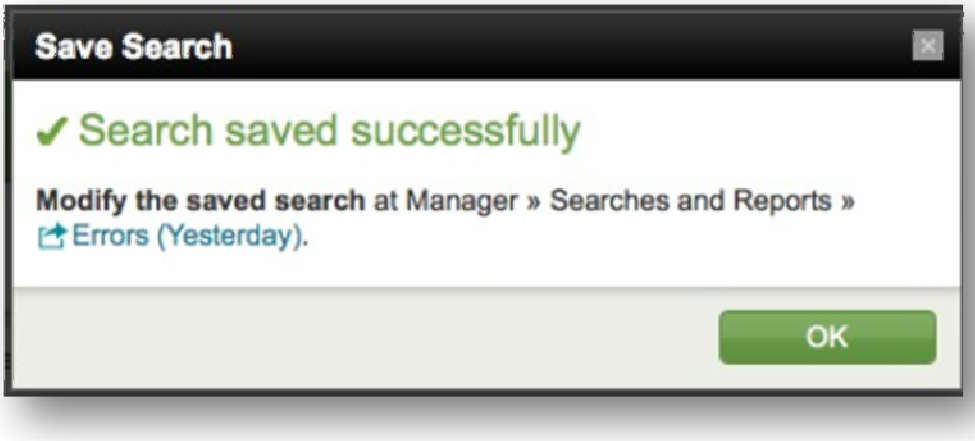


Το παράθυρο της αποθήκευσης ανοίγει.

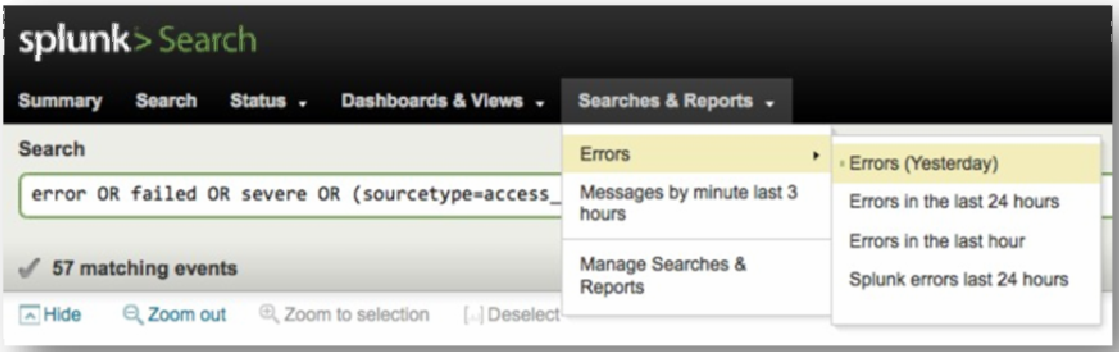
2. Ορίζουμε το όνομα της αναζήτησης Errors (Yesterday), το search string και το χρόνο τα αφήνουμε ως έχουν. Πατάμε Finish.



3. Το Spunk μας επιβεβαιώνει ότι η αναζήτηση μας αποθηκεύτηκε επιτυχώς.



4. Για να ανατρέξουμε στην αναζήτηση που μόλις αποθηκεύτηκε, πηγαίνουμε στο μενού του Splunk Searches and Reports, στο υπομενού Errors επειδή το όνομα που δόθηκε στην αναζήτηση περιέχει τη λέξη Error.



**Εάν θελήσουμε να τροποποιήσουμε μία αποθηκευμένη αναζήτηση, μεταβαίνουμε στο μενού Manage Searches & Reports και οδηγούμαστε σε μια νέα σελίδα όπου βρίσκονται όλες οι αναζητήσεις και οι εκθέσεις στις οποίες έχουμε πρόσβαση. Επιλέγουμε την αναζήτηση που επιθυμούμε και προβαίνουμε σε αλλαγή των στοιχείων της με την ίδια διαδικασία που ακολουθήθηκε κατά τη δημιουργία της.*

Χρήση εντολών Splunk

Πίσω στο ηλεκτρονικό κατάστημα, στο γραφείο εξυπηρέτησης πελατών. Στην ενότητα *Χρήση πεδίων για πιο στοχευμένες αναζητήσεις* πραγματοποιήθηκε αναζήτηση με στόχο τη λήψη αποτελεσμάτων για την αγορά λουλουδιών.

sourcetype=access_* action=purchase category_id=flowers

Τα αποτελέσματα της αναζήτησης έδιναν πληροφορίες σχετικά με την ποσότητα των λουλουδιών που αγοράστηκαν όμως δεν έδιναν απαντήσεις στα παρακάτω ερωτήματα:

- Ποια είναι τα πιο δημοφιλή προϊόντα στο ηλεκτρονικό κατάστημα;
- Πόσοι πελάτες αγόρασαν λουλούδια; Πόσα λουλούδια αγόρασε ο κάθε πελάτης;

Για να απαντηθούν αυτά τα ερωτήματα θα γίνει χρήση της Γλώσσας του Splunk, όντας πλούσια σε εντολές και λειτουργίες καθιστά εφικτό το φιλτράρισμα, την τροποποίηση και την αναπροσαρμογή των αποτελεσμάτων.

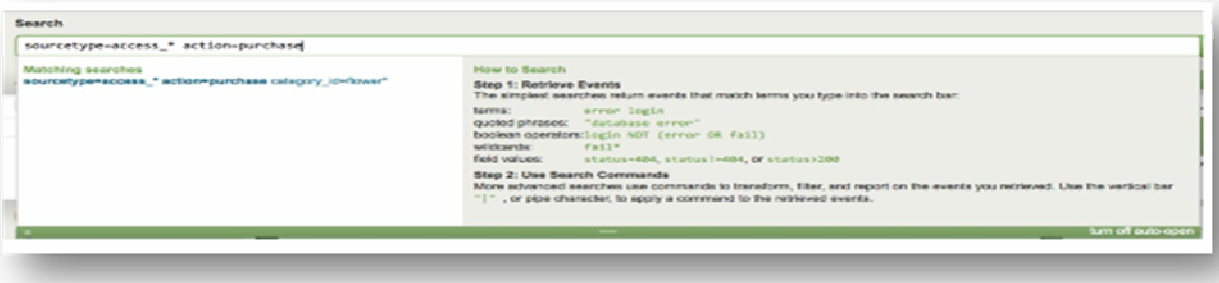
I. Ο βοηθός αναζήτησης

Παράδειγμα 1.

Ποια προϊόντα αγοράστηκαν περισσότερο στο διαδικτυακό κατάστημα;

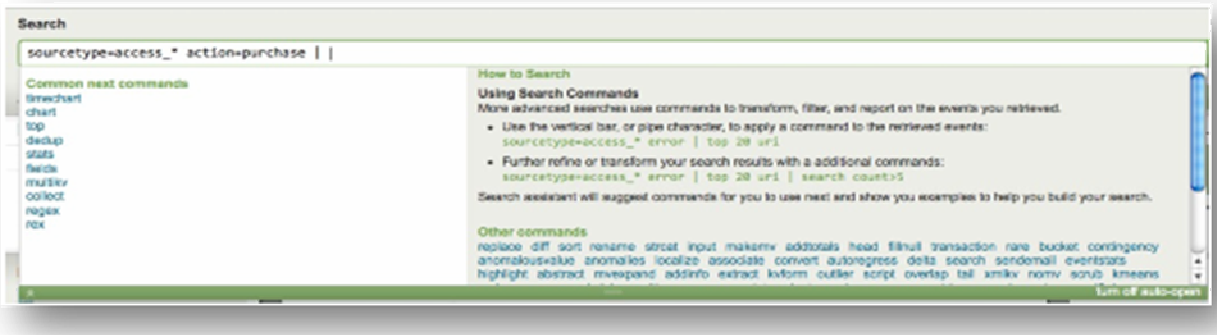
1. Επιστρέφοντας στον πίνακα αναζήτησης επιλέγουμε Yesterday στο χρόνο και πληκτρολογούμε την αναζήτηση :

sourcetype=access_* action=purchase



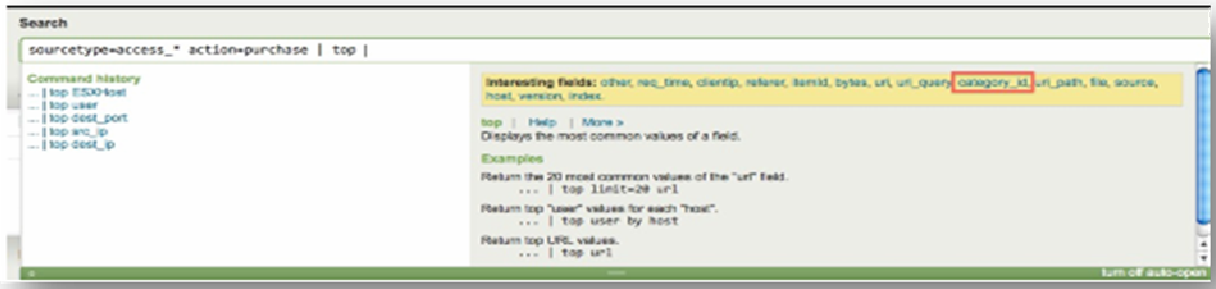
Καθώς γράφουμε στη γραμμή αναζήτησης, ο βοηθός αναζήτησης ανοίγει και εμφανίζονται πληροφορίες σχετικά με τη σύνταξη και τη χρήση των εντολών (στη δεξιά πλευρά)

2. Προσθέτουμε το χαρακτήρα «|» στη γραμμή αναζήτησης.



Ο βοηθός αναζήτησης ανοίγει για μία ακόμα φορά με προτάσεις εντολών που μπορούν να χρησιμοποιηθούν μετά την κάθετο («|»). Το ζητούμενο είναι τα πιο δημοφιλή προϊόντα του καταστήματος ανάμεσα στους πελάτες.

3. Επιλέγουμε την εντολή top.

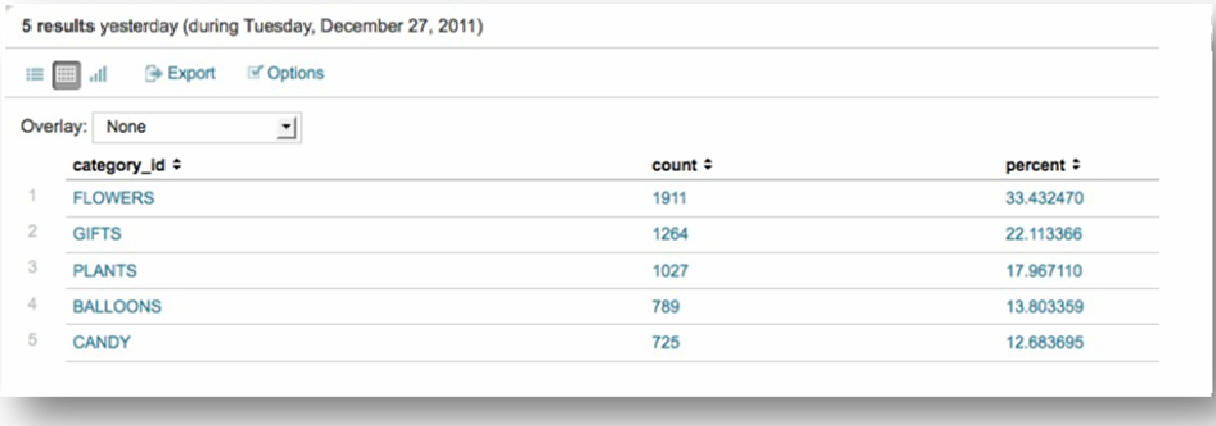


Σύμφωνα με το βοηθό η συγκεκριμένη εντολή χρησιμοποιείται για να αναδείξει τα πιο δημοφιλή πεδία εμφανίζοντας μερικά από αυτά στη δεξιά πλευρά.

4. Επιλέγουμε το πεδίο category_id και η αναζήτηση διαμορφώνεται :

sourcetype=access_* action=purchase | top category_id

Εμφανίζεται ένας πίνακας με τις πιο κοινές τιμές του πεδίου category_id. Η εντολή top φέρνει προεπιλεγμένα δέκα(10) αποτελέσματα, όμως το κατάστημα διαθέτει μόνο πέντε(5) κατηγορίες προϊόντων, επομένως εμφανίζονται μόνο πέντε(5) αποτελέσματα.



	category_id	count	percent
1	FLOWERS	1911	33.432470
2	GIFTS	1264	22.113366
3	PLANTS	1027	17.967110
4	BALLOONS	789	13.803359
5	CANDY	725	12.683695

Εξετάζοντας των πίνακα αποτελεσμάτων παρατηρούνται δυο νέα πεδία. Το πεδίο count το οποίο δηλώνει πόσες φορές έχουν προκύψει οι συγκεκριμένες τιμές και το πεδίο percent που δηλώνει το ποσοστό του count επί του συνόλου των αποτελεσμάτων.

Παράδειγμα 2.

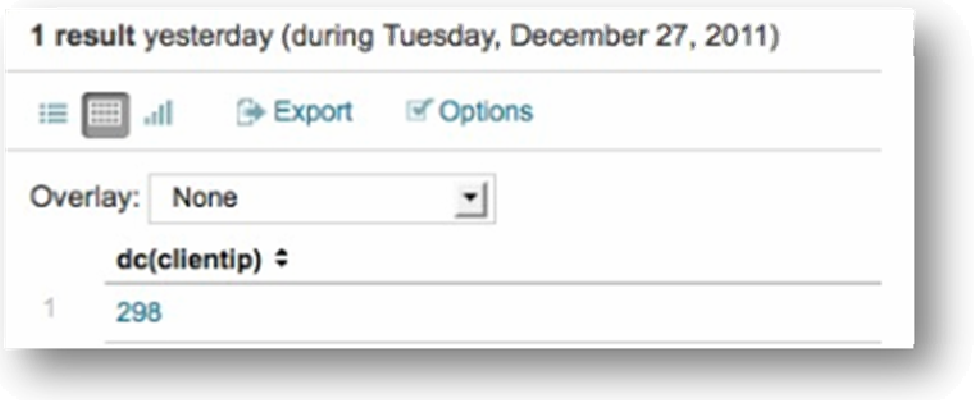
Πόσοι πελάτες αγόρασαν λουλούδια; Πόσα λουλούδια αγόρασε ο κάθε πελάτης;

Το ζητούμενο είναι να βρεθεί ο αριθμός των πελατών οι οποίοι αγόρασαν λουλούδια. Οι πελάτες διακρίνονται από τις IP διευθύνσεις τους οι οποίες αποτελούν τιμές του πεδίου clientip.

1. Χρησιμοποιούμε την εντολή stats και distinct_count() ή αλλιώς dc() :

sourcetype=access_* action=purchase category_id=flowers | stats dc(clientip)

Με αυτή την αναζήτηση ορίζουμε να μας επιστραφούν οι μοναδικές τιμές του πεδίου clientip που υπάρχουν στα events, μετρώντας τον κάθε πελάτη μόνο μια φορά και όχι κάθε φορά που πραγματοποιεί μια αγορά.



Η αναζήτηση φέρνει μια μοναδική τιμή η οποία μας λέει ότι 298 διαφορετικοί πελάτες αγόρασαν λουλούδια από το ηλεκτρονικό κατάστημα.

Το επόμενο βήμα είναι να βρεθεί ο αριθμός των λουλουδιών που αγόρασε ο κάθε πελάτης ξεχωριστά.

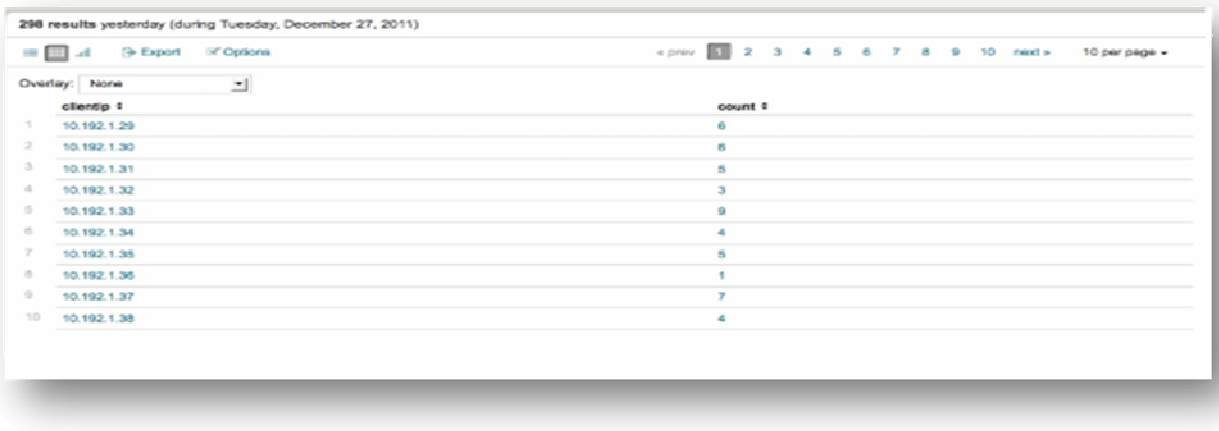
2. Χρησιμοποιούμε την εντολή stats:

sourcetype=access_* action=purchase category_id=flowers | stats count

Το count επιστρέφει μια μοναδική τιμή, δηλαδή τον αριθμό των events που ταιριάζουν στην αναζήτηση μας. Μια τέτοια αναζήτηση λοιπόν, θα φέρει τον αριθμό των λουλουδιών που αγοράστηκαν.

3. Για να βρούμε συγκεκριμένα πόσα αγοράσθηκαν από τον κάθε πελάτη προσθέτουμε τη λέξη by μετά την εντολή stats:

sourcetype=access_* action=purchase category_id=flowers | stats count BY clientip



Ο πίνακας που εμφανίζεται δείχνει στα αριστερά τον πελάτη και στα δεξιά το πεδίο count, που είναι ο αριθμός των λουλουδιών που αγόρασε.

II. Τροποποίηση αποτελεσμάτων

Τα αποτελέσματα που φαίνονται στον πίνακα, είναι άκρως κατανοητά σε κάποιον ο οποίος έχει ασχοληθεί άμεσα με τη διαδικασία της αναζήτησης. Το ερώτημα είναι τι γίνεται με κάποιον που δεν γνωρίζει τι αντιπροσωπεύουν τα πεδία; Παρακάτω θα δούμε πώς μπορεί να γίνει τροποποίηση της όψης των αποτελεσμάτων, έτσι ώστε να είναι κατανοητά από οποιονδήποτε.

1. Μετονομάζουμε το πεδίο count:

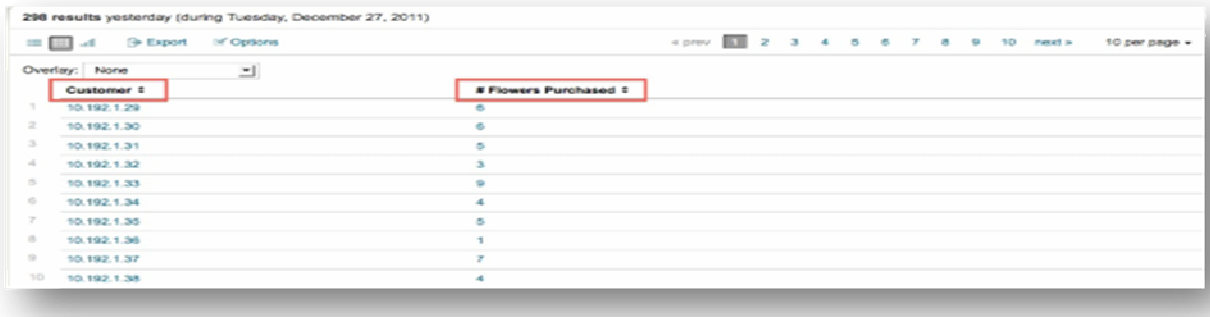
sourcetype=access_* action=purchase category_id=flowers | stats count AS "# Flowers purchased" by clientip

Οι κανόνες σύνταξης της εντολής stats επιτρέπουν τη μετονομασία ενός πεδίου χρησιμοποιώντας τη λέξη «AS». Αν το νέο όνομα του πεδίου είναι φράση χρησιμοποιούμε διπλά εισαγωγικά, αν είναι μια απλή λέξη δεν χρειάζεται καμία προσθήκη εισαγωγικών.

2. Χρησιμοποιούμε την εντολή rename για να αλλάξουμε το όνομα του πεδίου clientip :

sourcetype=access_* action=purchase category_id=flowers | stats count AS "# Flowers Purchased" by clientip | rename clientip AS Customer

Αυτό το search string όπως έχει διαμορφωθεί, έχει ως αποτέλεσμα τη μετονομασία του πεδίου clientip του πίνακα, σε Customer (Πελάτης) και του πεδίου count σε #Flowers Purchased (αριθμός λουλουδιών που αγοράστηκαν) :



Παράδειγμα.

Έστω ότι μας έχει ζητηθεί από τη διεύθυνση να ετοιμάσουμε μια αναφορά, σχετικά με το ποιος είναι ο πελάτης, που έχει πραγματοποιήσει τις περισσότερες αγορές την προηγούμενη ημέρα.

Το πρώτο βήμα είναι η ανακάλυψη του πελάτη, ο οποίος επισκέφτηκε περισσότερες φορές τη σελίδα του διαδικτυακού καταστήματος.

1. Χρησιμοποιούμε την εντολή *top* για τη λήψη των κορυφαίων αποτελεσμάτων, προσθέτουμε την εντολή limit=1 έτσι ώστε η αναζήτηση να μας φέρει ως αποτέλεσμα μόνο έναν πελάτη από το πεδίο clientip και ορίζουμε το Yesterday ως χρόνο στην αναζήτηση:

sourcetype=access_* action=purchase | top limit=1 clientip

Ο πελάτης λοιπόν, που επισκέφτηκε τις περισσότερες φορές το κατάστημα είναι ο πελάτης με Ip : *10.192.1.39* .

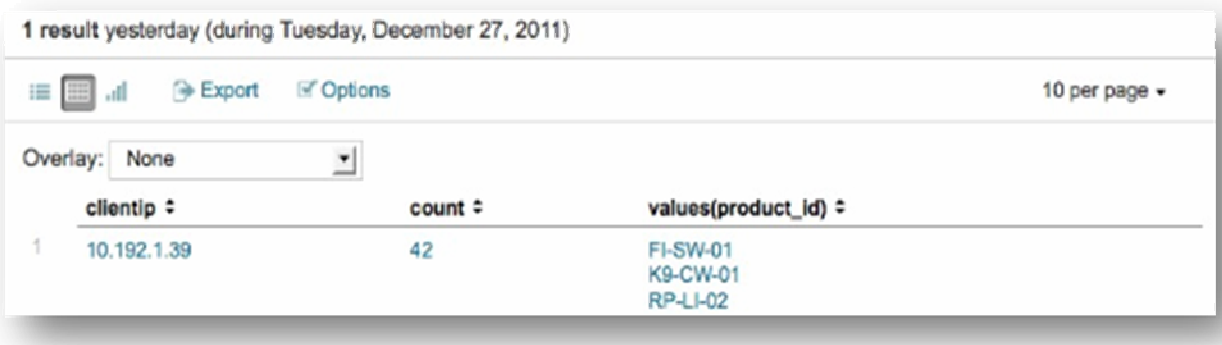
2. Χρησιμοποιούμε την εντολή stats για να δούμε τον ακριβή αριθμό των αγορών του πελάτη:

sourcetype=access_* action=purchase clientip=10.192.1.39 | stats count by clientip

3. Για να δούμε τα προϊόντα που αγόρασε ο πελάτης χρησιμοποιούμε ξανά την εντολή stats ακολουθούμενη από την εντολή value() :

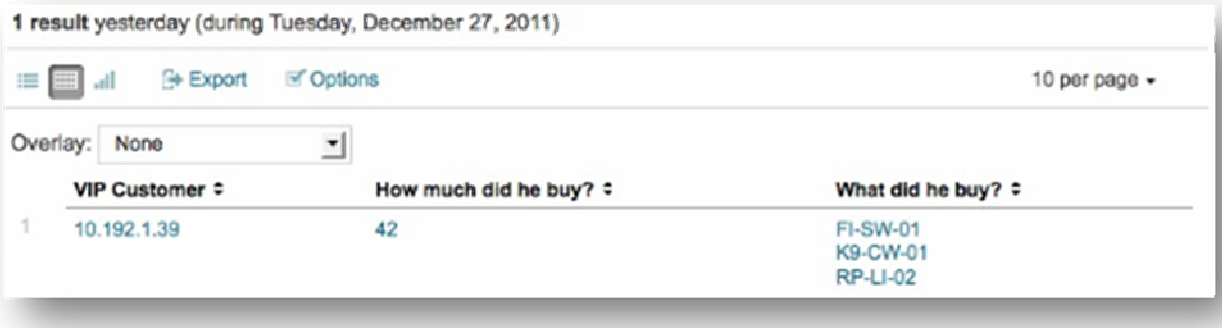
sourcetype=access_* action=purchase clientip=10.192.1.39 | stats count, values(product_id) by clientip

Αυτόματα προστίθεται στον πίνακα μια στήλη με όνομα values(product_id) η οποία περιέχει μια λίστα με τους κωδικούς των προϊόντων που αγόρασε ο συγκεκριμένος πελάτης.



4. Για τον ίδιο λόγο που έγινε μετονομασία των πεδίων στο παράδειγμα της προηγούμενης ενότητας, αναδιαμορφώνουμε το search string ως εξής:

sourcetype=access_* action=purchase clientip=10.192.1.39 | stats count, values(product_id) as product_id by clientip | rename count AS "How much did he buy?", product_id AS "What did he buy?",clientip AS "VIP Customer"



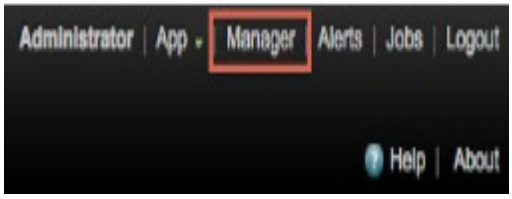
Πεδία Lookup

Τα πεδία Lookup(Lookup fields) είναι πεδία, τα οποία επιτρέπουν την αναφορά σε πεδία προερχόμενα από ένα εξωτερικό CSV αρχείο, το οποίο συσχετίζει τα πεδία με τα events των δεδομένων. Η χρήση αυτών των συσχετίσεων εμπλουτίζει τα events, προσθέτοντας ουσιαστικές πληροφορίες και αναζητήσιμα πεδία σε αυτά.

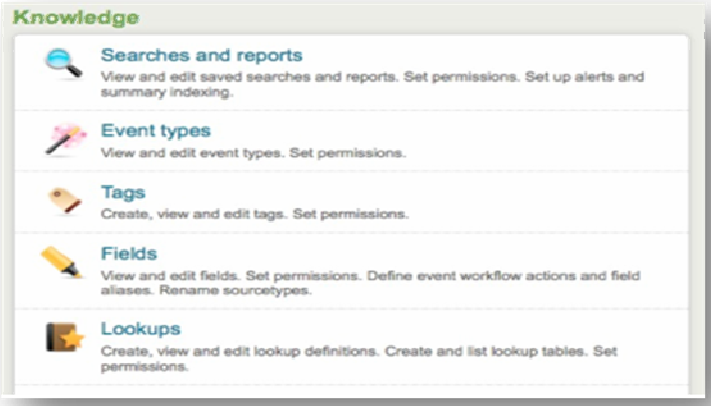
Στο παράδειγμα 3 της προηγούμενης ενότητας παρουσιάστηκε πίνακας με τη λίστα προϊόντων που παρήγγειλε ο πελάτης με το μεγαλύτερο αριθμό αγορών της προηγούμενης ημέρας. Τα προϊόντα παρουσιάζονταν με την κωδική τους ονομασία. Ο κωδικός προϊόντος (product ID) δεν προσδιορίζει την ακριβή ονομασία του προϊόντος. Αυτό επιτυγχάνεται με τη χρήση των Lookups.

Ακολουθεί η διαδικασία εισαγωγής του CSV file με ονομασία *product_lookups.csv* και ενδεικτικό παράδειγμα χρήσης των Lookups ύστερα από την εισαγωγή των νέων πεδίων στα δεδομένα του συστήματος.

1. Στο μενού περιήγησης του Splunk επιλέγουμε Manager.

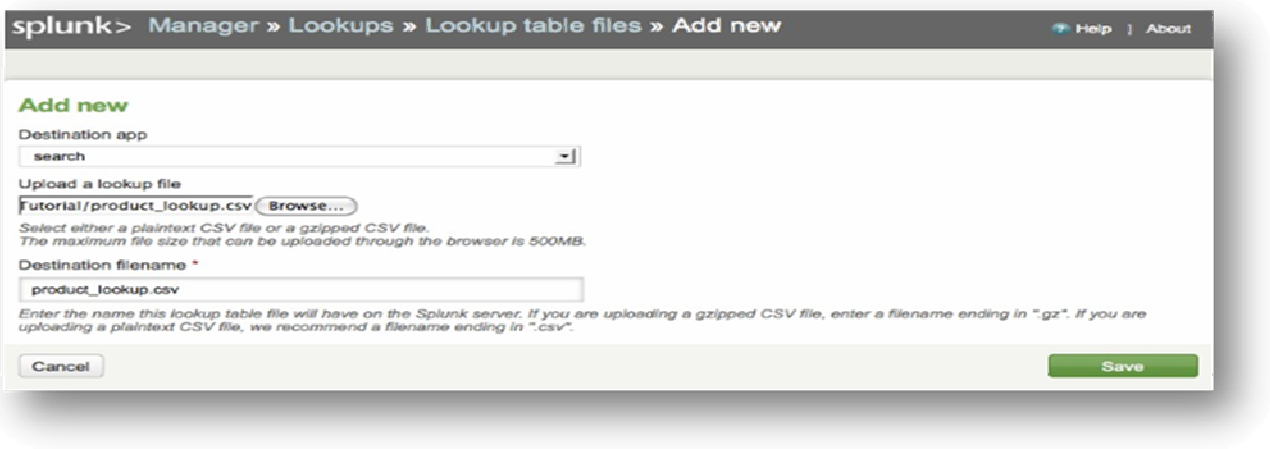


2. Οδηγούμαστε στη σελίδα ρυθμίσεων του Splunk. Στην κατηγορία Knowledge πατάμε Lookups.



Αυτόματα οδηγούμαστε το μενού Manager --> Lookups

3. Κάτω από τη στήλη Actions στα δεξιά του Lookup table files επιλέγουμε Add new.



Στο νέο παράθυρο διαλόγου που ανοίγει ξεκινάμε τη διαδικασία ανεβάσματος του csv αρχείου.

4. Αφήνουμε το Destination app με την προεπιλογή search. Αυτή η επιλογή επιτρέπει στο Splunk να προχωρήσει στην αποθήκευση του αρχείου στο Search app.

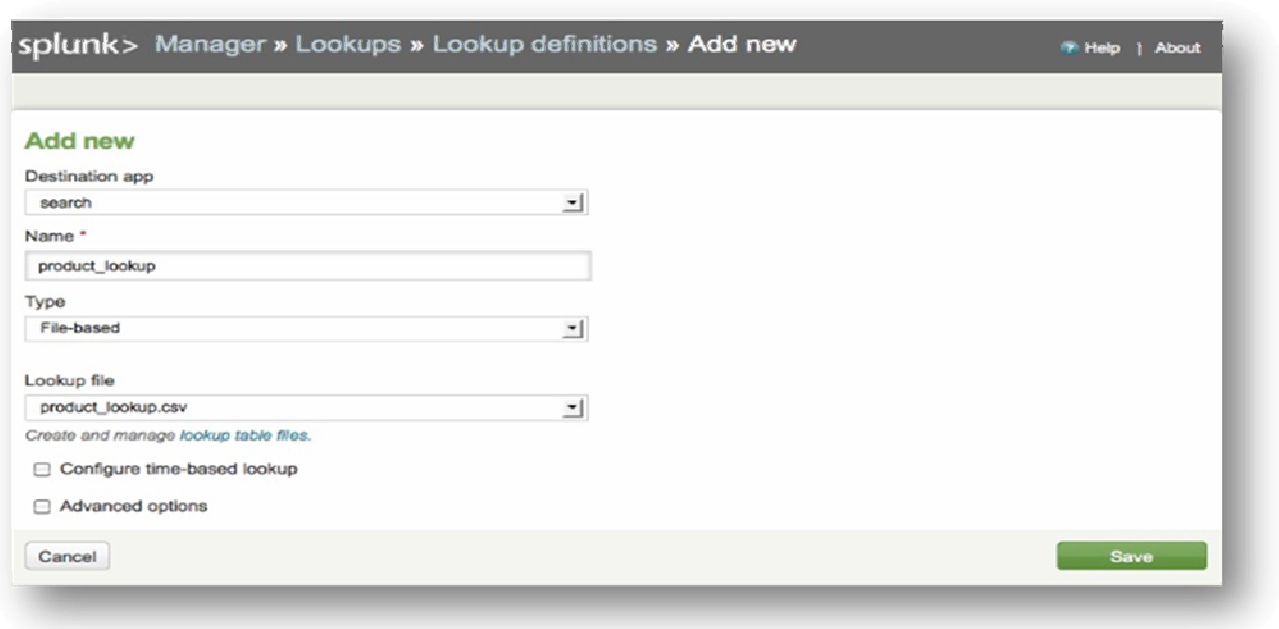
5. Στην επιλογή Upload a lookup file πατάμε Browse και επιλέγουμε την τοποθεσία του csv αρχείου.

6. Στο Destination filename πληκτρολογούμε το όνομα του αρχείου: **product_lookup.csv .**

7. Επιλέγουμε Save για να αποθηκευτεί η διαδικασία και επιστρέφουμε στο αρχικό μενού των Lookups.

Ορισμός Lookup

1. Πηγαίνουμε στο μενού Manager→ Lookups. Κάτω από τη στήλη Actions δίπλα στο Lookup definitions, πατάμε *Add New*.



2. Αφήνουμε την προεπιλογή search στο Destination app.

3. Ονομάζουμε το lookup product_lookup.

4. Στο πεδίο Type, επιλέγουμε File-based.

5. Στο Lookup file, επιλέγουμε product_lookup (το όνομα του lookup table).

6. Στις επιλογές Configure time-based lookup και Advanced options δεν κάνουμε τίποτα.

7. Πατάμε Save.

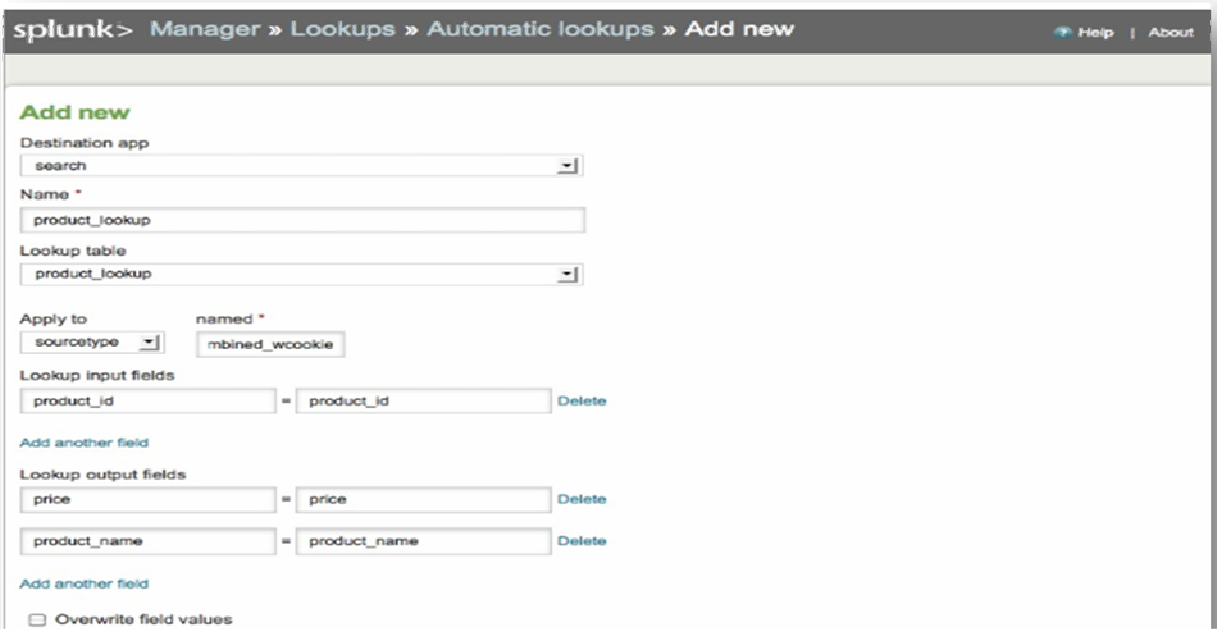
Τώρα το Splunk γνωρίζει ότι το product_lookup είναι ένα Lookup το οποίο βασίζεται σε ένα αρχείο CSV.

Κάνοντας αυτόματο το Lookup

Στο μενού Manager → Lookups:

1. Κάτω από τη στήλη *Actions* δίπλα στο Automatic lookups αυτή τη φορά επιλέγουμε *Add New*.

Αυτό μας οδηγεί στο μενού Manager → Lookups → Automatic lookups → Add New όπου θα ρυθμίσουμε το Lookup να τρέχει αυτόματα



2. Αφήνουμε την προεπιλογή *search στο* Destination app

3.Ονομάζουμε το αυτόματο lookup product_lookup.

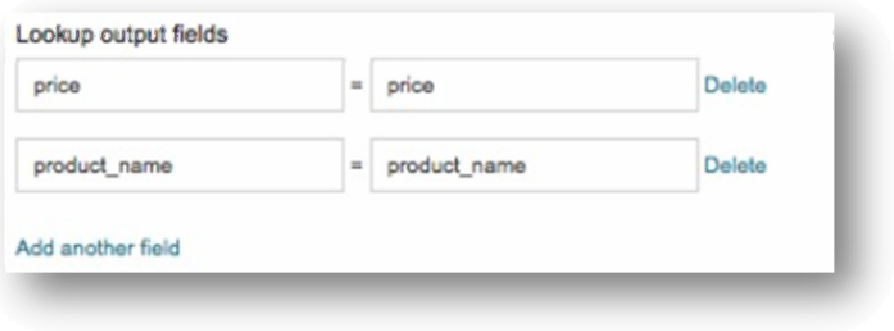
4. Στο πεδίο Lookup table, επιλέγουμε *product_lookup*.

5. Στα πεδία Apply to και named, επιλέγουμε *sourcetype* και type in *access_combined_wcookie*

6. Στα πεδία Lookup input fields πληκτρολογούμε:

Το πεδίο input είναι το πεδίο μέσα στα events μας που θα χρησιμοποιήσουμε για το συσχετισμό των πεδίων στο Lookup.

7.Στα πεδία Lookup output fields (πεδία εξόδου), γράφουμε το ακόλουθο. Χρησιμοποιούμε την επιλογή Add another field για να προσθέσουμε και άλλες τιμές.



Τα output fields είναι τα πεδία μέσα στον πίνακα του lookup τα οποία θέλουμε να προσθέσουμε στο index ώστε να γίνει ο συσχετισμός τους με τα πεδία των events. Σε αυτό το παράδειγμα προσθέτουμε τα πεδία: price, το οποίο περιέχει την τιμή για το

κάθε προϊόν (πεδίο product_id) και product_name, το οποίο περιέχει την ακριβή ονομασία για κάθε product_id πεδίο.

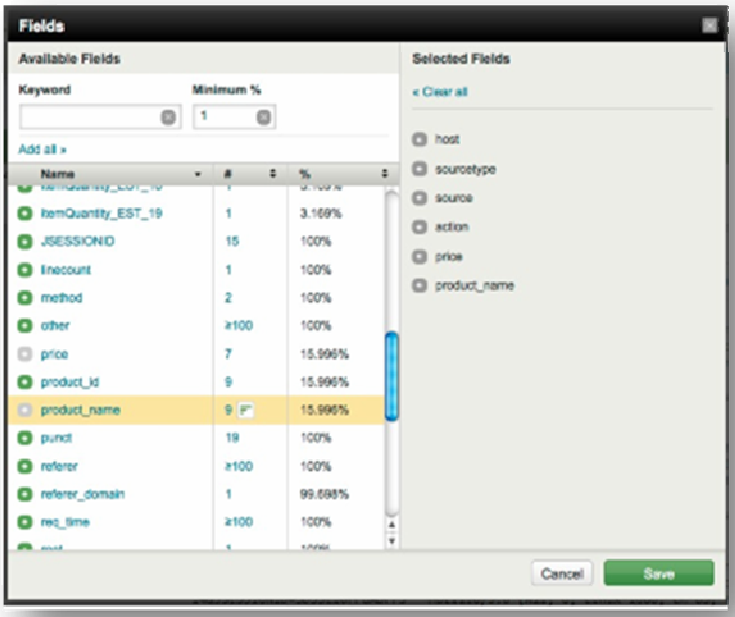
8. Αφήνουμε το checkbox Overwrite field values ως έχει.

Εάν το επιλέξουμε, το Splunk θα αντικαταστήσει όλα τα πεδία των δεδομένων των events με τις τιμές από το Lookup table.

9. Επιλέγουμε *Save*.

10. Επιστέφουμε στο dashboard αναζήτησης (<< Back to Search) και τρέχουμε την αναζήτηση για τη δραστηριότητα πρόσβασης στην ιστοσελίδα. Επιλέγουμε στο Time range , Other→ Yesterday sourcetype=access_*

Ρίχνοντας μια ματιά στη λίστα των πεδίων βλέπουμε ότι έχουν προστεθεί τα νέα πεδία Lookup product_id και product_name.



Τώρα μπορούμε να ξανατρέξουμε την προηγούμενη αναζήτηση σχετικά με τα προϊόντα που αγόρασε ο πελάτης που πραγματοποίησε τις περισσότερες αγορές την προηγούμενη ημέρα:

sourcetype=access_* action=purchase clientip=10.192.1.39 | stats count, values(product_id) as product_id by clientip | rename count AS "How much did he buy?", product_id AS "What did he buy?",clientip AS "VIP Customer"

Αυτή τη φορά αντικαθιστούμε το πεδίο product_id με το product_name:

sourcetype=access_* action=purchase clientip=10.192.1.39 | stats count, values(product_name) AS product_name by clientip | sort - count | rename count AS "How much did he buy?", product_name AS "What did he buy?", clientip AS "VIP Customer"

Το αποτέλεσμα που προκύπτει είναι ακριβώς το ίδιο με αυτό της αρχικής αναζήτησης, εμπλουτισμένο όμως αυτή τη φορά με τις ακριβείς ονομασίες των προϊόντων που αγόρασε ο πελάτης.

Παραδείγματα Αναζήτησης

Στην προηγούμενη ενότητα εισήχθησαν δύο νέα πεδία στα events του ηλεκτρονικού καταστήματος, χρησιμοποιώντας έναν πίνακα Lookup. Σε αυτή την

ενότητα θα γίνει ανακεφαλαίωση των γνώσεων, που αποκτήθηκαν μέσω μιας ακόμα σειράς παραδειγμάτων αναζητήσεων.

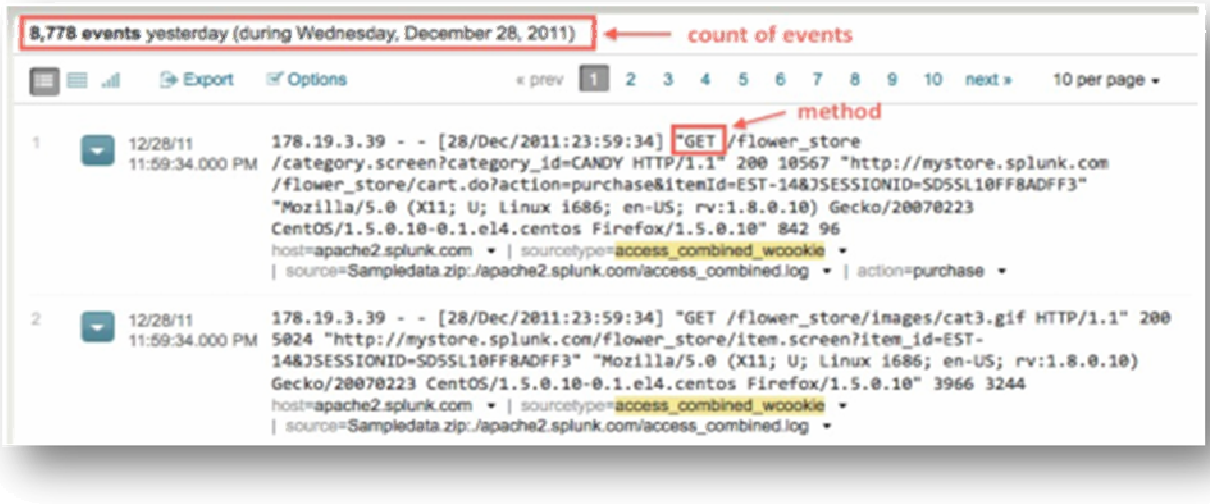
Πίσω στο ηλεκτρονικό κατάστημα λουλουδιών και ειδών δώρου, τρέχουμε αναζητήσεις για να συλλέξουμε πληροφορίες με σκοπό τη δημιουργία μιας αναφοράς σχετικά με τις αγορές που πραγματοποιήθηκαν χθες.

Παράδειγμα 1.

Πόσες φορές επισκέφτηκε κάποιος τη σελίδα του καταστήματος χθες;

1. Ξεκινάμε μια αναζήτηση για όλες τις επισκέψεις στη σελίδα. Επιλέγουμε στο Time range , Other→ Yesterday:

sourcetype=access_* method=GET



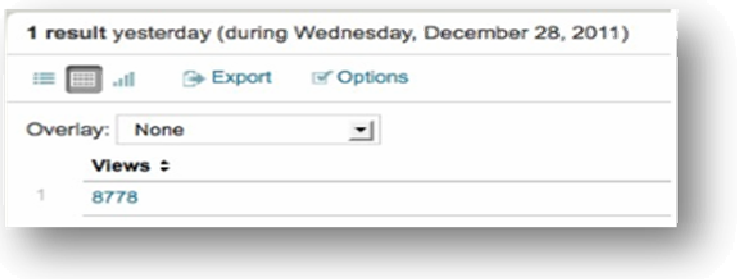
Το επόμενο βήμα είναι να μετρήσουμε τον αριθμό επισκέψεων στη σελίδα (ο αριθμός επισκέψεων στη σελίδα χαρακτηρίζεται από το πεδίο method).

2. Χρησιμοποιούμε την εντολή stats:

sourcetype=access_* method=GET | stats count AS Views

Εδώ, χρησιμοποιείται η εντολή stats count ώστε να μετρηθεί ο αριθμός των "GET" events ανάμεσα στα web access logs. Αυτός είναι ο συνολικός αριθμός που προκύπτει από την αναζήτηση και αντιστοιχεί με τον αριθμό των ανακτηθέντων

events. Αυτή η αναζήτηση ουσιαστικά συλλέγει και αποθηκεύει αυτό τον αριθμό events σε ένα πεδίο το οποίο μπορεί να χρησιμοποιηθεί.



Από τα αποτελέσματα του πίνακα βλέπουμε λοιπόν, ότι ο συνολικός αριθμός επισκέψεων στη σελίδα του ηλεκτρονικού καταστήματος την προηγούμενη ημέρα, είναι 8778. Η μετονομασία του πεδίου count σε views είναι απαραίτητη, για να αποφευχθεί σύγχυση αποτελεσμάτων παρακάτω.

3. Αποθηκεύουμε αυτή την αναζήτηση με το όνομα Pageviews(Yesterday).

Παράδειγμα 2.

Ποια είναι η διαφορά μεταξύ των επισκέψεων στην ιστοσελίδα και των αγορών που πραγματοποιήθηκαν;

Από το παράδειγμα 1 φάνηκε ότι ο αριθμός των επισκεπτών την προηγούμενη ημέρα ήταν 8778. Πόσοι από αυτούς τους επισκέπτες όμως αγόρασαν ένα προϊόν; Ποια είναι η ποσοστιαία διαφορά μεταξύ των επισκέψεων και αγορών στη σελίδα;

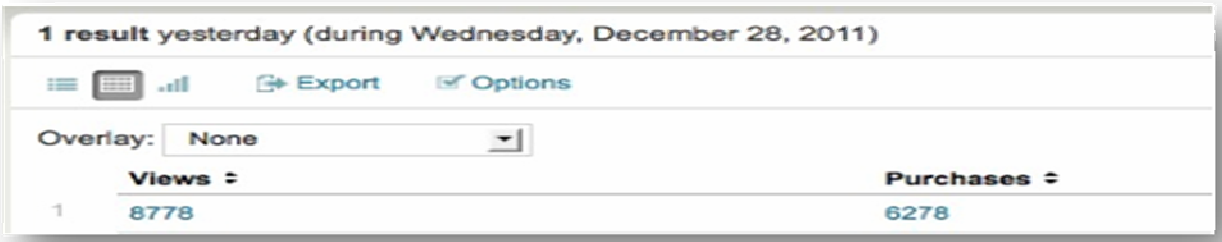
1. Ξεκινάμε την αναζήτηση του παραδείγματος 1 για χρόνο Yesterday:

sourcetype=access_* method=GET | stats count AS views

2. Χρησιμοποιούμε την εντολή stats για να μετρήσουμε τον αριθμό αγορών (οι αγορές χαρακτηρίζονται από το πεδίο action).

sourcetype=access_* method=GET | stats count AS Views,count(eval(action="purchase")) AS Purchases

Η εντολή count χρησιμοποιείται ξανά αυτή τη φορά, μαζί με την εντολή eval(), ώστε να μετρηθεί ο αριθμός των αγορών και να μετονομάσει το πεδίο action σε Purchases (αγορές).

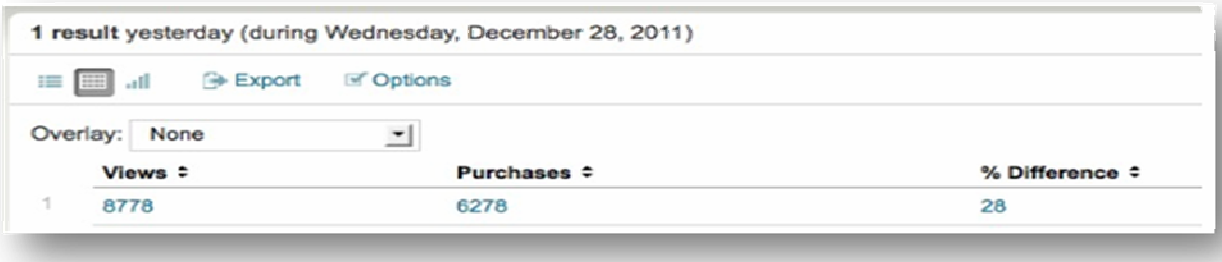


στην εντολή rename:

sourcetype=access_* method=GET | stats count AS Views, count(eval(action="purchase")) as

Purchases | eval percentage=round(100-(Purchases/Views*100)) | rename percentage AS "%Difference"

Η εντολή eval επιτρέπει την αξιολόγηση μιας έκφρασης και την αποθήκευση του αποτελέσματός της σε ένα πεδίο. Σ' αυτή την περίπτωση χρησιμοποιείται η εντολή round, για να στρογγυλοποιηθεί το υπολογιζόμενο ποσοστό των αγορών σε σχέση με τις επισκέψεις στη σελίδα.



4. Αποθηκεύουμε την αναζήτηση ως "%Difference Purchases/Views" (διαφορά αγορών/επισκέψεων).

<u>Παράδειγμα 3.</u>

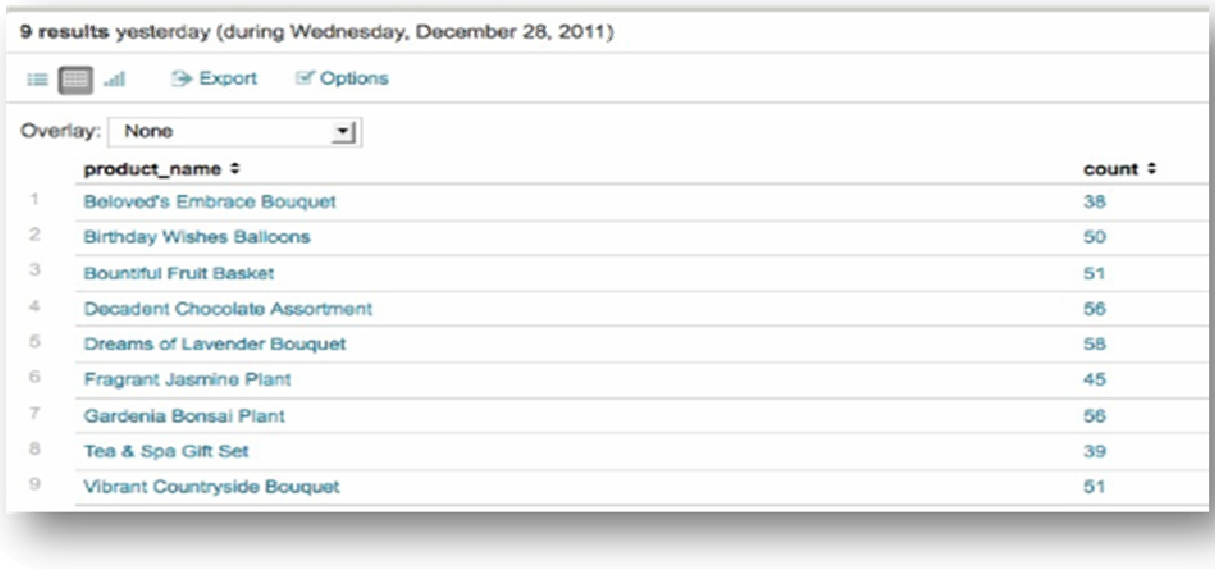
Τι προϊόντα αγοράστηκαν και πόσο κέρδος προέκυψε;

Αυτό το παράδειγμα απαιτεί τη χρήση των δύο νέων πεδίων, product_name και product_price, τα οποία προστέθηκαν στο παράδειγμα με τα Lookup.

1. Ξεκινάμε με μια αναζήτηση που αφορά όλες τις αγορές κατά όνομα προϊόντος για Time range, Other→Yesterday :

sourcetype=access_* action=purchase | stats count by product_name

Σε αυτόν τον πίνακα παρουσιάζεται ο αριθμός των προϊόντων που πωλήθηκαν χθες



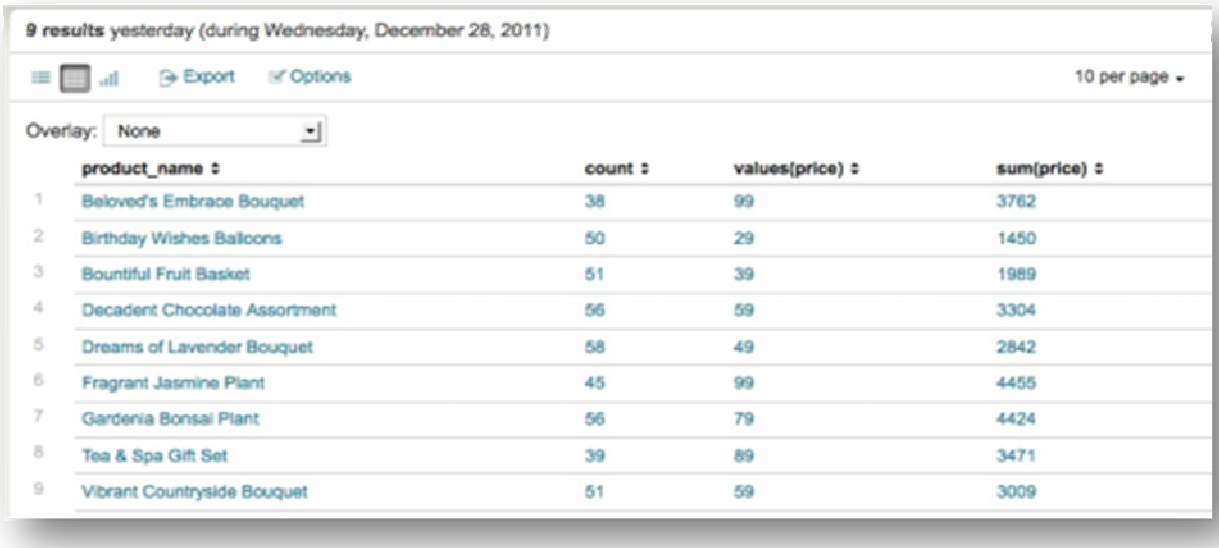
	product_name	count
1	Beloved's Embrace Bouquet	38
2	Birthday Wishes Balloons	50
3	Bountiful Fruit Basket	51
4	Decadent Chocolate Assortment	56
5	Dreams of Lavender Bouquet	58
6	Fragrant Jasmine Plant	45
7	Gardenia Bonsai Plant	56
8	Tea & Spa Gift Set	39
9	Vibrant Countryside Bouquet	51

ανά είδος.

2. Χρησιμοποιούμε την εντολή stats για να παραλάβουμε τον αριθμό των προϊόντων που αγοράστηκαν, την τιμή για το κάθε ένα από αυτά και το σύνολο των εσόδων που συγκεντρώθηκαν από τις αγορές.

sourcetype=access_* action=purchase | stats count, values(price), sum(price) by product_name

Η μέθοδος count() μετρά τον αριθμό των events. Η εντολή values() επιστρέφει την τιμή του κόστους για κάθε product_name. Το sum() αθροίζει τα κόστη για κάθε product_name.



9 results yesterday (during Wednesday, December 28, 2011)

Export Options 10 per page

Overlay: None

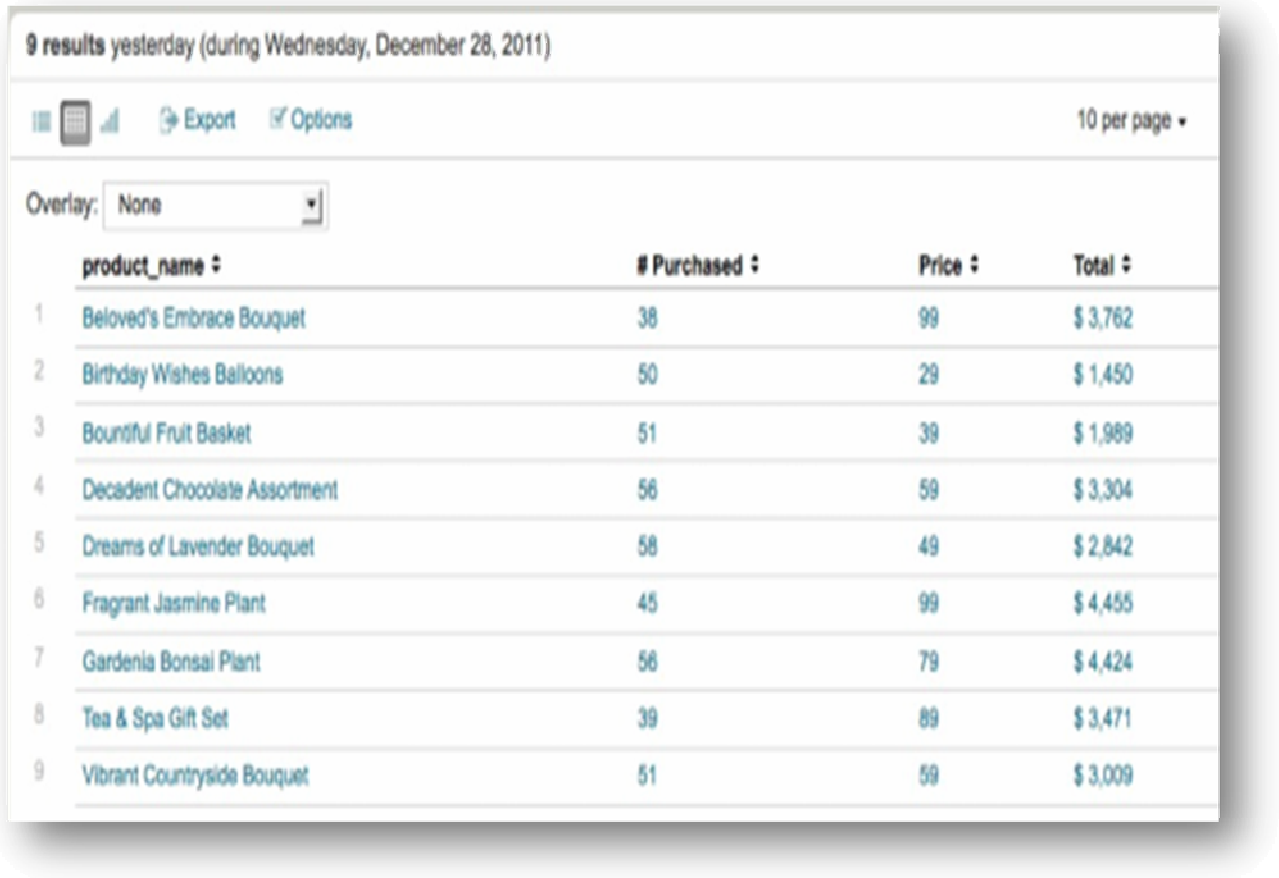
	product_name	count	values(price)	sum(price)
1	Beloved's Embrace Bouquet	38	99	3762
2	Birthday Wishes Balloons	50	29	1450
3	Bountiful Fruit Basket	51	39	1989
4	Decadent Chocolate Assortment	56	59	3304
5	Dreams of Lavender Bouquet	58	49	2842
6	Fragrant Jasmine Plant	45	99	4455
7	Gardenia Bonsai Plant	56	79	4424
8	Tea & Spa Gift Set	39	89	3471
9	Vibrant Countryside Bouquet	51	59	3009

3. Τώρα απλά χρειάζεται να μετονομάσουμε τα πεδία, ώστε να κάνουμε τον πίνακα αποτελεσμάτων να φαίνεται πιο ευανάγνωστος.

sourcetype=access_* action=purchase | stats count AS "# Purchased", values(price) AS Price,

sum(price) AS Total by product_name | eval Total="$ ".tostring(Total, "commas")

το “AS” χρησιμοποιείται για να μετονομάσει τους τίτλους των στηλών του πίνακα. Επίσης χρησιμοποιήθηκε η εντολή evals to string() ώστε να μετατρέψει τις υπολογισμένες τελικές τιμές σε ένα string και να τις τροποποιήσει ώστε να περιέχουν το χαρακτήρα “$” μια και δηλώνουν χρηματικό κόστος.



9 results yesterday (during Wednesday, December 28, 2011)

Export Options 10 per page

Overlay: None

	product_name	# Purchased	Price	Total
1	Beloved's Embrace Bouquet	38	99	$ 3,762
2	Birthday Wishes Balloons	50	29	$ 1,450
3	Bountiful Fruit Basket	51	39	$ 1,989
4	Decadent Chocolate Assortment	56	59	$ 3,304
5	Dreams of Lavender Bouquet	58	49	$ 2,842
6	Fragrant Jasmine Plant	45	99	$ 4,455
7	Gardenia Bonsai Plant	56	79	$ 4,424
8	Tea & Spa Gift Set	39	89	$ 3,471
9	Vibrant Countryside Bouquet	51	59	$ 3,009

4. Αποθηκεύουμε την αναζήτηση ως “Purchases&Revenue” για χρόνο Yesterday.

<u>Παράδειγμα 4.</u>

Πόσες προσπάθειες ολοκλήρωσης παραγγελίας κρίθηκαν αποτυχημένες;

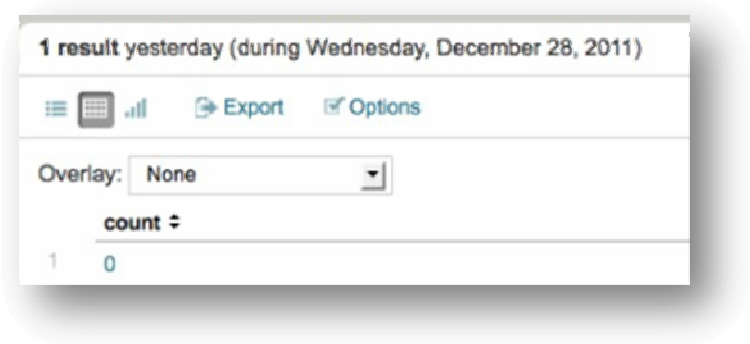
1. Τρέχουμε την αναζήτηση για αποτυχημένες προσπάθειες αγοράς την προηγούμενη ημέρα:

sourcetype=access_* action=purchase status=503

Αυτή η αναζήτηση επιστρέφει τα αποτελέσματα όλων των events που αφορούν τις αποτυχημένες παραγγελίες οπότε μένει να μετρηθεί ο αριθμός τους.

2. Χρησιμοποιούμε την εντολή stats:

sourcetype=access_* action=purchase status=503 | stats count



Αυτή η αναζήτηση επιστρέφει μια μοναδική τιμή, το μηδέν, γεγονός που σημαίνει ότι χθες δεν αντιμετωπίστηκε κανένα πρόβλημα στις παραγγελίες.

3. Αποθηκεύουμε αυτή την αναζήτηση ως “Failed Purchases(Yesterday)” (Αποτυχημένες αγορές χθες).

Παραδείγματα εκθέσεων

Σε αυτή την ενότητα με τη χρήση των αναζητήσεων, οι οποίες αποθηκεύτηκαν στην ενότητα *παραδείγματα αναζήτησης* , θα εξηγηθεί ο τρόπος δημιουργίας Εκθέσεων (Reports), με τη βοήθεια διαγραμμάτων (charts).

Οι αναζητήσεις που πραγματοποιήθηκαν παραπάνω για το ηλεκτρονικό κατάστημα **«Flowers & Gifts Shop»**, επέστρεφαν κάποια μοναδική τιμή (για παράδειγμα τον αριθμό των αποτυχημένων προσπαθειών ολοκλήρωσης παραγγελιών) ή ένα πίνακα αποτελεσμάτων (λίστα των προϊόντων που αγοράστηκαν). Παρακάτω θα παρουσιαστούν αυτές οι αναφορές με τη μορφή γραφημάτων.

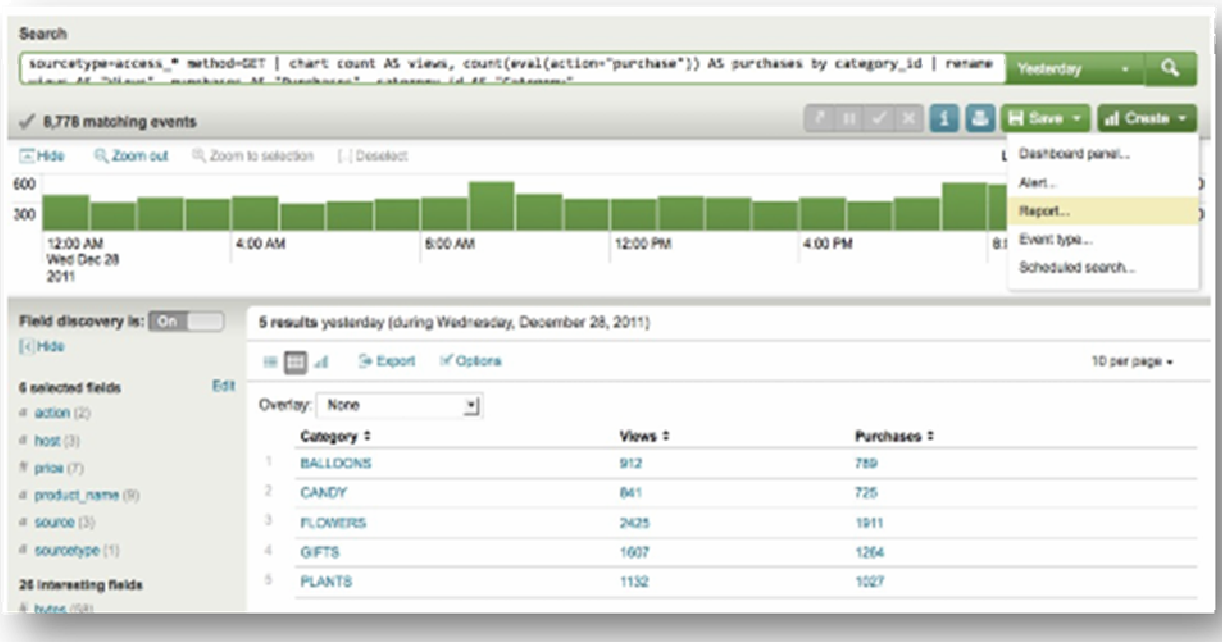
Παράδειγμα 1.

Πόσες φορές κοίταξε κάποιος ένα προϊόν και πόσες φορές αγοράστηκε. Σε αυτό το παράδειγμα θα φανεί με τη βοήθεια γραφήματος ο αριθμός, αυτών των views που είχε ένα προϊόν στη σελίδα και ο αριθμός των αγορών που το αφορούν.

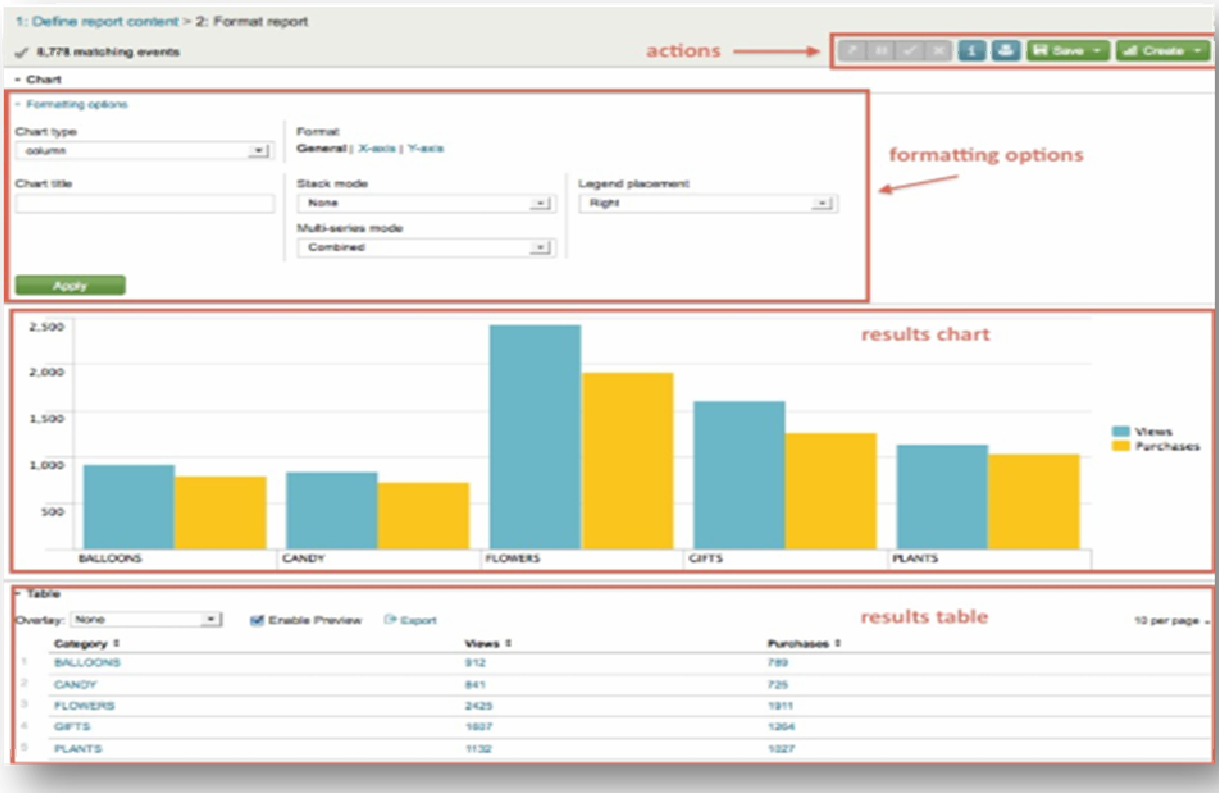
1. Ανατρέχουμε στην αποθηκευμένη αναζήτηση %Purchases & Revenue(Yesterday) και την τροποποιούμε:

sourcetype=access_* method=GET | chart count AS views, count(eval(action="purchase")) ASpurchases by category_id | rename views AS "Views", purchases AS "Purchases", category_id AS "Category"

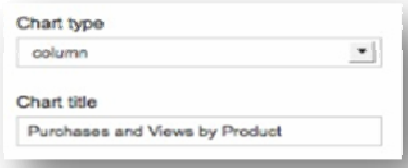
Η εντολή chart επιτρέπει τη δημιουργία διαγραμμάτων αξόνων, ορίζοντας τα ονόματα τους με την εντολή by.



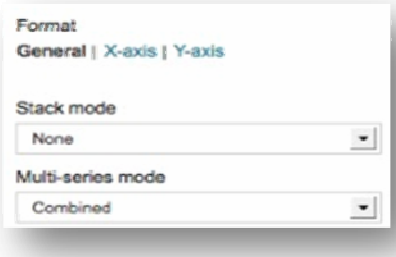
2. Πατάμε στην επιλογή Create πάνω δεξιά και επιλέγουμε Report από τη λίστα. Επειδή έχουμε χρησιμοποιήσει την εντολή chart έχει ήδη διαμορφωθεί το μενού ρυθμίσεων για το διάγραμμα, όπως βλέπουμε στην εικόνα (αριθμος εικονας).



3. Κάτω από τις επιλογές ρυθμίσεων (Formating options), αφήνουμε την επιλογή chart type στην προεπιλογή column ώστε το γράφημα να έχει τη μορφή στηλών. Ονομάζουμε το chart “Purchases & Views by Product type” (Αγορές και εμφανίζεις ανά τύπο προϊόντος).

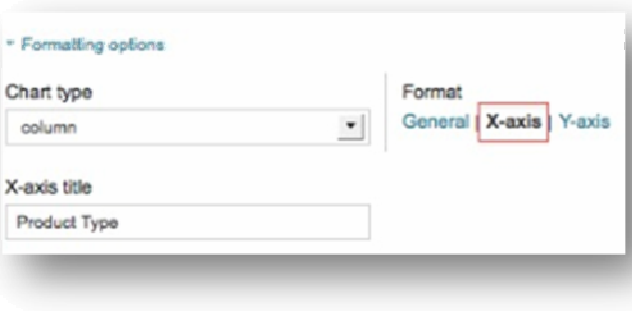


4. Κάτω από το General αφήνουμε τις επιλογές ως έχουν.



5. Κάτω από την επιλογή Format πατάμε x-axis:

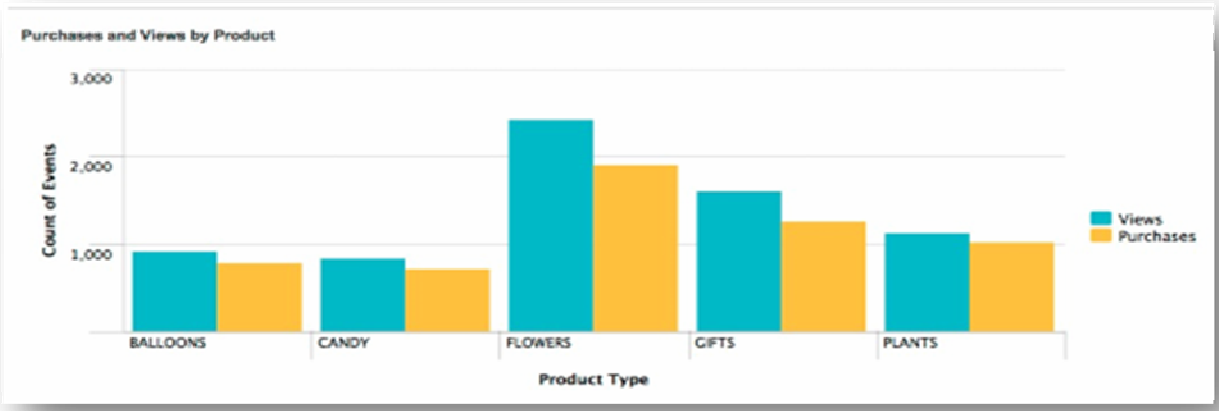
Πληκτρολογούμε στο πεδίο “Product type” για να ονομάσουμε τον άξονα x.



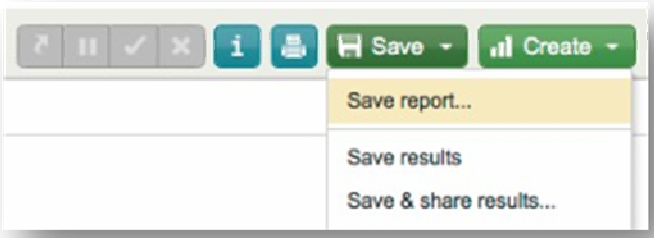
6. Κάτω από την επιλογή Format πατάμε y-axis:

Πληκτρολογούμε στο πεδίο “Count of events” για να ονομάσουμε τον άξονα y.

7. Επιλέγουμε Apply (Αποδοχή).

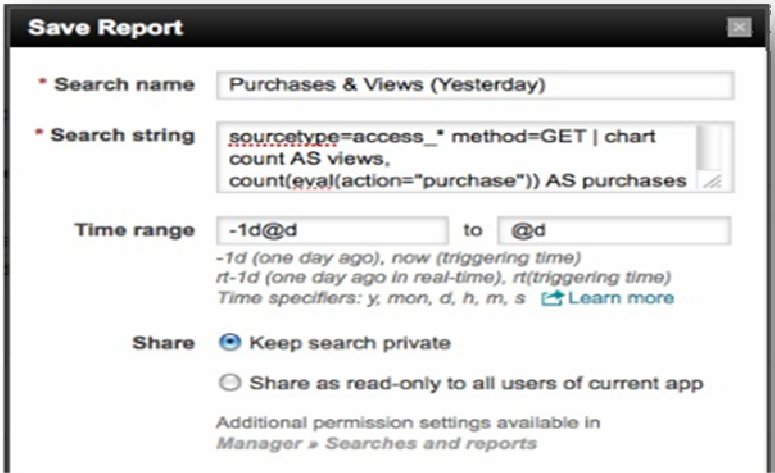


Στο γράφημα που εμφανίζεται παρουσιάζονται οι αγορές και οι εμφανίζεις των προϊόντων σε μορφή στηλών.



8. Πατάμε Save και επιλέγουμε Save Report από τη λίστα:

Το παράθυρο αποθήκευσης της έκθεσης εμφανίζεται. Στο πεδίο Search name πληκτρολογούμε το όνομα της έκθεσης Purchases & Views (Yesterday) και πατάμε Finish.



Παράδειγμα 2.

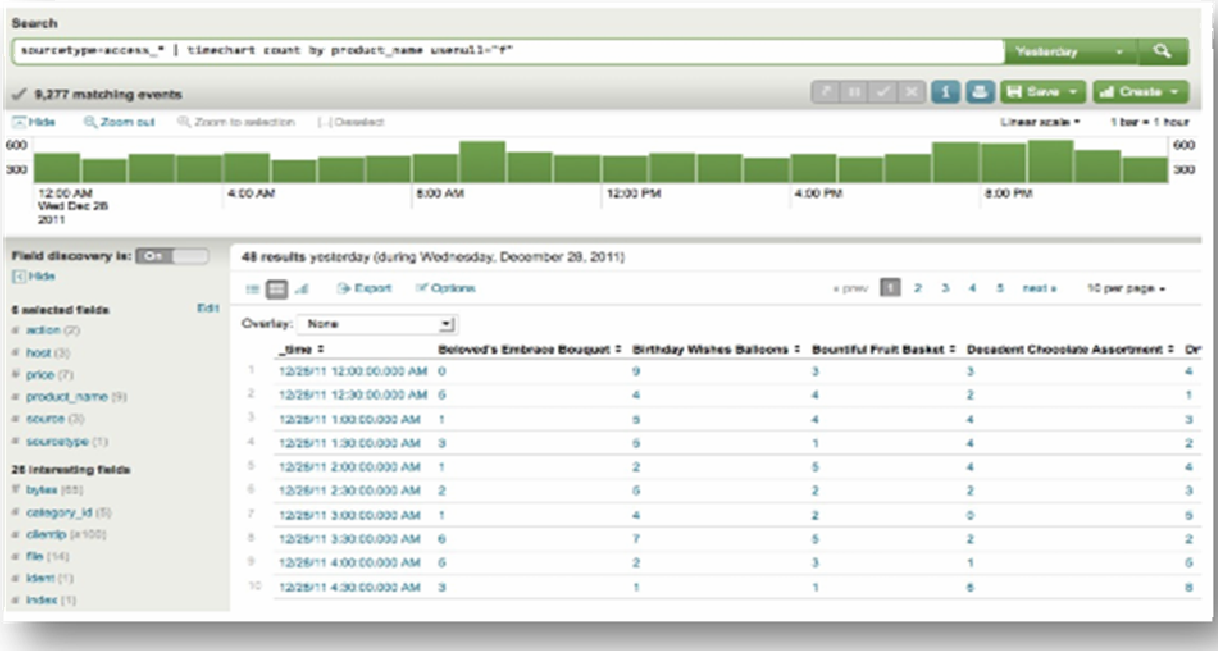
Κορυφαίες πωλήσεις ανά κατηγορία προϊόντος.

Η δημιουργία αυτού του Report, απαιτεί τη χρήση του πεδίου Product_name που εισήχθη από το Lookup table, για να μετρηθεί ο αριθμός των αγορών που πραγματοποιήθηκε για κάθε προϊόν την προηγούμενη ημέρα.

1. Πληκτρολογούμε την αναζήτηση:

sourcetype=access_* | timechart count(eval(action="purchase")) by product_name usenull="f"

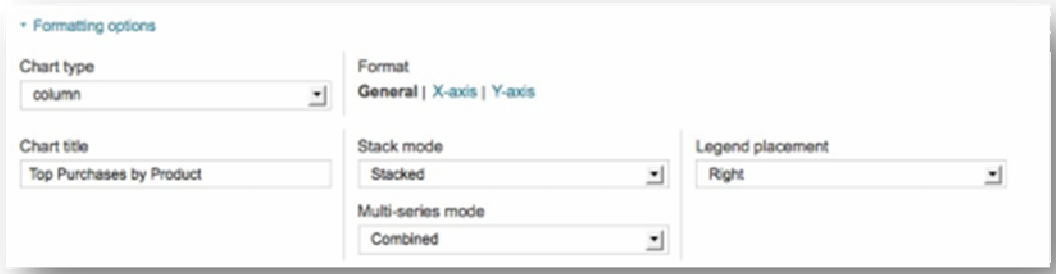
Η εντολή count χρησιμοποιείται για να μετρηθεί ο αριθμός των events και η εντολή usenull για να εξασφαλιστεί ότι το chart θα περιέχει μη μηδενικές τιμές για το πεδίο product_name.



2. Επιλέγουμε Create report.

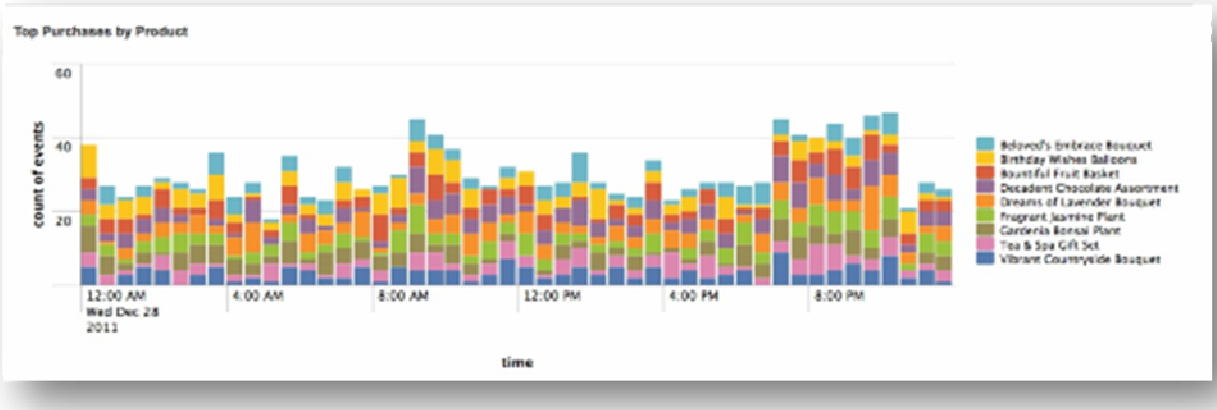
Επειδή έχουμε χρησιμοποιήσει την εντολή timechart το μενού των επιλογών διαμορφώνεται διαφορετικά από το μενού για το chart.

3. Κάτω από την επιλογή Formatting options αλλάζουμε το chart type σε column, ονομάζουμε το chart Top Purchases by product και επιλέγουμε Stacked στο πεδίο Stack.



Με τη χρήση της εντολής timechart οι άξονες x και y ονομάζονται αυτόματα. Ο x ονομάζεται time και ο y ονομάζεται count of events.

4. Επιλέγουμε Apply.



Κάθε μία από τις στήλες αντιπροσωπεύει τα διαφορετικά προϊόντα που αγοράστηκαν μέσα σε χρονικό διάστημα μισής ώρας.

5. Πατάμε Save και επιλέγουμε Save Report. Ονομάζουμε την αναφορά Products Purchases (Yesterday). Προσθέτουμε μια σύντομη περιγραφή της αναφοράς και πατάμε Save.

Δημιουργία Dashboard

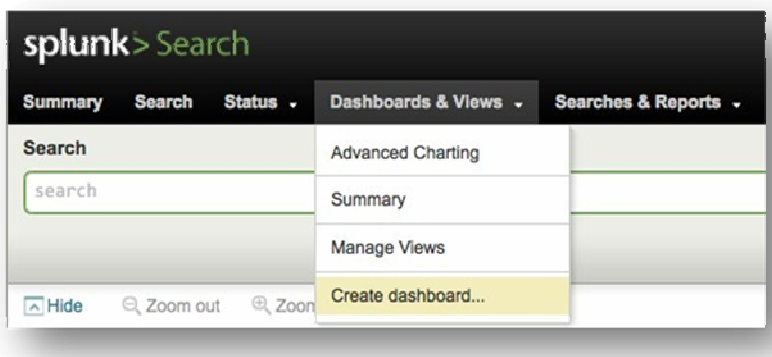
«Επιστρέφουμε» στο ηλεκτρονικό κατάστημα «**Flower & Gift Shop**». Βρισκόμαστε στη διαδικασία δημιουργίας ενός dashboard που θα δείχνει μετρήσεις σχετικά με τις αγορές των προϊόντων κάθε ημέρα.

Για αυτό το Dashboard θα χρησιμοποιήσουμε τις αποθηκευμένες αναζητήσεις που δημιουργήσαμε τις προηγούμενες ημέρες:

- Products Purchased (Yesterday)
- Products & Revenue (Yesterday)
- Purchases & Views (Yesterday)

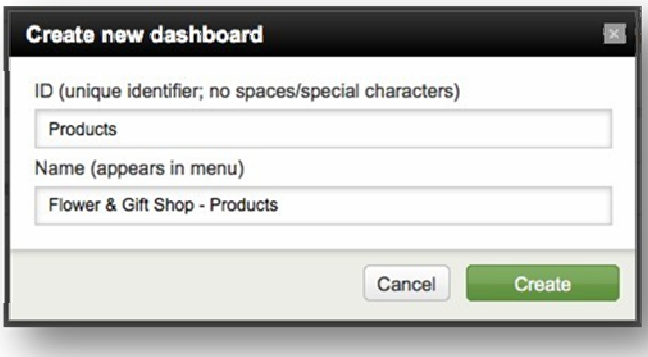
Ανοίγουμε το Search app.

1. Κάνουμε κλικ στο μενού Dashboard & Views και από την αναδυόμενη λίστα επιλέγουμε το Create dashboard.



Το παράθυρο οιαλογου που ανοιγει επιτρεπει να οριστει ενα νεο dasnboard.

2. Δημιουργία καινούριου dashboard:



3. Ορίζουμε '. Το ID είναι το όνομα που χρι βρισκόμαστε σε άλλα dashboards μέσα στο Splunk.

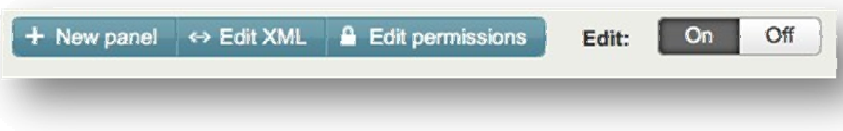
4. Ονομάζουμε το dashboard, Flower & Gift Shop. Αυτό το όνομα είναι και η ετικέτα που θα δούμε να υπάρχει στα μενού πλοήγησης και στην κορυφή του dashboard.

5. Επιλέγουμε Create.

Αυτή η επιλογή μας πηγαίνει στο καινούριο dashboard, το οποίο είναι άδειο. Ας ξεκινήσουμε να το γεμίζουμε με panels.

6. Στην κορυφή του dashboard, δίπλα στο όνομα του, βρίσκονται οι επιλογές του dashboard. Όταν το Edit είναι απενεργοποιημένο , θα δούμε επιλογές εκτύπωσης του dashboard και παράδοση σε PDF.

7. Για να αρχίσουμε την επεξεργασία του dashboard, αλλάζουμε το Edit σε ON.



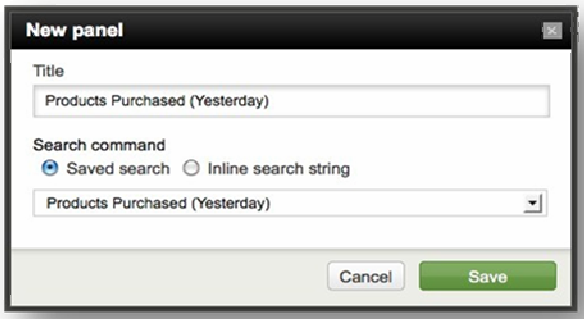
Όταν ενεργοποιηθεί το Edit, θα δούμε 3 επιλογές:

- New panel, το οποίο μας επιτρέπει την πρόσθεση panels στο dashboard.
- Edit XML, που μας επιτρέπει την επεξεργασία του κώδικα XML για το dashboard.
- Edit permissions , που μας επιτρέπει τον έλεγχο της προσβασιμότητας στο dashboard.

8. Για να προσθέσουμε ένα panel στο dashboard, επιλέγουμε New panel.

Αυτό ανοίγει το παράθυρο διαλόγου New panel , το οποίο επιτρέπει τον ορισμό των ιδιοτήτων για το panel.

9. Για να προσθέσουμε ένα panel στο dashboard, δίνουμε ένα όνομα και καθορίζουμε την αναζήτηση που συσχετίζεται με αυτό.



10. Κάτω από το “Title”, στο πεδίο πληκτρολογούμε "Products Purchased (Yesterday)". Αυτή είναι η ετικέτα για το panel.

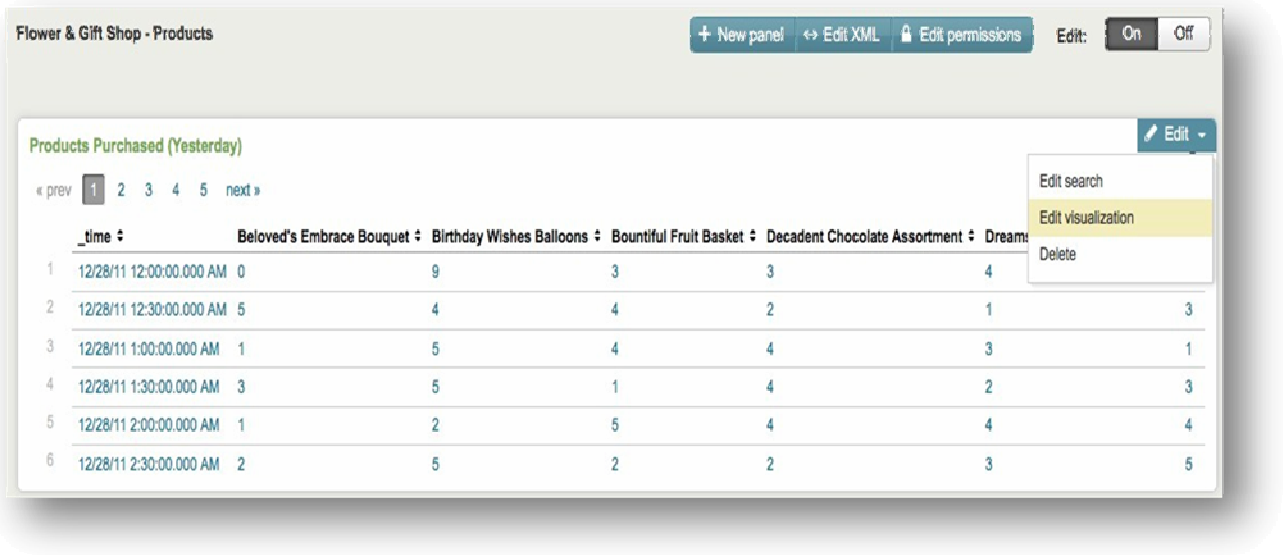
11. Κάτω από το “Search command”, επιλέγουμε “Saved search"

Όλα τα dashboard είναι συνδεδεμένα με τις αναζητήσεις. Μπορούμε να προσδιορίσουμε, αν ένα panel τρέχει από μια προκαθορισμένη αποθηκευμένη αναζήτηση, ή αν χρησιμοποιεί μια αναζήτηση σχεδιασμένη ειδικά για το panel. Για αυτά τα dashboards, θα χρησιμοποιήσουμε αποθηκευμένες αναζητήσεις και αναφορές.

12. Από τη λίστα , επιλέγουμε την αποθηκευμένη αναζήτηση με όνομα "Products Purchased (Yesterday)".

13. Επιλέγουμε Save.

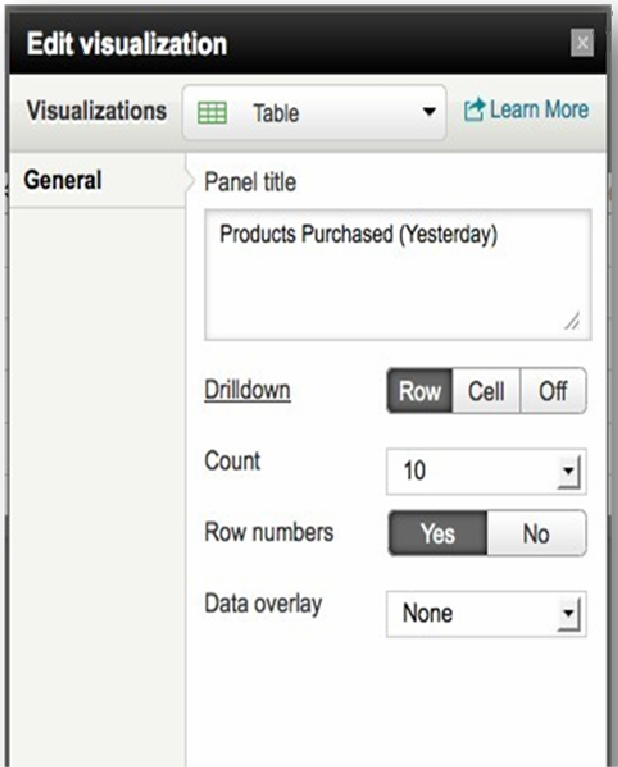
Τώρα έχουμε προσθέσει ένα καινούριο panel στο "Flower & Gifts Shop - Products" dashboard. Εδώ τα αποτελέσματα της αναζήτησης προβάλλονται με τη μορφή ένος πίνακα. Αυτή δεν είναι η επιθυμητή προβολή για το panel, οπότε προβαίνουμε στην



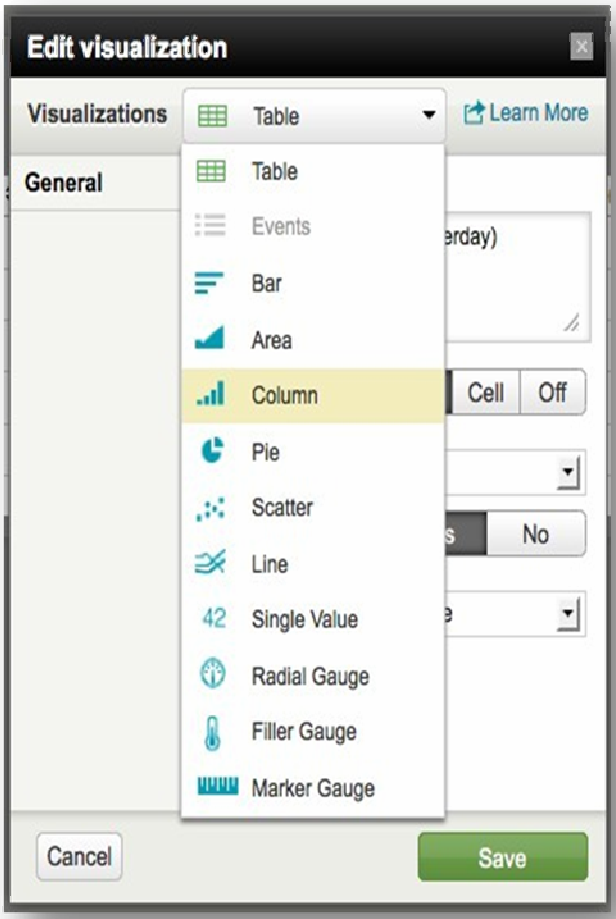
αλλαγή του.

14. Για το panel, επιλέγουμε Edit→ Edit visualization από τη λίστα.

Αυτό ανοίγει το παράθυρο διαλόγου Edit visualization, που μας επιτρέπει τον καθορισμό του τρόπου εμφάνισης των αποτελεσμάτων αναζήτησης στο panel: data table, events list, charts, single value panels, and gauges.

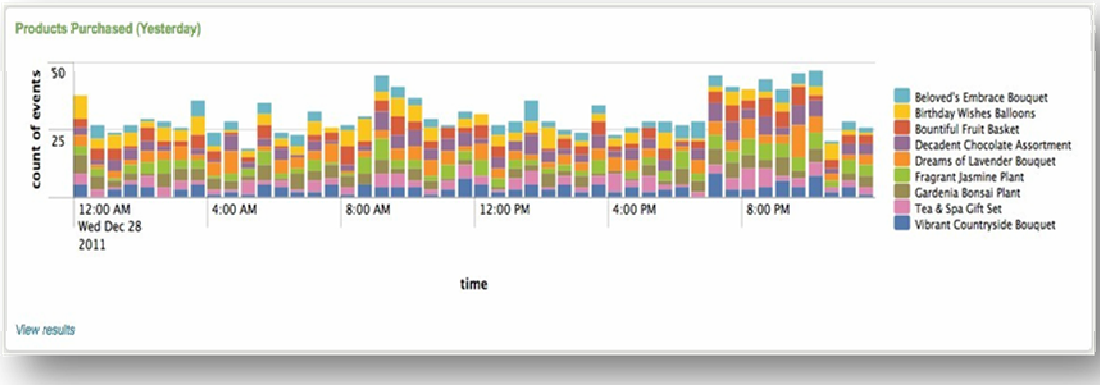


15. Από τη λίστα "Visualizations", επιλέγουμε Column για να εμφανίσουμε τα



αποτελέσματα μας σε γράφημα στήλης .

16. Επιλέγουμε Save.



Προσθέτουμε δύο επιπλέον panel στο dashboard:

17. Προσθέτουμε ένα panel με όνομα Purchases & Views (Yesterday) για τον αριθμό των αγορών και προβολών που έγιναν χθες (# Purchases & Views). Αλλάζουμε την προβολή, ώστε να εμφανίζονται σε γράφημα στηλών.

18. Προσθέτουμε ένα panel με όνομα Products & Revenue (Yesterday) για να προβάλουμε τα προϊόντα που πουλήθηκαν χτες καθώς επίσης και τα έσοδα που υπήρχαν από τις πωλήσεις (Purchases and Revenue (Yesterday). Αλλάζουμε τον τρόπο προβολής ώστε να βλέπουμε έναν πίνακα δεδομένων.

19. Όταν προσθέσουμε τα καινούρια panel, φτιάχνουμε τα παράθυρα ώστε να

εμφανίζονται ως εξής:

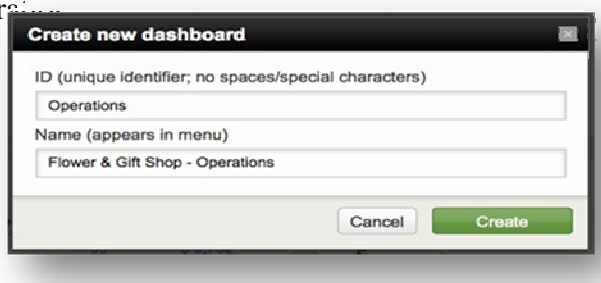
Αυτό είναι το dashboard των προϊόντων μας. Τώρα με παρόμοιο τρόπο θα δημιουργήσουμε ένα operations dashboard.

«Flower & Gift Shop» Operations

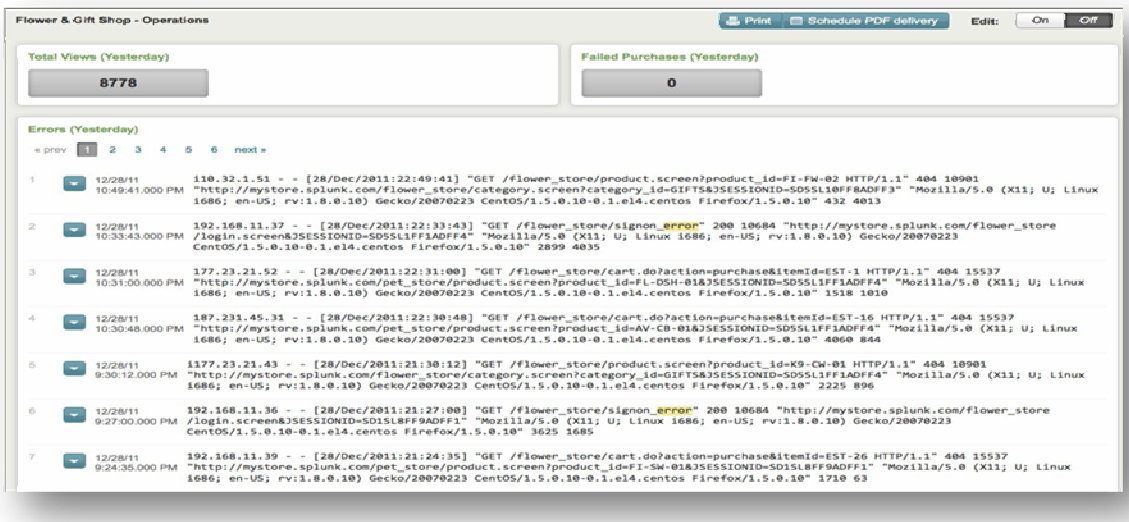
Το δεύτερο dashboard περιέχει απλές αναφορές που μπορούμε να δούμε στο ξεκίνημα της ημέρας και να πάρουμε πληροφορίες σχετικά με πρόσφατη διαδικτυακή δραστηριότητα. Για αυτό το dashboard, θα χρησιμοποιήσουμε τις εξής αποθηκευμένες αναζητήσεις:

- Total views (Yesterday).
- Failed purchases (Yesterday).
- Errors (Yesterday).

Επιστρέφουμε στο Search app. Επιλέγουμε Dashboards & Views→Create dashboard από την αναδυόμενη λίστα και ορίζουμε ένα καινούριο dashboard για το «**Flower & Gift Shop**» - Operations.



1. Για αυτό το dashboard, θα προσθέσουμε τρία panel: δύο panel μοναδικών τιμών και ένα panel, στο οποίο θα εμφανίζει τη λίστα με τα events.Θα εμφανίζεται κάπως έτσι:



2. Το πρώτο panel χρησιμοποιεί την αποθηκευμένη αναζήτηση "Total views (Yesterday)" και είναι ένα panel μοναδικής τιμής.

3. Το δεύτερο panel χρησιμοποιεί την αποθηκευμένη αναζήτηση "Failed purchases (Yesterday)" και είναι ένα panel μοναδικής τιμής.

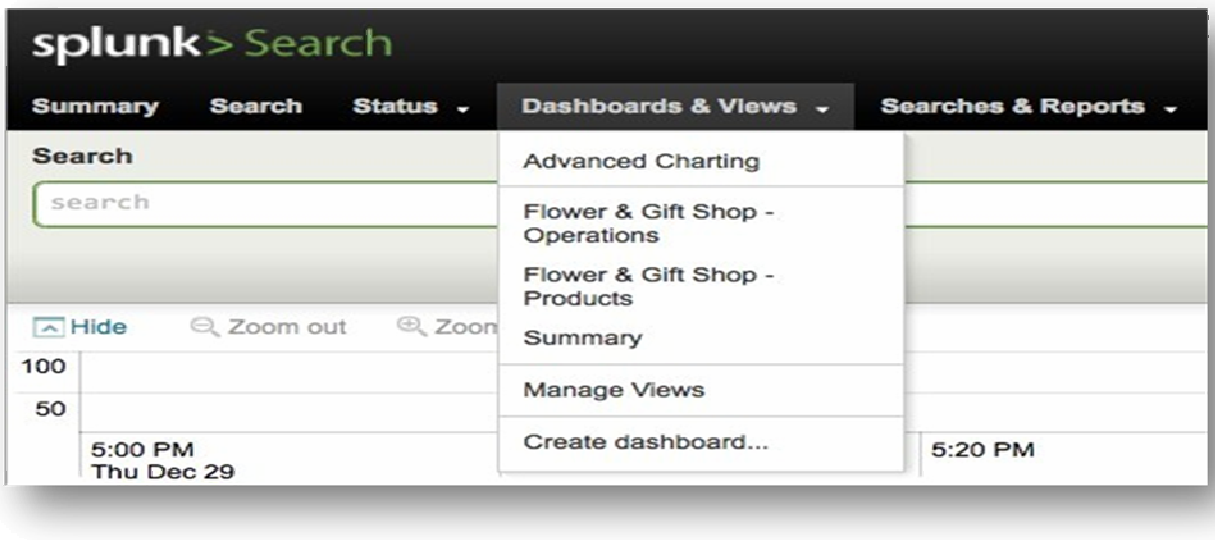
4. Το τρίτο panel χρησιμοποιεί την αποθηκευμένη αναζήτηση "Errors (Yesterday)" και είναι ένα event list panel.

5. Όταν προσθέσουμε τα καινούρια panel, τα φτιάχνουμε ώστε να εμφανίζονται όπως στην παραπάνω εικόνα.

Αυτό είναι το «**Flower & Gift Shop**» Operations dashboard.

Προβολή αποθηκευμένων Dashboard.

Αφού αποθηκεύσουμε τα dashboards, μπορούμε να τα βρούμε στο Search App κάτω από το Dashboards & Views:



Από αυτή τη λίστα, μπορούμε επίσης να τροποποιήσουμε ή να διαχειριστούμε τα dashboard που ήδη έχουμε.

Κεφάλαιο 2

Social Media

Η έννοια των Social Media

Ο όρος Social Media είναι ιδιαίτερα διαδεδομένος όμως σε κάποιες περιπτώσεις είναι δύσκολο να δοθεί ο ακριβής ορισμός του λόγω των πολλών διαστάσεων που έχει. Ο καλύτερος λοιπόν τρόπος για να ορίσει κάποιος την έννοια των Social Media είναι να εξετάσεις τα επιμέρους στοιχεία τους.

Τα Media είναι ένα εργαλείο επικοινωνίας, όπως η εφημερίδα ή το ραδιόφωνο, οπότε κατ' αντιστοιχία θα μπορούσαμε να χαρακτηρίσουμε τα Social Media ως εργαλεία επικοινωνίας με κοινωνικό χαρακτήρα.

Τα απλά μέσα από επικοινωνιακής πλευράς μοιάζουν με μονόδρομο καθώς μπορεί κανείς να διαβάσει μια εφημερίδα ή να παρακολουθήσει ένα δελτίο ειδήσεων στην τηλεόραση, αλλά με περιορισμένες δυνατότητες αλληλεπίδρασης..

Αντίθετα τα Social Media ως απόρροια αυτού που ονομάζουμε Web 2.0 ενθαρρύνουν την αμφίδρομη επικοινωνία. Μέσω των Social Media κάθε χρήστης έχει πρόσβαση όχι μόνο στην εύρεση και δημοσίευση περιεχομένου αλλά και στη διαδραστικότητα με το δημοσιευμένο περιεχόμενο ή άλλους χρήστες. Η

διαδραστικότητα αυτή μπορεί να περιορίζεται σε κάτι απλό όπως τη δημοσίευση σχολίων ή την αξιολόγησή του περιεχομένου της παρεχόμενης πληροφορίας ή μπορεί να είναι περισσότερο πολύπλοκή όπως συμβαίνει για παράδειγμα στην κοινότητα του Flixter η οποία παρέχει στα μέλη της προτάσεις ταινιών βασιζόμενη στις αξιολογήσεις ατόμων με παρόμοια ενδιαφέροντα.

Οι περισσότερες υπηρεσίες Social Media ενθαρρύνουν και επιδιώκουν τη συζήτηση, τα σχόλια, την αλληλεπίδραση και το διαμοιρασμό οποιασδήποτε πληροφορίας μεταξύ των χρηστών. Στην έννοια Media θα μπορούσαμε να δώσουμε τον ορισμό της σύγχρονης επικοινωνίας μιας και όλα όσα αναφέρονται παραπάνω δεν είναι τίποτα άλλο από σύγχρονους διαμοιραστές πληροφορίας. Οποιαδήποτε είδους και ποιότητα πληροφορίας μπορεί να ταξιδέψει μέσα από πληθώρα εφαρμογών του διαδικτύου. Η διαφορά με τις παραδοσιακές μορφές επικοινωνίας είναι αρχικά το εύρος που μπορεί να μεταδοθεί η πληροφορία και κατά δεύτερον ότι ο χρήστης είναι ο βασικός πρωταγωνιστής. Τα Social Media είναι ένα σύγχρονο απλοποιημένο εργαλείο επικοινωνίας. Ωστόσο η χρήση τους και ειδικότερα η αποτελεσματικότητα τους εξαρτάται σε μεγάλο βαθμό από το χρήστη.

Κατηγορίες Social Media

Τα Social Media κατηγοριοποιούνται σε:

- **Social News**: Πρόκειται για sites με ειδήσεις και άρθρα όπου ο χρήστης μπορεί να ψηφίσει και να σχολιάσει. Τα άρθρα με τους περισσότερους ψήφους αναβαθμίζονται και προωθούνται προς τους αναγνώστες(Digg, Sphinn, Newsvine, BallHype κ.α.).

- **Social Sharing**: Sites που δίνουν τη δυνατότητα να δημιουργίας και διαμοιρασμού αρχείων ήχου και εικόνας(Youtube, Flickr, Devianart)

- **Social Bookmarking**: Sites που δίνουν τη δυνατότητα εύρεσης και αποθήκευσης δικτυακών τόπων και χρήσιμων πληροφοριών. Οι σελιδοδείκτες αποθηκεύονται online και διαμοιράζονται αντίστοιχα σε άλλους χρήστες(Diigo, BlogMarks, Faves).

- **Social Networks**: Πρόκειται ίσως για την πιο διαδεδομένη μορφή Social Media μιας και προσφέρει πιο άμεση επικοινωνία μεταξύ των χρηστών. Ένα τεράστιο μέσο κοινωνικής δικτύωσης που εκμηδενίζει τις αποστάσεις και ξεπερνά τα παραδοσιακά μέσα επικοινωνίας. Μέσα από αυτά τα site οι χρήστες επικοινωνούν μεταξύ τους, ενημερώνονται και ανταλλάσσουν πληροφορίες σχετικά με τα ενδιαφέροντα τους και τις δραστηριότητες τους(Twitter, Facebook, GooglePlus, Myspace).

Τα Social Media στη ζωή του σύγχρονου ανθρώπου και η σημασία των Social Networks

> **"We have technology, finally, that for the first time in human history allows people to really maintain rich connections with much larger numbers of people. It used to be, your connected group was really your immediate community, your neighborhood, your village, your tribe. The more we connect people, the more people know one another, the better the world will be."**
>
> Pierre Omidyar, eBay Founder

Τα Social Media τα τελευταία χρόνια σημειώνουν αλματώδη ανάπτυξη. Είναι μια τάση της εποχής που πλέον τείνει να γίνει τρόπος ζωής εφόσον σύμφωνα με έρευνα η οποία διεξήχθη από το ITU (International Telecommunication Union) και παρουσιάζεται στο "Trends In Telecommunication Reform" (2012) οι χρήστες των Social Media παγκοσμίως ανέρχονται στο 1.000.000.000 με ολοένα αυξητικές τάσεις.

Τα Social Media αποτελούν ένα καθημερινό τεράστιο όγκο περιεχομένου που κυκλοφορεί στο διαδίκτυο, με πολύ μεγάλες δυνατότητες σχεδόν για οποιεσδήποτε ανάγκες. Εκτός από την διασκέδαση ή την επικοινωνία μεταξύ των χρηστών τους, μπορεί να προσφέρει πληροφόρηση και δικτύωση για συνεργασία σε επιστήμονες, προώθηση προϊόντων ή υπηρεσιών...

Αν εξεταστεί σε αυστηρά επιχειρηματικό επίπεδο, η δύναμη που δίνεται τον καταναλωτή είναι τεράστια. Οι πηγές ενημέρωσης και επιρροής δεν είναι μόνο τα ΜΜΕ αλλά και οι διαδικτυακοί φίλοι ή ακόμα και άγνωστοι που είχαν μια εμπειρία με κάποια υπηρεσία ή προϊόν και το ανέφεραν στο Facebook, Twitter ή σε κάποιο σχόλιο ενός blog.

Τα Social Media θα αποκτούν σταδιακά συνεχώς μεγαλύτερο μερίδιο της ενημέρωσης, επικοινωνίας και επομένως επιρροής μας.

Οι πλατφόρμες **Social Networking** δεν περιορίζονται στην παροχή δυνατοτήτων που αποσκοπούν στη επανασύνδεση φίλων, στην επικοινωνία, στη συμμετοχή σε online παιχνίδια. Στην πραγματικότητα τα Social Networks είναι κάτι παραπάνω, είναι ένας νέος εναλλακτικός τρόπος επικοινωνίας, αλληλεπίδρασης και διασύνδεσης μελών διαφόρων ομάδων σε προσωπικό ή εταιρικό επίπεδο, δωρεάν ή με ιδιαίτερα χαμηλό κόστος.

Αν είναι λοιπόν είναι επιβεβλημένη η παρουσία ενός οργανισμού ή μιας εταιρίας στο διαδίκτυο πρέπει κανείς να αναλογιστεί ποσό πιο σημαντική είναι η επικοινωνία και η δημιουργία διαλόγου με το κοινό του παρέχοντας "χρήσιμο" περιεχόμενο. Άλλωστε πώς αλλιώς θα γνώριζε το κοινό για τη δραστηριότητά, τα προϊόντα ή τις υπηρεσίες που παρέχει μια εταιρία;

Κάποια λοιπόν από τα πλεονεκτήματα της χρήσης των Social Media από Οργανισμούς και επιχειρήσεις είναι τα εξής: Προσφέρουν γρήγορη και άμεση επικοινωνία με το κοινό. Βοηθούν στη στελέχωση μιας παραγωγικής επικοινωνίας με πιθανούς πελάτες και τους φέρνει ένα βήμα πιο κοντά σε μια πιθανή συνεργασία. Δίνουν τη δυνατότητα απόκτησης αξιόπιστων δεδομένων σχετικά με τη ζήτηση υπηρεσιών και προϊόντων από το αγοραστικό κοινό ή απόψεων του όσων αφορά τις υπηρεσίες ή το προφίλ ενός οργανισμού ή εταιρείας με σκοπό την καλύτερη προσαρμογή των διαφημιστικών πλάνων και την ποιότητα υπηρεσιών. Τα Social Networks μπορούν να εμπλέξουν το κοινό με το μια εταιρεία με φυσικό ή συναισθηματικό τρόπο ανάλογα με το πώς αυτή θα επιλέξει να προβάλλεται, ικανοποιώντας βασικές αγοραστικές αλλά και ανθρωπιστικές ανάγκες του . Όταν η επικοινωνία με το κοινό είναι εποικοδομητική και σε προσωπικό επίπεδο, κάνει τον κάθε εμπλεκόμενο να νιώθει σημαντικό μέρος αυτής της διεπαφής και ο διαφημιζόμενος φορέας έχει την ευκαιρία να αποκτήσει μια πελατοκεντρική φιλοσοφία, δημιουργώντας ένα νέο περιβάλλον για την επιχείρηση του αποκομίζοντας νέες ιδέες που τον καθιστούν προσιτό και απαραίτητο στο κοινό.Τέλος τα θετικά αποτελέσματα δεν αφορούν μόνο τη σχέση ενός οργανισμού ή επιχείρησης με τους πελάτες τους αλλά αφορούν και τη σχέση του ανθρώπινου δυναμικού που τους στελεχώνει. Οι εταιρείες που αναπτύσσουν τα δικά τους Social networks πετυχαίνουν να φέρουν κοντά ομάδες εργαζομένων που βρίσκονται σε απομακρυσμένα γραφεία, ενισχύουν το δέσιμο μεταξύ των εργαζομένων και τους βοηθούν να λειτουργήσουν πιο αποτελεσματικά στο έργο που έχουν αναλάβει.

Τι είναι το Twitter

Το Twitter, το οποίο φτιάχτηκε το 2006 από τον Τζακ Ντόρσεϊ, είναι μια δωρεάν Social network και micro-blogging υπηρεσία, η οποία επιτρέπει στους χρήστες του να γράφουν σύντομα μηνύματα και να διαβάζουν τα μηνύματα άλλων χρηστών της υπηρεσίας (τα γνωστά ως tweets). Social γιατί επιτρέπει την επαφή και αλληλεπίδραση με άλλα μέλη του και Μικρο-blogging γιατί δίνει τη δυνατότητα σε κάποιον να γράψει την κατάστασή του μέσα σε 140 χαρακτήρες με εικόνες ή άλλα μέσα.

Στην πορεία το Twitter έγινε και άλλα πράγματα, όπως μέρος προώθησης ιδεών, προϊόντων και νέων και φυσικά εξελίχθηκε σε μια πλατφόρμα asynchronous Chat, όπου η συζήτηση μπορεί να εξελιχθεί σε μεγαλύτερη διάρκεια, αλλά και με περισσότερα άτομα απ' ότι ένα κλασικό Chat.

Το ιδιαίτερο χαρακτηριστικό του Twitter είναι η δυνατότητα ταχείας διάδοσης των νέων σε ολόκληρο τον κόσμο σε πραγματικό χρόνο. Στο παρελθόν συνέβαινε συχνά οι ειδήσεις, όπως π.χ. σεισμών ή άλλων καταστροφών, να μεταδίδονται γρηγορότερα σε ολόκληρο τον κόσμο μέσω του Twitter, παρά μέσω των ραδιοφωνικών σταθμών και των εφημερίδων. Η προώθηση των νέων γίνεται σε κλάσματα δευτερολέπτου από την δημοσιογραφία των πολιτών. Το Δεκέμβριο του 2008 την ίδια ώρα που η Αθήνα καιγόταν «φωτιά είχε πιάσει» και το Twitter από χιλιάδες tweets για τη δολοφονία του Αλέξη Γρηγορόπουλου και την κοινωνική έκρηξη που πυροδότησε. Μέσω του Twitter άνθρωποι από τη Συρία παρουσιάζουν τη συριακή επανάσταση όπως τη βιώνουν οι ίδιοι.

Το Twitter χρησιμοποιείται επίσης ως μέσο προώθησης ιδεών και πολιτικών απόψεων και συχνά διαδραματίζει σημαντικό ρόλο στις πολιτικές εξελίξεις. Σήμερα η

πολιτική δεν ασκείται πλέον μόνο στα έδρανα της Βουλής και στα πολιτικά γραφεία αλλά και μέσα των Social Network. Όλο και περισσότεροι πολιτικοί δημιουργούν λογαριασμούς στο Twitter τους οποίους χρησιμοποιούν ως πολιτικό βήμα. Είναι χαρακτηριστικό άλλωστε πως από τους 164 επικεφαλής κρατών σε όλο τον κόσμο, οι 123 χρησιμοποιούν ήδη το Twitter, διαθέτοντας είτε προσωπικό προφίλ είτε επίσημο «θεσμικό» λογαριασμό, τον οποίο θα παραδώσουν σε αυτόν που θα τους διαδεχθεί όταν αποχωρήσουν από το αξίωμα. Αυτό είναι το συμπέρασμα έρευνας που δημοσιοποίησε η εταιρεία αναλύσεων Digital Daya, σύμφωνα με την οποία παρουσία στο κοινωνικό δίκτυο έχουν παγκοσμίως 3 στους 4 ηγέτες.

Βασιζόμενη σε στοιχεία του Δεκεμβρίου του 2012, η μελέτη δείχνει πως οι ανώτατοι κρατικοί αξιωματούχοι που χρησιμοποιούν το Twitter έχουν αυξηθεί κατά 93% από το 2010, όταν άρχισαν να καταγράφονται στατιστικά δεδομένα χρήσης της πλατφόρμας. Μάλιστα, η μεγαλύτερη αύξηση παρατηρείται από το τρίτο τρίμηνο του 2011 μέχρι σήμερα, με το αντίστοιχο ποσοστό να φτάνει στο 78%.

Το Twitter εκτός των άλλων αποτελεί την ενσάρκωση του Social Media Marketing. Μέσω του Twitter προβάλλονται και καθιερώνονται οι νέες τάσεις στον τρόπο ζωής, ντυσίματος, διασκέδασης και προωθούνται προϊόντα και υπηρεσίες. Προώθηση προϊόντων και υπηρεσιών γίνεται με διάφορους τρόπους. Για παράδειγμα η σειρά Mad Men έφτιαξε Twitter λογαριασμούς για τους πρωταγωνιστές της. Το ίδιο έκανε και η σειρά The Big Bang Theory. Επίσης πολλά καταστήματα, blogs, forums, ειδησεογραφικά sites, τηλεοπτικά κανάλια έχουν ανοίξει λογαριασμό.

Σε μια εποχή που το ηλεκτρονικό εμπόριο γνωρίζει ιδιαίτερη άνθηση το Twitter παίζει το ρόλο ηλεκτρονικής βιτρίνας. Πασίγνωστες αλλά και άλλες λιγότερο γνωστές εταιρίες μέσω των Twitter λογαριασμών τους προωθούν τα προϊόντα τους και τις υπηρεσίες τους, ενημερώνουν το καταναλωτικό τους κοινό και φυσικά τους εν δυνάμει καταναλωτές των προϊόντων τους, διαδίδουν εταιρικά νέα, πληροφορούν για δράσεις κοινωνικής ευθύνης και δημιουργούν κανάλια επικοινωνίας με ομάδες ενδιαφερομένων

Πρωτοπόρες εταιρείες, όπως η Procter & Gamble, η IBM και η Nestle αξιοποιούν τα Social Media για να επιτύχουν τα παραπάνω και πολλά περισσότερα. Το Twitter, το Facebook και άλλες πλατφόρμες κοινωνικής δικτύωσης έχουν ήδη αποδειχθεί πολύτιμο εργαλείο marketing για τις επιχειρήσεις. Οι εργοδότες αναφέρουν το“brand building” ως την πλέον υποσχόμενη λειτουργία των Social

Media. Δεν είναι τυχαίο το γεγονός ότι το54% των επιχειρήσεων της λίστας Fortune 100 χρησιμοποιούν το Twitter για να την επικοινωνία με τους πελάτες τους και το 29% διατηρεί fan page στο Facebook. Επίσης, το"brand building" είναι, σύμφωνα με όσους συμμετείχαν στην έρευνα της Manpower, η πλέον υποσχόμενη λειτουργία των Social Media.

Ως εργαλείο Social Media Marketing το Twitter προσφέρει στους χρήστες του πολλά πλεονεκτήματα κι αυτό συντελεί στην επιτυχία του. Στα θετικά χαρακτηριστικά του περιλαμβάνονται:

- Το μηδαμινό κόστος χρήσης του
- Η δημιουργία λογαριασμού και η χρήση της πλατφόρμας του δεν απαιτεί ιδιαίτερες γνώσεις ή δεξιότητες από το χρήστη
- Το εύρος του κοινού στο οποίο απευθύνεται, το οποίο δεν περιορίζεται στα στενά τοπικά σύνορα.
- Η αμεσότητά του καθώς η πληροφορίες δημοσιεύονται σε πραγματικό χρόνο
- Η δυνατότητα αλλαγής ή αναπροσαρμογής των δημοσιεύσεων με πολύ απλό τρόπο και χωρίς επιπρόσθετο κόστος.

Η εξέλιξη αυτή του Twitter σε εργαλείο Marketing γέννησε την ανάγκη δημιουργίας εφαρμογών για την μελέτη, εκτίμηση και εξαγωγή συμπερασμάτων σχετικά με τις τάσεις του κοινού, τη δραστηριότητα του και τις αντιδράσεις του στα διάφορα tweets.

Κεφάλαιο 3

Android

Ιστορική Αναδρομή

Ξεκινώντας την περιήγηση στον κόσμο του Android, θα ήταν καλό να αναφερθούν ορισμένα σημαντικά ιστορικά στοιχεία. Κάτι που δε γνωρίζουν πολλοί, είναι το γεγονός ότι η **Android Inc.** στο ξεκίνημά της αποτελούσε μια ανεξάρτητη εταιρεία ανάπτυξης λογισμικού, η οποία ιδρύθηκε στο **Palo Alto της California, USA** από τους **Andy** Rubin, Rich Miner, Nick Sears και Chris White. Σύμφωνα με τα λόγια του Rubin, ο στόχος της εταιρείας ήταν «…**να δημιουργήσει έξυπνες κινητές συσκευές, οι οποίες θα έχουν επίγνωση της θέσης του ιδιοκτήτη καθώς και των επιλογών του…**». Αρχικά η ομάδα του Android λειτουργούσε μυστικά, αλλά η μεγάλη ανάπτυξη στο λειτουργικό ξεκίνησε μετά την εξαγορά του από τη Google το 2005.

Όλα ξεκίνησαν την άνοιξη του 2005, όταν ο ευφυής Andy Rubin θέλησε να χρησιμοποιήσει τη Google ως κατ' εξοχήν μηχανή αναζήτησης για το T-Mobile Sidekick, μια φέρελπιν συσκευή κινητού, την οποία είχε αναπτύξει με την ομάδα συνεργατών του. Για το σκοπό αυτό επεδίωξε να συναντήσει με τον Larry Page, έναν εκ των δύο ιδρυτών της εταιρείας Google. Στη συνάντηση αυτή ο Rubin παρουσίασε το Android ως ένα εν δυνάμει παγκόσμιο ανοικτό λειτουργικό σύστημα που θα άλλαζε για πάντα τον τρόπο που διαδράσης των χρηστών με το κινητό τους, τονίζοντας ταυτόχρονα τη σταθερή υπεροχή που παρατηρείται στις συνήθειες του αγοραστικού κοινού των κινητών τηλεφώνων, σε αντιδιαστολή με τις πωλήσεις ηλεκτρονικών υπολογιστών. Την ίδια στιγμή ο Page δεν ήθελε να γίνει απλά ένας υποστηρικτής του λειτουργικού Android αλλά αποσκοπούσε στο να γίνει ιδιοκτήτης του.

Τον Αύγουστο του 2005, η **Google Inc.** εξαγόρασε την Android καθιστώντας τη θυγατρική της, με βασικά στελέχη της τους Rubin, Miner και White. Επρόκειτο για ένα τολμηρό εγχείρημα, το οποίο αρκετά αργότερα ο αντιπρόεδρος του τμήματος ανάπτυξης της Google, **David Lawee**, αναγνώρισε ως την καλύτερη διαπραγμάτευση που έγινε ποτέ *(''…best deal ever!'', 16th annual Stanford Accel Symposium).*

Την ίδια χρονιά κυκλοφόρησε στην αγορά ένας πανίσχυρος ανταγωνιστής, το γνωστό σε όλους iPhone της Apple. Εν αναμονή της απάντησης της Google στην Apple επιχειρηματικός και τεχνολογικός κόσμος αρχικά υπέθεσε ότι η Google σχεδίαζε θα έβγαζε στη αγορά το αντίπαλο δέος του iPhone, ένα gPhone, εφόσον την περίοδο της εξαγοράς η Android δεν ήταν ιδιαιτέρως γνωστή. Όμως όλες οι εκτιμήσεις και οι υποθέσεις της αγοράς διαψεύστηκαν από την Google οποία την περίοδο εκείνη και μέχρι και το 2007 η Google δούλευε σιωπηλά πάνω στο Android κατοχυρώνοντας πατέντες και ψάχνοντας συνεργάτες.

Στις 5 Νοεμβρίου του 2007 ανακοινώθηκε η δημιουργία της Open Handset Alliance*, ενός συνεταιρισμού που αποτελούνταν από 34 συνολικά εταιρείες με αντικείμενο το hardware, το software και τις τηλεπικοινωνίες (Google, Samsung, Qualcomm, NVidia, Motorola, T-Mobile, KEA) σκοπός του οποίου ήταν η καθιέρωση του Android ως ένα ανοικτό λογισμικό και η κυκλοφορία των πρώτων smartphones με Android. Σήμερα η Open Handset Alliance αριθμεί 84 μέλη που συνεργάζονται για την παρουσίαση καινοτόμων προτάσεων στον τομέα των κινητών και την προσφορά στους καταναλωτές προϊόντων κινητής τηλεφωνίας λιγότερο ακριβά αλλά όχι εις βάρος της ποιότητας και της λειτουργικότητάς τους.

Το πρώτο smartphone με λειτουργικό Android κυκλοφόρησε το 2008, ένα χρόνο μετά την ίδρυση της Open Handset Alliance, από την HTC και ονομαζόταν HTC Dream. Από κει και έπειτα πολλές εταιρείες με πρώτη τη Samsung, την κορυφαία εταιρεία σε πωλήσεις κινητών παγκοσμίως και στην οποία οφείλεται κατά μεγάλο βαθμό η εξάπλωση του Android, δεκάδες εταιρείες υιοθέτησαν το Android ως λειτουργικό και κατάφεραν να το κάνουν κυρίαρχο λειτουργικό αυτή τη στιγμή στην αγορά , όπως φαίνεται και από τα στοιχεία που δίνονται από το International Data Corporation αλλά και από τα δεδομένα που προέκυψαν από έρευνα που διενεργήθηκε το 2012 για λογαριασμό της **mobiThinking** .

Global smartphone operating system share in 2012 and 2016, according to IDC					Global smartphone operating system share in 2012, 2013 and 2016, according to Canalys			

Ορισμός και δομή του Android

Το Android είναι ένα λειτουργικό σύστημα που ενσωματώνεται σε φορητές και μη φορητές συσκευές όπως είναι τα **smartphones**, τα **tablet computers** και **netbooks** .

Πρόκειται για ένα λογισμικό ανοικτού κώδικα (open source) και αποτελεί μία ολοκληρωμένη, ανοιχτή και δωρεάν πλατφόρμα κινητών τηλεφώνων. Οι σχεδιαστές της βασίστηκαν σ' ένα ασφαλές λειτουργικό σύστημα και κατασκεύασαν ένα δυνατό πλαίσιο λογισμικού το οποίο έχει το πλεονέκτημα την ποικίλα ανάπτυξη εφαρμογών.

Η πλατφόρμα Android παρέχεται μέσω της διαδικασίας ανοιχτής πηγής. Ως εκ τούτου η πρόσβαση στα χαρακτηριστικά των συσκευών, όταν οι προγραμματιστές αναπτύσσουν τις εφαρμογές τους, είναι ελεύθερη. Είναι σημαντικό επίσης να αναφερθεί πως το υποκείμενο λειτουργικό σύστημα του Android έχει κατοχυρωθεί με την άδεια δημόσιας χρήσης GNU General Public License Version 2 (GPLv2), μια ισχυρή άδεια που υποχρεώνει τις βελτιώσεις τρίτων να εξακολουθούν να εμπίπτουν στους όρους των προτύπων ανοιχτής πηγής. Δεν καταβάλλεται κανένα χρηματικό ποσό για την ανάπτυξη εφαρμογών Android, για άδειες χρήσης, για πνευματικά δικαιώματα καθώς και για απόκτηση μιας εφαρμογής.

Το **Android SDK** ***(Software Development Kit)*** παρέχει δωρεάν τα απαραίτητα εργαλεία και **APIs** (***Application Programming Interfaces***) για να αναπτυχθούν προγράμματα, χρησιμοποιώντας την γλώσσα προγραμματισμού **Java**. Η ανάπτυξη λογισμικού, που γίνεται με την βοήθεια ενός **plugin** ***(Android Development Tools, ADT)*** της Google που εγκαθίσταται στον **Eclipse**, καθώς και ο **emulator** εκτελούνται τόσο στα Windows όσο και σε Linux. Περισσότερες

λεπτομέρειες σχετικά με την εγκατάσταση των βιβλιοθηκών του Android καθώς και με την ανάπτυξη εφαρμογών θα δούμε σε επόμενο κεφάλαιο.

Πλήθος προγραμματιστών ασχολείται με την ανάπτυξη εφαρμογών σε Android, επεκτείνοντας τη λειτουργικότητα των συσκευών, γράφοντας κώδικα σε μια προσαρμοσμένη έκδοση της Java. Αξίζει να αναφερθεί ότι σήμερα υπάρχουν πάνω από 650.000 εφαρμογές Android διαθέσιμες στους χρήστες μέσω του Android Market, το Online κατάστημα της Google στο οποίο θα γίνει εκτενής αναφορά σε σχετικό κεφάλαιο.

Ενημερώσεις Android

Με την πάροδο του χρόνου η πλατφόρμα του Android έχει εξελιχθεί σε σχέση με την αρχική έκδοση του Σεπτέμβριου του 2008 . Κάθε ενημερωμένη έκδοση αποσκοπεί στο να διορθώσει τυχόν σφάλματα προηγούμενων εκδόσεων του λογισμικού και στην προσθήκη νέων χαρακτηριστικών. Μια ενδιαφέρουσα πληροφορία χωρίς να αφορά το τεχνολογικό κομμάτι αυτό καθεαυτό είναι πως κάθε ενημέρωση του λειτουργικού συστήματος Android αναπτύσσεται κάτω από μία κωδική ονομασία που βασίζεται σε κάποιο όνομα επιδορπίου!

Εν συνεχεία θα παρουσιαστούν με χρονολογική σειρά οι κυριότερες εκδόσεις του Android και τα χαρακτηριστικά τους.

Έκδοση 1.0 (Apple Pie)

Η έκδοση 1.0 κυκλοφόρησε με το πρώτο Android smartphone HTC Dream στις 23 Σεπτεμβρίου 2008.

Τα χαρακτηριστικά της περιελάμβαναν:

- Το Android Market, μέσω το οποίου ήταν δυνατή η λήψη εφαρμογών και ενημερώσεων.
- Περιηγητή διαδικτύου με δυνατότητα ζουμ για την προβολή HTML και XHTML σελίδων
- Την υποστήριξη κάμερας, χωρίς ωστόσο να υπάρχει η δυνατότητα αλλαγής της ανάλυσης από το χρήστη.
- Τη δυνατότητα δημιουργίας και επεξεργασίας φακέλων αρχείων.
- Την υποστήριξη πρωτοκόλλων POP3, IMAP4 και SMTP.
- Τη δυνατότητα συγχρονισμού του λογαριασμού Gmail με την εφαρμογή Gmail.
- Την εφαρμογή **People** για το συγχρονισμό των επαφών Google του χρήστη.
- Την εφαρμογή **Calendar** για το συγχρονισμό του ημερολογίου Google
- Το **Google Sync** για διαχείριση του συγχρονισμού των εφαρμογών Gmail, People και Calendar.

- Η συνεργασία των Google εφαρμογών Google Maps, Latitude και Street View, παρείχε στο χρήστη τη δυνατότητα να εντοπίσει τοπικές επιχειρήσεις και να λάβει οδηγίες κατεύθυνσης με τη βοήθεια του **GPS**.
- Αναζήτηση Google για εφαρμογές τηλεφώνου, επαφές, ημερολόγιο, κτλ.
- Τη δυνατότητα ανταλλαγής άμεσων μηνυμάτων, μέσω του **Google Talk**.
- Αποστολή άμεσων μηνυμάτων, μηνυμάτων κειμένου και MMS.
- Το **Media Player** που επέτρεπε την αναπαραγωγή πολυμέσων.
- Εμφάνιση ειδοποιήσεων *(notifications)* στη γραμμή κατάστασης *(status bar)*.
- Η υπηρεσία φωνητικής κλήσης επέτρεπε την πραγματοποίηση τηλεφωνημάτων χωρίς να προηγηθεί πληκτρολόγηση του ονόματος ή του αριθμού.
- Ο χρήστης μπορούσε να ορίσει μια εικόνα φόντου ή μια φωτογραφία πίσω από την αρχική οθόνη
- Ειδοποιήσεις στη μπάρα κατάστασης.
- Δυνατότητα αναπαραγωγής βίντεο **YouTube**.
- Οι κοινές εφαρμογές συμπεριλάμβαναν ξυπνητήρι, αριθμομηχανή, dialer, gallery φωτογραφιών και ρυθμίσεις.
- Τέλος, υποστηρίζονταν τεχνολογίες **Wi-Fi** και **Bluetooth**

Έκδοση 1.1 (Banana Bread)

Στις 9 Φεβρουαρίου του 2009, κυκλοφόρησε η έκδοση 1.1 για το κινητό T-Mobile G1 και μόνο. Η ενημέρωση επιδιόρθωσε κάποια σφάλματα (bugs), άλλαξε το API και πρόσθεσε ένα σύνολο χαρακτηριστικών.

Αναλυτικότερα προστέθηκαν τα εξής χαρακτηριστικά:

- Λεπτομέρειες και σχόλια στους χάρτες ώστε, κατά τη διάρκεια της αναζήτησης μέσω της εφαρμογής Maps, να είναι δυνατή η προβολή λεπτομερειών που αφορούν επιχειρήσεις και τοποθεσίες.
- Επιμήκυνση του χρόνους απενεργοποίησης της οθόνης κατά τη διάρκεια κλήσεων με χρήση της ανοικτής ακρόασης και δυνατότητα απόκρυψης του πληκτρολογίου κλήσης.
- Υποστήριξη επισυναπτόμενων αρχείων στα μηνύματα.
- Προσθήκη του χαρακτηριστικού marquee στα στοιχεία που απάρτιζαν τη διάταξη της διεπαφής χρήστη.

Έκδοση 1.5 (Cupcake)

Στις 30 Απριλίου του 2009, κυκλοφόρησε η επίσημη ενημέρωση 1.5 για την πλατφόρμα Android. Προστέθηκαν πολλά νέα χαρακτηριστικά και αρκετές αναβαθμίσεις της διεπαφής χρήστη. Στα χαρακτηριστικά αυτής της έκδοσης περιλαμβάνονταν:

- Νέο εικονικό πληκτρολόγιο με δυνατότητα πρόβλεψης κειμένου.
- Υποστήριξη widgets – μικρά πλαίσια εφαρμογών με δυνατότητα ενσωμάτωσής τους σε άλλες εφαρμογές, όπως η Αρχική οθόνη.
- Δυνατότητα αναπαραγωγής βίντεο αρχείων σε MPEG4 και 3GP μορφή.
- Αυτόματη σύζευξη με ακουστικό Bluetooth μέσα σε μια συγκεκριμένη απόσταση.
- Δυνατότητα αντιγραφής και επικόλλησης στον περιηγητή.
- Εμφάνιση φωτογραφίας ή εικόνας για κάθε επαφή.
- Άμεση μετάβαση στα στοιχεία μίας επαφής από το ιστορικό κλήσεων.
- Δυνατότητα περιστροφής της οθόνης.

- Δυνατότητα «ανεβάσματος» βίντεο στο YouTube.
- Δυνατότητα «ανεβάσματος» εικόνας στο Picassa.

Έκδοση 1.6 (Donut)

Στις 15 Σεπτέμβρη 2009 κυκλοφόρησε η επόμενη νέα έκδοση.

Τα χαρακτηριστικά αυτής της νέας έκδοσης περιελάμβαναν:

- Δυνατότητα ολοκληρωμένης διεπαφής κάμερας, βιντεοκάμερας και έκθεσης φωτογραφιών και βίντεο.
- Μαζική διαγραφή φωτογραφιών.
- Βελτιωμένη αναζήτηση και δυνατότητα προβολής στιγμιότυπων των εφαρμογών στο Android Market.
- Καλύτερη αναζήτηση ιστορικού, επαφών, αγαπημένων και στο διαδίκτυο μέσω της αρχικής οθόνης.
- Βελτιωμένη τεχνολογία υποστήριξης CDMA/EVDO, 802.1x, VPNs και προσθήκη μίας text-to-speech μηχανής.
- Αναβαθμισμένη φωνητική αναζήτηση, με μικρότερο χρόνο απόκρισης και καλύτερη συνεργασία με τις ενσωματωμένες εφαρμογές της συσκευής, συμπεριλαμβανομένης και της φωνητικής κλήσης των επαφών.
- Υποστήριξη για ανάλυση οθόνης WVGA.
- Μεγαλύτερη ταχύτητα στις εφαρμογές αναζήτησης και κάμερας.
- Νέο πλαίσιο εφαρμογών Gesture και νέο εργαλείο ανάπτυξης GestureBuilder.

Έκδοση 2.0/2.1 (Éclair)

Στις 26 Οκτωβρίου του 2009, έγινε διαθέσιμη η ενημέρωση 2.0 Μεταξύ των αλλαγών που πραγματοποιήθηκαν περιλαμβάνονταν:

- Μεγαλύτερη ταχύτητα του υλικού.

- Αναζήτηση όλων των αποθηκευμένων μηνυμάτων *(SMS, MMS)*. Αυτόματη διαγραφή παλαιότερων μηνυμάτων μιας συνομιλίας, όταν αυτά ξεπερνούσαν ένα προκαθορισμένο όριο.
- Υποστήριξη περισσότερων αναλύσεων και μεγεθών της οθόνης.
- Ανανεωμένο γραφικό περιβάλλον.
- Νέο γραφικό περιβάλλον του περιηγητή διαδικτύου και υποστήριξη HTML5.
- Νέα λίστα επαφών.
- Καλύτερη αναλογία λευκού-μαύρου στο περιθώριο.
- Βελτιωμένη εφαρμογή Google Maps 3.1.2.
- Υποστήριξη του Microsoft Exchange.
- Ενσωματωμένη υποστήριξη flash για την κάμερα.
- Δυνατότητα επιλογής μιας φωτογραφίας επαφής
- Δυνατότητα αποστολής email, SMS και τηλεφωνικής κλήσης.
- Όσον αφορούσε την κάμερα, με την έκδοση Éclair πλέον υπήρχε υποστήριξη flash, ψηφιακό zoom, λειτουργία σκηνής, ισορροπία λευκού, εφέ χρωμάτων, macro εστίαση.
- Εξυπνότερο λεξικό που μάθαινε από την χρήση των λέξεων και περιελάμβανε τα ονόματα των επαφών.
- Κλάση MotionEvent για την αναγνώριση multi-touch ενεργειών.
- Βελτιωμένο και ταχύτερο εικονικό πληκτρολόγιο.
- Υποστήριξη Bluetooth 2.1.
- Οι εικόνες φόντου και αρχικής οθόνης μπορούσαν πλέον να είναι κινούμενες.

Έκδοση 2.2.x (Froyo)

Στις 20 Μαΐου 2010 εκδόθηκε η ενημέρωση 2.2 η οποία περιλάμβανε τις εξής αλλαγές:

- Βελτιώσεις στην ταχύτητα του λειτουργικού, στη μνήμη και γενικά στην απόδοση του συστήματος.
- Επιπρόσθετες βελτιστοποιήσεις στην ταχύτητα των εφαρμογών εξαιτίας της υλοποίησης του JIT (Just In Time compilation).

- Ενσωμάτωση της V8 JavaScript μηχανής του Chrome στην εφαρμογή του περιηγητή διαδικτύου.
- Καλύτερη υποστήριξη του Microsoft Exchange.
- Βελτιωμένη εκκίνηση των εφαρμογών με συντομεύσεις για τις εφαρμογές του περιηγητή διαδικτύου και του τηλεφώνου.
- Υποστήριξη USB.
- Προσθήκη επιλογής για την απενεργοποίηση της πρόσβασης σε δεδομένα πάνω σε ένα κινητό δίκτυο.
- Αναβαθμισμένη Market εφαρμογή με ομαδική και αυτόματη ανανέωση εφαρμογών.
- Γρήγορη εναλλαγή μεταξύ πολλών γλωσσών πληκτρολογίου και των λεξικών τους.
- Φωνητική κλήση και διαμοίραση αρχείων μέσω Bluetooth.
- Υποστήριξη αριθμητικών και αλφαριθμητικών κωδικών.
- Υποστήριξη πεδίου για ανέβασμα αρχείων στην εφαρμογή του περιηγητή διαδικτύου.
- Δυνατότητα αναπαραγωγής GIFs αρχείων από τον περιηγητή διαδικτύου.
- Δυνατότητα εγκατάστασης εφαρμογών στην επεκτάσιμη μνήμη.
- Υποστήριξη Adobe Flash 10.1.

Έκδοση 2.3 (Gingerbread)

Η εν λόγω έκδοση κυκλοφόρησε στις 6 Δεκεμβρίου 2010 με το Linux kernel 2.6.35. Συνοπτικά, τα νέα χαρακτηριστικά της ήταν τα ακόλουθα:

- Ενημερωμένη διεπαφή χρήστη – μηχανής για απλότητα και ταχύτητα.
- Υποστήριξη πολύ μεγάλων μεγεθών οθόνης καθώς και αναλύσεων *(**WXGA** και άνω)*
- Υποστήριξη για **VoIP** τηλεφωνία.
- Αναφορικά με το εικονικό πληκτρολόγιο, υπήρξε εξέλιξη που ενέπιπτε στην γρηγορότερη και εξυπνότερη εισαγωγή κειμένου, με βελτιωμένη ακρίβεια.

- Βελτιστοποιημένη η λειτουργία της αντιγραφής – επικόλλησης. Δυνατότητα επιλογής της επιθυμητής λέξης με απλό **press-hold**.
- Το **άμεσο πεδίο επικοινωνίας *(Near Field Communication, NFC)*** επέτρεπε στο χρήστη να διαβάσει μια NFC ετικέτα ενσωματωμένη σε μια αφίσα, σε ένα αυτοκόλλητο ή μια διαφήμιση.
- Νέα εφέ ήχου, όπως είναι η αντήχηση, η εξίσωση, κτλ.
- Ο νέος οδηγός λήψεων *(Download Manager)* παρείχε στους χρήστες εύκολη πρόσβαση σε οποιοδήποτε ληφθέν αρχείο.
- Δυνατότητα πρόσβασης σε πολλαπλές κάμερες της συσκευής, συμπεριλαμβανομένης και αυτής που βρίσκεται στο μπροστινό μέρος του κινητού *(εφόσον υπήρχε)*.
- Υποστήριξη αναπαραγωγής βίντεο για επεκτάσεις **WebM/VP8** και **AAC** κωδικοποίηση ήχου.
- Βελτιωμένη διαχείριση ενέργειας με έναν πιο ενεργό ρόλο στη διαχείριση των εφαρμογών που διατηρούσαν τη συσκευή σε έντονη λειτουργία για πάρα πολύ ώρα.
- Ενισχυμένη υποστήριξη για ανάπτυξη κώδικα.
- Μεταπήδηση του συστήματος αρχείων από **YAFFS** σε **ext4** στις νεώτερες συσκευές.
- Βελτιώσεις σε ήχο και γραφικά, γεγονός που βοηθούσε σημαντικά τους προγραμματιστές παιχνιδιών.
- Δυνατότητα συλλογής «απορριμμάτων» για αύξηση της απόδοσης.
- Υποστήριξη περισσότερων αισθητήρων (*sensors)*, όπως τα γυροσκόπια και τα βαρόμετρα.

Έκδοση 3.x (Honeycomb)

Στις 22 Φεβρουαρίου του 2011, κυκλοφόρησε η ενημέρωση 3.0 η οποία ήταν η πρώτη έκδοση που απευθυνόταν αποκλειστικά σε tablet φορητές συσκευές. Η πρώτη συσκευή που είχε την έκδοση 3.0 ήταν το tablet Motorola Xoom. Οι αλλαγές που πραγματοποιήθηκαν ήταν οι εξής:

- Σχεδιασμός του γραφικού περιβάλλοντος έτσι ώστε να είναι βέλτιστο για tablet συσκευές.
- Προσθήκη Action Bar, για πρόσβαση σε επιλογές περιεχομένου, πλοήγησης, widgets, κ.α. στο πάνω μέρος της οθόνης.
- Προσθήκη System Bar, για γρήγορη πρόσβαση σε ειδοποιήσεις και εικονικά κουμπιά πλοήγησης στο κάτω μέρος της οθόνης.
- Απλουστευμένο σύστημα διαχείρισης πολλών διεργασιών.
- Επανασχεδιασμένο πληκτρολόγιο, για γρήγορη, αποτελεσματική και ακριβή πληκτρολόγηση σε μεγάλες οθόνες.
- Επανασχεδιασμένη και πιο απλή διεπαφή για αντιγραφή/επικόλληση.
- Υποστήριξη πολλαπλών καρτελών στον περιηγητή διαδικτύου που αντικαθιστά τα πολλά παράθυρα.
- Άμεση πρόσβαση στην κάμερα και στις δυνατότητες που αυτή είχε να προσφέρει (φλας, ζουμ, κλπ).
- Δυνατότητα προβολής άλμπουμ και φωτογραφιών σε πλήρη οθόνη.
- Νέες διεπαφές για την καλύτερη οργάνωση των επαφών και των e-mails του χρήστη.
- Υποστήριξη βίντεο συνομιλίας μέσω Google Talk.
- Επιτάχυνση υλικού (hardware acceleration).
- Υποστήριξη πολυπύρηνων επεξεργαστών.
- Δυνατότητα κρυπτογράφησης των δεδομένων.

Έκδοση 4.0.x (Ice Cream Sandwich)

Η πρώτη έκδοσή της, 4.0.1, κυκλοφόρησε στις 19 Οκτώβρη του 2011 και απαριθμούσε αρκετά νέα χαρακτηριστικά:

- Εικονικά κουμπιά στο γραφικό περιβάλλον που αντικαθιστούσαν τα πραγματικά κουμπιά.
- Διαχωρισμός των widgets σε νέα καρτέλα.
- Εύκολη δημιουργία φακέλων μέσω drag-and-drop μηχανισμού.
- Δυνατότητα πιο γρήγορης ή πιο αργής αναπαραγωγής των μηνυμάτων του τηλεφωνητή.
- Ενσωματωμένη λήψη screenshots.
- Βελτιωμένη λειτουργία διόρθωσης σφαλμάτων στην πληκτρολόγηση.
- Πρόσβαση στις εφαρμογές ακόμα και με κλειδωμένη οθόνη.
- Βελτιωμένη λειτουργία αντιγραφής/επικόλλησης.
- Υποστήριξη φωνητικής υπαγόρευσης σε πραγματικό χρόνο.
- Δυνατότητα ξεκλειδώματος της συσκευής μέσω λογισμικού αναγνώρισης προσώπου.
- Νέος περιηγητής διαδικτύου με δυνατότητα υποστήριξης μέχρι και 16 καρτελών.
- Νέα βελτιωμένη εφαρμογή χειρισμού της κάμερας με δυνατότητα ζουμ ενώ πραγματοποιεί εγγραφή.
- Δυνατότητα επεξεργασίας εικόνων.
- Υποστήριξη WebP αρχείων εικόνας.
- Επιτάχυνση υλικού στη διεπαφή χρήστη.
- Δυνατότητα εγγραφής βίντεο σε 1080p.

Έκδοση 4.1(Jelly Bean)

Στις 9 Ιουλίου 2012 κυκλοφόρησε η ενημέρωση 4.1, η οποία έφερε πολλά και ενδιαφέροντα στοιχεία. Η πρώτη συσκευή που είχε το Jelly Bean ήταν το tablet Google Nexus 7. Παρακάτω παρουσιάζονται κάποια από τα νέα χαρακτηριστικά της έκδοσης αυτής:

- ενισχυμένη προσιτότητα, η οποία εστιάζει το πού τοποθετεί ο χρήστης το χέρι του καθώς εκτελεί εντολές στην οθόνη αφής.
- App widgets με ικανότητα αλλαγής μεγέθους

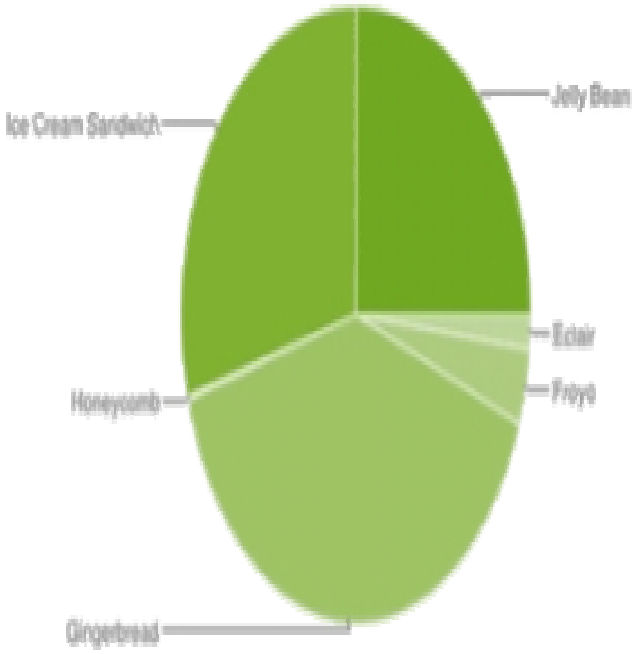
- Νέες μορφές απεικόνισης
- Προεπισκόπηση Live wallpaper
- Φωτογραφίες επαφών υψηλότερης ανάλυσης
- Γρήγορη εύρεση συσκευών που προστίθονταν ή αφαιρούνταν
- Εντοπισμός των δυνατοτήτων της κάθε συσκευής
- Χρήση δόνησης για τις συσκευές εισόδου
- Νέα κινούμενα εικονίδια και νέοι τρόποι μετάβασης
- Υπηρεσία εύρεσης υπηρεσιών Wifi-Direct
- Διαχείριση εύρους δικτύου
- Πρόσβαση σε Media codecs
- Έξοδος USB Audio
- Έναρξη ηχογράφησης Audio
- Πολυκάναλος ήχος και υποστήριξη κωδικοποίησης/αποκωδικοποίησης ήχου AAC 5.1
- Προεπεξεργασία ήχου
- Συνεχής Αναπαραγωγή χωρίς παύσεις
- Media Router
- Καλύτερη εμπειρία HTML5 video, με touch-to-play/pause και ομαλή μετάβαση σε full screen mode.
- Μεγαλύτερες ταχύτητες rendering και μειωμένη χρήση μνήμης
- Καλύτερη απόδοση στο HTML5/CSS3/Canvas animation
- Βελτιωμένη εισαγωγή κειμένου
- Google Play services, όπως η πιστοποίηση και η ενσωμάτωση του Google+ στις εφαρμογές
- Ανανεωμένη JavaScript Engine
- Υποστήριξη HTML5 Media Capture
- Google Cloud Messaging for Android
- Κρυπτογράφηση εφαρμογών
- Έξυπνα App Updates

Μερίδιο αγοράς

Η ενότητα ολοκληρώνεται με ένα γράφημα, το οποίο δημοσιεύτηκε από τη Google τον Απρίλιο του 2013, που απεικονίζει το μερίδιο που καταλαμβάνει στην αγορά η κάθε έκδοση Android. Όπως προκύπτει από τα στοιχεία της έρευνας ξ εκδόσεις με τις ψηλότερα ποσοστά πωλήσεων είναι Gingerbread με ποσοστά που προσεγγίζουν το 40%, ακολουθούν οι εκδόσεις Ice Cream Sandwich και Jelly Bean με ποσοστά 29,3% και 23% αντίστοιχα και τέλος οι κατά πολύ παλαιότερες εκδόσεις Froyo, Eclair και Donut φαίνονται να αγγίζουν συνολικά το 10%

Version	Codename	API	Distribution
1.6	Donut	4	0.1%
2.1	Eclair	7	1.7%
2.2	Froyo	8	4.0%
2.3-2.3.2	Gingerbread	9	0.1%
2.3.3-2.3.7		10	39.7%
3.2	Honeycomb	13	0.2%
4.0.3-4.0.4	Ice Cream Sandwich	15	29.3%
4.1.x	Jelly Bean	16	23.0%
4.2.x		17	2.0%

Data collected during a 14-day period ending on April 2, 2013.
Any versions with less than 0.1% distribution are not shown.



Πηγή γραφήματος: http://www.macobserver.com/tmo/cool_stuff_found/post/thinking-differently-about-android-numbers

To Android Market

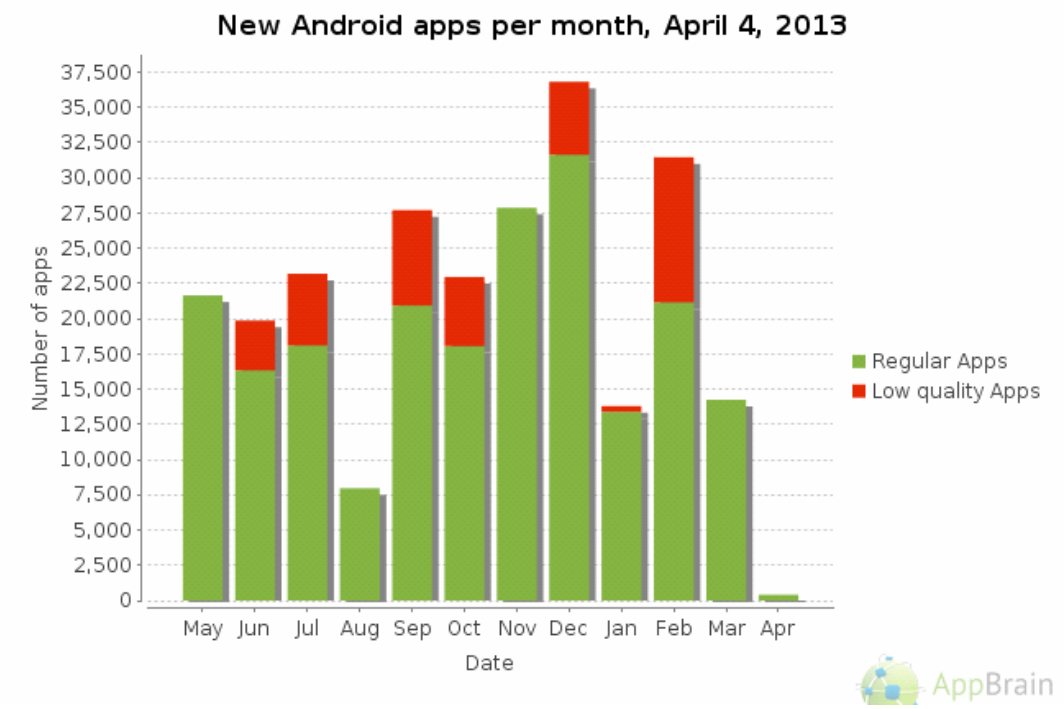
Το Android Market είναι ένα ηλεκτρονικό κατάστημα λογισμικού που αναπτύχθηκε από την Google και απευθύνεται σε συσκευές που διαθέτουν Android λειτουργικό. Στις περισσότερες συσκευές υπάρχει εγκατεστημένη η εφαρμογή Market, η οποία επιτρέπει στους χρήστες να περιηγηθούν και να κατεβάσουν βιβλία, ταινίες, μουσική και εφαρμογές που δημοσιεύονται από τους προγραμματιστές.

Η επίσημη ανακοίνωση εμφάνισης του Market έγινε στις 28 Αυγούστου 2008 από την Google και η διαθεσιμότητα προς τους χρήστες ξεκίνησε στις 22 Οκτώβρη του 2008. Στη συνέχεια, παρατίθενται ορισμένοι πίνακες με κάποια σημαντικά

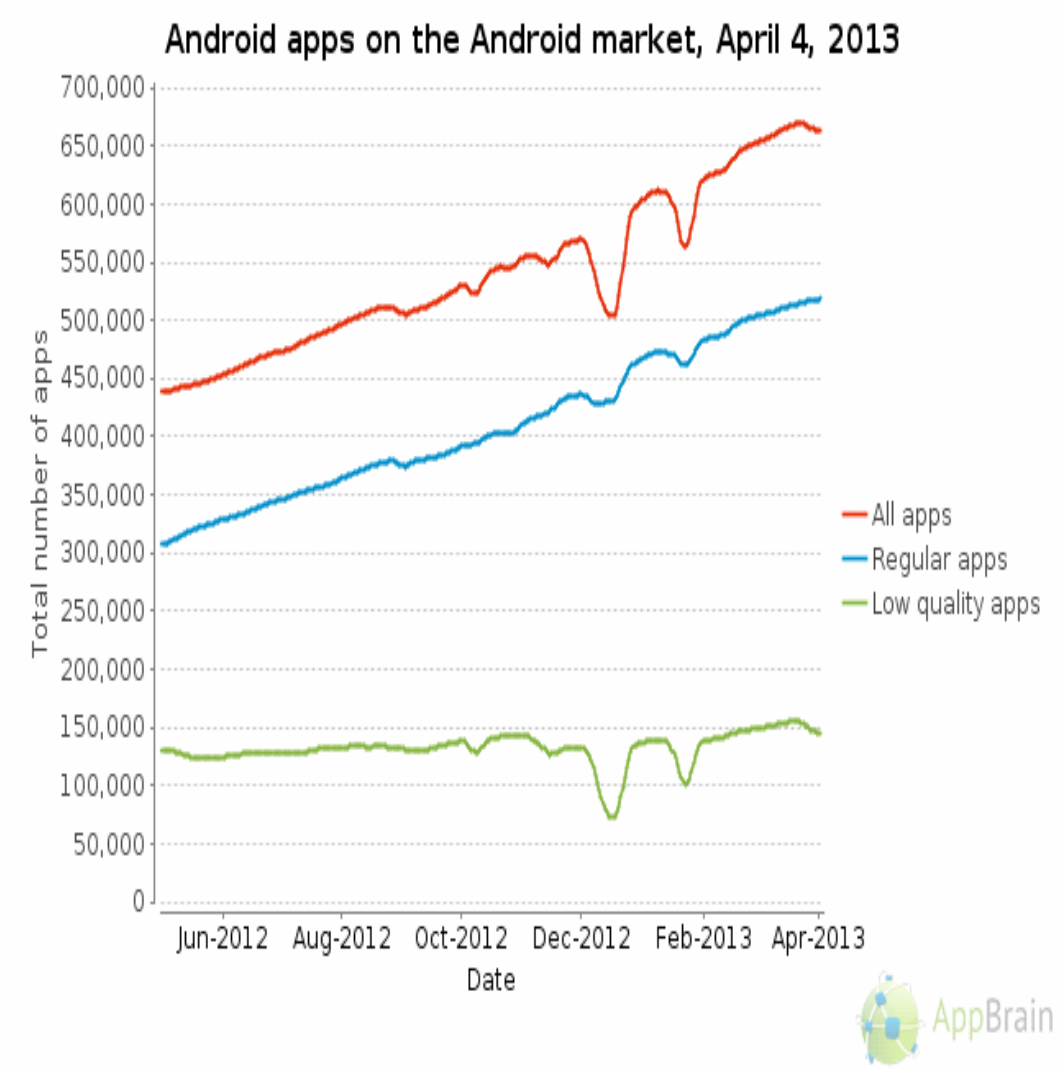
στοιχεία γύρω από τον όγκο των εφαρμογών που παρέχονται από το Market, την ποιότητα αλλά και το ποσοστό των δωρεάν διαθέσιμων εφαρμογών στα γνωστότερα marketplaces.

Current number of free apps in the market: **524055**
Current number of paid apps in the market: **143939**

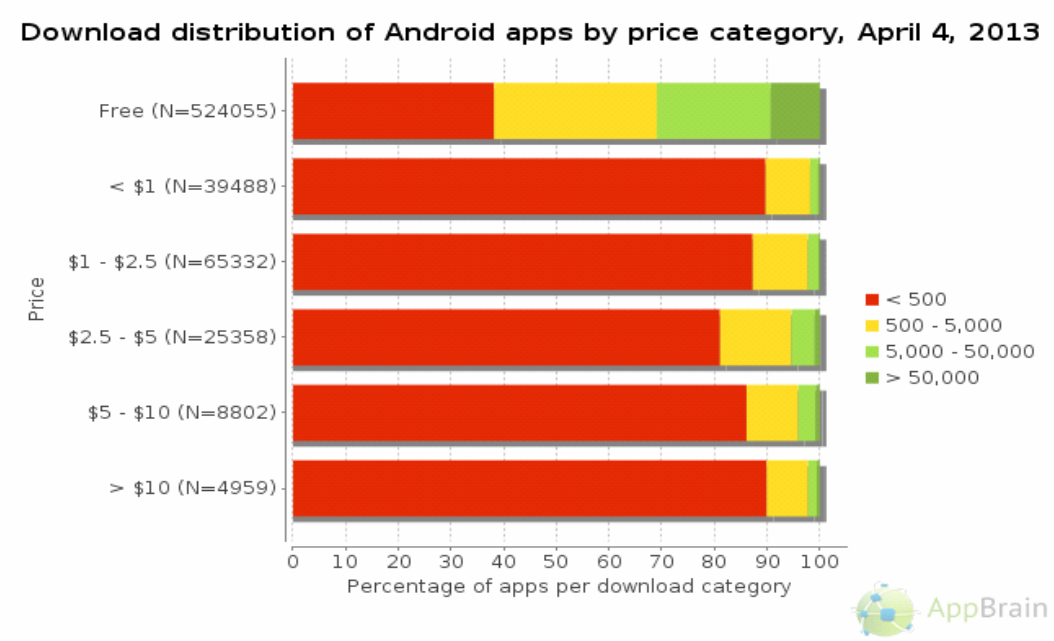
Στο παρακάτω γράφημα, που φτιάχτηκε με την online εφαρμογή της Google – Appbrain, παρουσιάζεται ο αριθμός των νέων, των κανονικών και των χαμηλής ποιότητας εφαρμογών που προστίθενται στο Android Market το μήνα!



Το επόμενο γράφημα αφορά τον αριθμό των διαθέσιμων εφαρμογών στο Android Market με τελευταία ενημέρωση στις 4 Απριλίου 2013.Το AppBrain low quality app (εφαρμογή που αναγνωρίζει τις εφαρμογές χαμηλής ποιότητας), ανιχνεύει αυτόματα τις εφαρμογές που δεν έχουν καμιά χρησιμότητα. Το Google καταργεί εφαρμογές περίπου κάθε 15 λεπτά, οπότε ο συνολικός αριθμός των διαθέσιμων Android apps μειώνεται. Οι εφαρμογές που καταργήθηκαν κατηγοριοποιούνται ως συνήθως από το σύστημα ως εφαρμογές χαμηλής ποιότητας (low quality apps).



Τέλος, το γράφημα που ακολουθεί απεικονίζει τις προτιμήσεις των χρηστών σε εφαρμογές με κριτήριο την τιμή τους.



Το Android Market φιλτράρει την λίστα των αιτήσεων για εφαρμογές με σκοπό να υπάρχει συμβατότητα με την συσκευή που διαθέτει ο χρήστης. Επιπλέον περιορισμοί εισάγονται στην περίπτωση που οι ίδιοι οι προγραμματιστές έχουν συνδέσει τις εφαρμογές τους με συγκεκριμένους φορείς ή χώρες για επαγγελματικούς λόγους. Από τον Μάιο του 2011, οι χρήστες σε 131 χώρες του κόσμου μπορούν να αγοράσουν τις εφαρμογές που εισάγονται στο Marketplace του Android. Ωστόσο, οι εφαρμογές Android δεν είναι απαραίτητο να προέρχονται αποκλειστικά από το Marketplace. Αντιθέτως, οι χρήστες έχουν την δυνατότητα να κατεβάσουν εφαρμογές και από τις ιστοσελίδες των δημιουργών τους.

Όσον αφορά την εφαρμογή του Android Market, πρέπει να τονιστεί ότι δεν είναι **open source**. Μόνο οι Android συσκευές που ικανοποιούν τα κριτήρια συμβατότητας της Google μπορούν να έχουν δυνατότητα πρόσβασης στον κλειστό κώδικα του Android Market app.

Ολοκληρώνοντας, δεν πρέπει να παραλειφθεί να αναφερθεί πως προγραμματιστές 29 χωρών μπορούν να πωλούν τις εφαρμογές τους στο Market. Από την τιμή της εφαρμογής, οι προγραμματιστές λαμβάνουν το 70%, ενώ το υπόλοιπο 30% κατανέμεται μεταξύ των μεσολαβητών πληρωμής. Η Google δεν παίρνει καθόλου μερίδιο από της πληρωμές και τα έσοδα διανέμονται στους προγραμματιστές μέσω του **Google Checkout**.

Κακόβουλο λογισμικό και ασφάλεια

Σύμφωνα με την έρευνα: «Why Eve and Mallory Love Android: Analysis of Android SSL (In)Security» η οποία διεξήχθη το έτος 2012 από το Leibniz University of Hannover και το Philipps University of Marburg, πολύ γνωστές εφαρμογές για το Android, οι οποίες διατίθενται από το επίσημο κατάστημα Google Play, δεν προστατεύουν αποτελεσματικά από τους εγκληματίες του κυβερνοχώρου ευαίσθητα δεδομένα των χρηστών τους, όπως τους κωδικούς online banking ή τα στοιχεία πρόσβασης σε υπηρεσίες e-mail.

Οι ερευνητές εξέτασαν τις 13.500 δημοφιλέστερες εφαρμογές από το Google Play, διαπιστώνοντας ότι 41 από αυτές παρουσίαζαν «κερκόπορτες», οι οποίες μπορούν να αξιοποιηθούν για την κλοπή προσωπικών πληροφοριών. «Σκηνοθετώντας» ένα δίκτυο Wi-Fi και χρησιμοποιώντας ένα ψηφιακό εργαλείο υποκλοπών, κατάφεραν σε αυτές τις 41 περιπτώσεις να παρεμβληθούν μεταξύ της «έξυπνης» συσκευής και των αντίστοιχων ιστοσελίδων με τα οποία επικοινωνούσαν οι application.

Με αυτό τον τρόπο, σύμφωνα με την ανακοίνωσή τους, μπόρεσαν να κλέψουν κωδικούς πρόσβασης σε κοινωνικά δίκτυα, συνθηματικά από online τραπεζικές υπηρεσίες και λογαριασμούς e-mail. Ακόμη χειρότερα, κατάφεραν να «ξεγελάσουν» ή να απενεργοποιήσουν τα προγράμματα antivirus που βρίσκονταν στις συσκευές, για

να εγκαταστήσουν κακόβουλο λογισμικό που τους επέτρεπε να αλλάζουν τη λειτουργία των προγραμμάτων κατά το δοκούν.

Όπως ανέφεραν χαρακτηριστικά στο άρθρο τους, «Μπορούσαμε να συγκεντρώσουμε πληροφορίες για τραπεζικούς λογαριασμούς, διαπιστευτήρια PayPal, American Express και άλλα [..] Πετύχαμε να καταγράψουμε συνθηματικά για τις online υπηρεσίες American Express, Diners Club, Paypal, Facebook, Twitter, Google, Yahoo, Microsoft Live ID, Box, WordPress. Επίσης, μπορέσαμε να παρέμβουμε στη διαδικασία αυτόματης ενημέρωσης των antivirus, ώστε να απενεργοποιήσουμε τα antivirus ή να αφαιρέσουμε εφαρμογές από τις συσκευές, ακόμη και το ίδιο το antivirus».

Οι ερευνητές δεν προέβησαν στην αποκάλυψη της ταυτότητας των 41 μη ασφαλών εφαρμογών για το Android που είναι ευάλωτες, ανέφεραν όμως πως δύο απ' αυτές τις εφαρμογές που εντόπισαν ως κακόβουλες έχουν κατεβαστεί από 39,5 και 185 εκατομμύρια χρήστες. Ο αριθμός των ευάλωτων εφαρμογών μάλιστα μπορεί στην πραγματικότητα να είναι μεγαλύτερος. Από τις 13.500 δωρεάν εφαρμογές που ερευνήθηκαν, συνολικά οι 1.074, το 8% δηλαδή, βρέθηκαν να είναι δυνητικά ευπαθείς σε exploits.

Τα ευρήματα αυτά δείχνουν τον αρκετά εύθραυστο χαρακτήρα των πρωτοκόλλων SSL και TLS, ο συνδυασμός των οποίων αποτελεί τη βάση για την κρυπτογράφηση της συντριπτικής πλειοψηφίας των ιστοσελίδων.

Όλη αυτή η κατάσταση μπορεί να αποδοθεί στο γεγονός ότι η πλατφόρμα Android γίνεται νούμερο ένα στόχος των malwares λόγω της υψηλής δημοτικότητας της. Για τους λόγους αυτούς η **Google** πέρα από τις εφαρμογές antivirus που παρέχονται στο market δημιουργημένες από εταιρείες ειδικούς στον τομέα της ασφάλειας (Avast, Lookout, AV-Test) αποφάσισε να προσθέσει μια ακόμη **δικλείδα ασφαλείας στο λειτουργικό της**. Έχει την **κωδική ονομασία Bouncer (πορτιέρης)** και στόχος του είναι να ελέγχει τόσο τις νέες όσο και τις ήδη υπάρχουσες εφαρμογές για γραμμές κακόβουλου κώδικα. Μόλις εντοπίσει κάτι επικίνδυνο, ενημερώνει το χρήστη ώστε να να την αφαιρέσει προστατεύοντας με τον τρόπο αυτό τη συσκευή του.

Ιδιωτικό απόρρητο

Προτού ολοκληρωθεί αυτό το κεφάλαιο αξίζει να γίνει αναφορά σε κάποια ζητήματα που αφορούν την προστασία των προσωπικών δεδομένων των χρηστών. Οι κινητές συσκευές περιέχουν περισσότερες προσωπικές πληροφορίες από τα περισσότερα προσωπικά ημερολόγια. Αλλά ιδιοκτησιακά συστήματα, ακόμη και τα περισσότερα κινητά Android, σχεδιάστηκαν για να αφήνουν τα δεδομένα αυτά στο έλεγχο εταιριών όπως η Google και η Apple. Οι περισσότεροι χρήστες δεν έχουν πλήρη έλεγχο των προσωπικών δεδομένων στη συσκευή τους. Βολικές λύσεις για συγχρονισμό και εφεδρικά αντίγραφα δεδομένων είναι το τέχνασμα για όλο και περισσότερους ανθρώπους να αποθηκεύουν όλα τα δεδομένα τους σε κεντρικούς εξυπηρετητές, η διαχείριση των οποίων ανήκει σε ορισμένους εμπορικούς οργανισμούς. Οι πολυεθνικές αυτές έχουν συνήθως την έδρα τους στις Ηνωμένες Πολιτείες και απαιτούν από το χρήστη να παραδώσει τα δεδομένα του στην κυβέρνηση των Ηνωμένων Πολιτειών υποβάλλοντας σχετικό αίτημα. Οποιοσδήποτε διαθέτει τα προσωπικά δεδομένα κάποιου, μπορεί να τον ελέγχει. Άρα μη-ελεύθερες συσκευές είναι απειλή για τη δημοκρατία και τη σύγχρονη κοινωνία.

Η ιδιωτικότητα και η προστασία της είναι ένας από τους σημαντικότερους λόγους για να υποστηρίξει κάποιος το Ελεύθερο Λογισμικό. Ιδιοκτησιακά πρόσθετα όπως το Carrier IQ κατασκοπεύουν τους χρήστες των έξυπνων κινητών χωρίς εκείνοι να το γνωρίζουν. Πολλές εφαρμογές από την αγορά περιέχουν κακόβουλα χαρακτηριστικά. Διαβάζουν τα προσωπικά σας δεδομένα, όπως το βιβλίο διευθύνσεων και την «αρχική σελίδα», ή χρησιμοποιούν τα Google Analytics για την αποστολή δεδομένων στη Google. Αυτά είναι μικρά παραδείγματα που έχουν ανακαλυφθεί μέχρι τώρα. Η απουσία ελευθερίας εμποδίζει την ανεξάρτητη έρευνα και οι μυστικές λειτουργίες κατασκοπείας γίνονται μόνο γνωστές τυχαία.

Τα περισσότερα έξυπνα κινητά ζητούν από τους χρήστες να συνδεθούν και να ταυτοποιηθούν σε έναν κεντρικό εξυπηρετητή πριν την πρώτη χρήση της συσκευής τους. Οι χρήστες πρέπει να εμπιστευτούν τον εξυπηρετητή χωρίς να γνωρίζουν τι πληροφορίες έχουν αποθηκευθεί και πώς γίνονται αντικείμενο επεξεργασίας ή πώς συσχετίζονται με άλλα δεδομένα. Τα Android smartphones έχουν τη δυνατότητα να

αναφέρουν τη θέση του Wi-Fi access point με το οποίο συνδέονται. Έτσι, οι συνεχώς μετακινούμενοι χρήστες συνεισφέρουν στη δημιουργία τεράστιων βάσεων δεδομένων, οι οποίες περιέχουν φυσικούς χώρους όπου υπάρχουν εκατοντάδες access points. Οι εν λόγω βάσεις δεδομένων καταρτίζουν ηλεκτρονικούς χάρτες για τον εντοπισμό των smartphones, οι οποίοι επιτρέπουν σε εφαρμογές αλλά και ολόκληρες εταιρείες να διανέμουν αγγελίες και διαφημίσεις βασισμένες στην τοποθεσία του χρήστη.

Το ζήτημα είναι πως η πλειοψηφία των χρηστών δεν έχει τη δυνατότητα να παρακολουθεί τον τρόπο με τον οποίο οι εν λόγω εφαρμογές αποκτούν πρόσβαση σε ευαίσθητα δεδομένα, όπως είναι π.χ. η θέση και το ID του hardware.Η ανάγκη προσδιορισμού του τρόπου φιλτραρίσματος αυτών των πληροφοριών, οδήγησε στη δημιουργία λογισμικού παρακολούθησης των εφαρμογών από τρίτους, όπως είναι το **TaintDroid**, ένα project μεταξύ των **Intel Penn State University** και **Duke University**. Ωστόσο, οι χρήστες μπορούν επίσης να ενημερωθούν για τη συμπεριφορά μιας εφαρμογής μέσω της σύμβασης άδειας που εμφανίζεται συνήθως κατά την εγκατάσταση, αλλά έχει παρατηρηθεί ότι η πλειοψηφία των χρηστών δεν διαβάζουν ή δεν κατανοούν το ψιλά γράμματα νομικού περιεχομένου στις συμφωνίες αδειών και συχνά προχωρά χωρίς να γνωρίζει. Ενίοτε ακόμη και κατά την εγκατάσταση οι έλεγχοι αδειών συχνά δεν υποδεικνύουν στο χρήστη το γεγονός ότι διάφορα δεδομένα ενδέχεται να χρησιμοποιηθούν ακόμα και με καταχρηστικό τρόπο

Ως απάντηση στα θέματα διαρροής ευαίσθητων προσωπικών δεδομένων , το 2012 το Ευρωπαϊκό Ίδρυμα Ελεύθερου Λογισμικού (Free Software Foundation Europe - FSFE) ξεκίνησε τη δράση «Ελευθερώστε το Android σας!». Ο Torsten Grote, μέλος του FSFE και εμπνευστής της δράσης έκανε την ακόλουθη δήλωση:
«Στους χρήστες αξίζει να έχουν πλήρη έλεγχο στις κινητές συσκευές τους. Αν το τηλέφωνό σας δουλεύει με Ελεύθερο Λογισμικό, εσείς είστε το αφεντικό. Αν εκτελεί ιδιοκτησιακό λογισμικό, παραδίδετε τον έλεγχο της ψηφιακής σας ζωής σε κατασκευαστές και προγραμματιστές εφαρμογών».

Η δράση «Ελευθερώστε το Android σας!» διαφημίζει εκδόσεις Android που έχουν βελτιστοποιηθεί για να έχει ο χρήστης τον έλεγχο και μια εναλλακτική αγορά που παρέχει αποκλειστικά εφαρμογές ελεύθερες όπως στην ελευθερία. Επίσης απευθύνει πρόσκληση για συμμετοχή σε διάφορες πρωτοβουλίες και για την

αναγνώριση βασικών εφαρμογών οι οποίες δεν έχουν ακόμη ελεύθερες εναλλακτικές λύσεις.

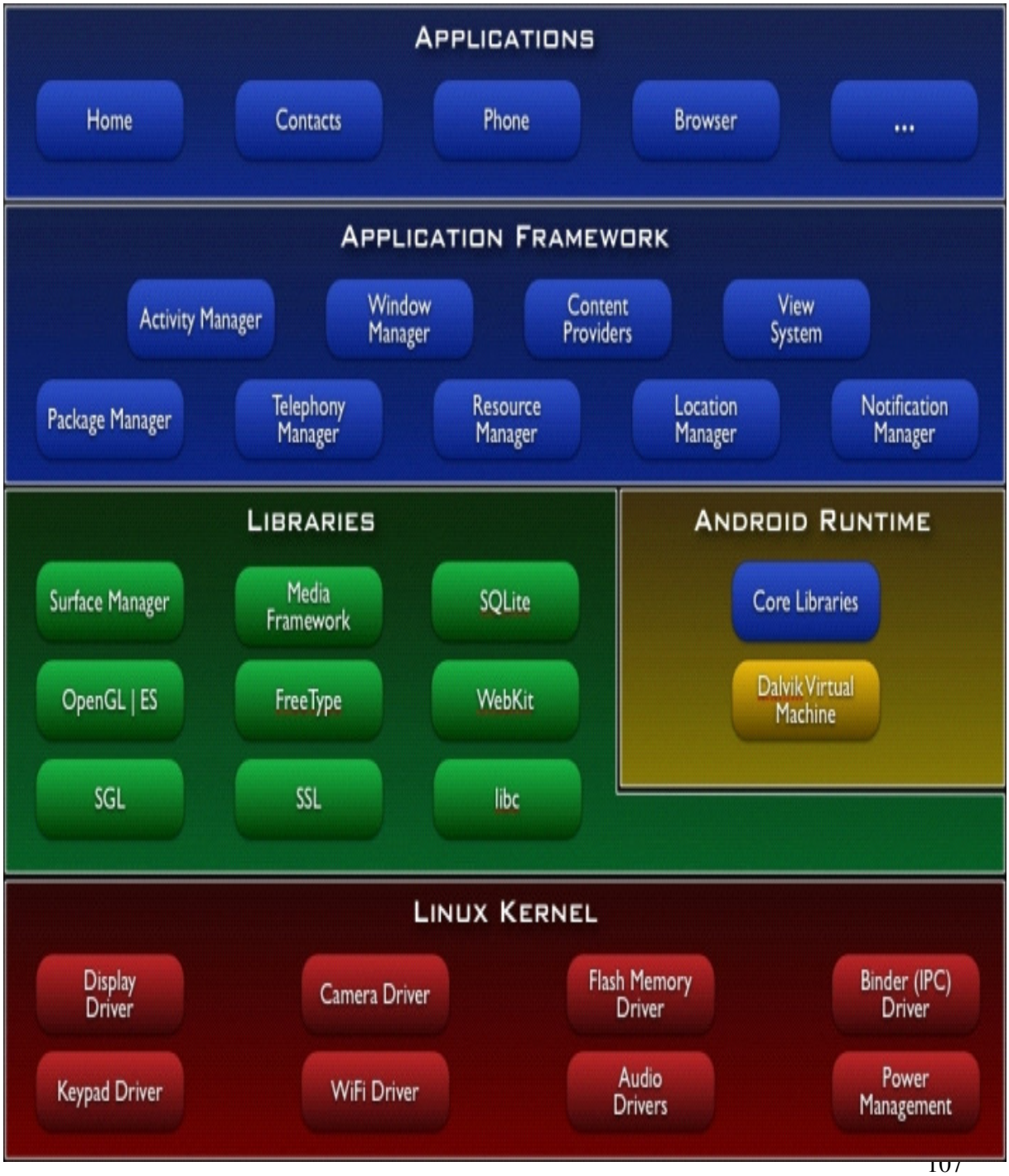
«Το λειτουργικό σύστημα Android μπορεί να είναι κατά κύριο λόγο ελεύθερο, αλλά πολλές εφαρμογές δεν είναι», δηλώσε ο Karsten Gerloff, Πρόεδρος του FSFE. «Οι κινητές συσκευές περιέχουν πολλά στοιχεία για τη ζωή μας. Με αυτήν τη δράση, δεν θα ευαισθητοποιήσουμε μόνο για το πόσο σημαντική είναι η ιδιωτικότητα και η ελευθερία στα έξυπνα κινητά και στα πινάκια. Θα δώσουμε επίσης στους χρήστες τα μέσα για να βελτιώσουν οι ίδιοι τις δικές στους συσκευές».

Η δράση Ελευθερώστε το Android σας ενθαρρύνει τον κόσμο να έρχεται σε επαφή με προγραμματιστές χρήσιμων ιδιοκτησιακών εφαρμογών. Συχνά οι εφαρμογές αυτές διανέμονται χωρίς χρέωση, αλλά όχι με κάποια ελεύθερη άδεια χρήσης. Η ανταπόκριση και οι ενστάσεις των προγραμματιστών συλλέγονται και αναλύονται σε ένα wiki.

Αυτή τη στιγμή το FSF και ο Γερμανικός οργανισμός ιδιωτικού απορρήτου FoeBuD e.V. συνεργάζονται με το FSFE σε μια προσπάθεια να βελτιώσουν τις συνθήκες για την ελευθερία στο λογισμικό και το ιδιωτικό απόρρητο στο χώρο των κινητών. Το FSFE με χαρά προσβλέπει στη συμμετοχή και άλλων οργανώσεων στη δράση αυτή.

Αρχιτεκτονική του Android

Το Android αποτελείται από 5 επίπεδα τα οποία αποτελούν τα κύρια συστατικά του λειτουργικού συστήματος. Στο παρακάτω διάγραμμα παρουσιάζεται η αρχιτεκτονική του Android ενώ στη συνέχεια ακολουθεί η ανάλυση κάθε επίπεδου ξεχωριστά.



Εφαρμογές –Applications

Το Android είναι εφοδιασμένο με ένα σύνολο εφαρμογών στις οποίες μεταξύ των άλλων περιλαμβάνονται :

- e-mail client,
- πρόγραμμα για αποστολή και λήψη SMS
- ημερολόγιο
- χάρτες
- περιηγητής διαδικτύου
- κατάλογο επαφών κλπ.

Η γλώσσα προγραμματισμού όλων αυτών των εφαρμογών είναι η Java.

Πλαίσιο Εφαρμογής – Application Framework

Μέσω της ανοιχτής πλατφόρμας ανάπτυξης του, το Android, παρέχει τη δυνατότητα δημιουργίας εξαιρετικά πλούσιων και καινοτόμων εφαρμογών. Οι προγραμματιστές είναι ελεύθεροι να εκμεταλλευτούν όλα τα πλεονεκτήματα που τους προσφέρει το υλικό της συσκευής, να έχουν πρόσβαση σε πληροφορίες που έχουν σχέση με την τοποθεσία, να τρέξουν υπηρεσίες στο περιθώριο, να ορίσουν ειδοποιήσεις, να προσθέσουν σημειώσεις στη μπάρα κατάστασης και να εκτελέσουν πλήθος άλλων εργασιών.

Οι προγραμματιστές έχουν πλήρη πρόσβαση στα ίδια APIs που χρησιμοποιούν οι βασικές εφαρμογές. Η ίδια η αρχιτεκτονική των εφαρμογών είναι σχεδιασμένη κατά τέτοιο τρόπο ώστε να απλοποιεί την επαναχρησιμοποίηση των διάφορων συστατικών μερών. Οποιαδήποτε εφαρμογή μπορεί να θέσει διαθέσιμες προς χρήση τις δυνατότητές της σε οποιαδήποτε άλλη εφαρμογή που μπορεί να κάνει χρήση αυτών των δυνατοτήτων. Όλες οι εφαρμογές αποτελούνται από ένα σύνολο υπηρεσιών και συστημάτων που περιλαμβάνουν:

- Ένα πλούσιο και επεκτάσιμο σύνολο από *Views* που μπορεί να χρησιμοποιηθεί για το χτίσιμο μίας εφαρμογής. Στο σύνολο περιλαμβάνονται

λίστες, πλέγματα, πλαίσια κειμένου, κουμπιά και ένας ενσωματωμένος περιηγητής διαδικτύου.

- *Content Providers* (διανομείς περιεχομένου) που επιτρέπουν στις εφαρμογές να έχουν πρόσβαση στα δεδομένα άλλων εφαρμογών ή να κοινοποιήσουν στις άλλες εφαρμογές τα δικά τους δεδομένα.
- Ένα *Resource Manager* (διαχειριστής πόρων) που παρέχει πρόσβαση σε πόρους όπως αλφαριθμητικά που έχουν σχέση με την τοποθεσία, τα γραφικά και τα αρχεία των σχεδιαγραμμάτων.
- Ένα *Notification Manager* (διαχειριστής ειδοποιήσεων) που επιτρέπει στις εφαρμογές να εμφανίζουν ειδοποιήσεις στη μπάρα κατάστασης.
- Ένα *Activity Manager* (διαχειριστής δραστηριοτήτων) που ελέγχει τον κύκλο ζωής των εφαρμογών και την εναλλαγή μεταξύ αυτών.

Εγγενείς Βιβλιοθήκες – Native Libraries

Το Android περιλαμβάνει ένα σύνολο βιβλιοθηκών των C/C++ που χρησιμοποιούνται από διάφορα συστατικά μέρη του συστήματος. Οι δυνατότητες αυτών των βιβλιοθηκών γίνονται διαθέσιμες στους προγραμματιστές μέσω του πλαισίου εφαρμογών του Android. Παρακάτω παρουσιάζονται μερικές από τις βασικές βιβλιοθήκες του συστήματος:

- **Βιβλιοθήκη συστήματος C –** μία υλοποίηση της στάνταρ βιβλιοθήκης της C για ενσωματωμένες συσκευές βασισμένες στο Linux.
- **Βιβλιοθήκες πολυμέσων –** βασισμένες στο OpenCORE αυτές οι βιβλιοθήκες υποστηρίζουν την αναπαραγωγή πολλών δημοφιλών προτύπων ήχου, στατικών αρχείων εικόνας και βίντεο όπως MPEG4, H.264, MP3, AAC, AMR, JPG και PNG.
- **Surface Manager –** διαχειρίζεται την πρόσβαση στο υποσύστημα της οθόνης και συνθέτει 2D και 3D επίπεδα γραφικών από πολλαπλές εφαρμογές.
- **LibWebCore –** μία σύγχρονη μηχανή περιηγητή διαδικτύου που υποστηρίζει τον περιηγητή του Android και το ενσωματωμένο web view.
- **SGL –** η μηχανή που παράγει τα 2D γραφικά.

- **3D βιβλιοθήκες –** μία υλοποίηση βασισμένη στα APIs του OpenGL ES 1.0.
- **FreeType –** υποστήριξη vector και bitmap.
- **SQLite –** μία ισχυρή και ελαφριά μηχανή σχεσιακών βάσεων δεδομένων διαθέσιμη σε όλες τις εφαρμογές.

Περιβάλλον χρόνου εκτέλεσης-Android Runtime

Το Android περιλαμβάνει ένα σύνολο βασικών βιβλιοθηκών που παρέχουν το μεγαλύτερο μέρος της λειτουργικότητας που είναι διαθέσιμη στις βασικές βιβλιοθήκες της Java. Κάθε εφαρμογή που εκτελείται στο Android είναι μία ξεχωριστή διεργασία με το δικό της στιγμιότυπο της εικονικής μηχανής Dalvik. Η Dalvik είναι έτσι γραμμένη, ώστε κάθε φορητή συσκευή να μπορεί να τρέξει πολλαπλές εικονικές μηχανές αποτελεσματικά. Επιπροσθέτως, η εικονική μηχανή Dalvik εκτελεί αρχεία της μορφής Dalvik Executable (.dex) η οποία είναι βελτιστοποιημένη για χαμηλή κατανάλωση μνήμης. Η εικονική μηχανή βασίζεται σε καταχωρητές και εκτελεί κλάσεις που έχουν μεταφραστεί από έναν Java compiler και έχουν μετασχηματιστεί σε .dex μορφή μέσω του εργαλείου “dx”. Τέλος, η Dalvik βασίζεται στον πυρήνα του Linux για τη λειτουργικότητα της σε χαμηλό επίπεδο όπως η διαχείριση νημάτων και μνήμης.

Πυρήνας Linux

Το Android βασίζεται στην έκδοση 2.6 του πυρήνα του Linux για τις βασικές υπηρεσίες του συστήματος, όπως την ασφάλεια, τη διαχείριση μνήμης, τη διαχείριση διεργασιών, τη στοίβα δικτύου και το μοντέλο οδήγησης των συσκευών. Ο πυρήνας, επιπλέον, λειτουργεί και σαν ένα αφαιρετικό επίπεδο μεταξύ του υλικού και του υπόλοιπου λογισμικού.

Κεφάλαιο 4

Ανάπτυξη εφαρμογής

Σκοπός- Χρησιμότητα εφαρμογής Twitter-Splunk Mobile

Ξεχωριστή σημασία παρουσιάζει το γεγονός ότι οι χρήστες του Twitter συχνά αναφέρονται σε ιστοσελίδες ή άλλους χρήστες στις δημοσιεύσεις τους χρησιμοποιώντας το πρόθεμα «@», τα λεγόμενα mentions, καθώς και hashtags, λέξεις κλειδιά οι οποίες ξεκινούν με το πρόθεμα «#»και χρησιμοποιούνται για να ομαδοποιούν δεδομένα και να τα κατατάσουν σε κατηγορίες. Με την επιλογή ενός mention ο χρήστης μεταφέρεται στον υπερσύνδεσμο στον οποίο αναφέρεται μετά το «@», ενώ με την επιλογή ενός hashtag μπορεί να δει τα τελευταία tweets που το περιλαμβάνουν. Ο τεράστιος όγκος πληροφοριών που βρίσκεται στο twitter το καθιστά κατάλληλο εργαλείο για να ενημερωθεί κάποιος για θέματα που τον ενδιαφέρουν.

Σκοπός αυτής της εφαρμογής είναι η συλλογή και αξιοποιήση των πληροφοριών που αναφέρθηκαν παραπάνω. Αυτό θα γίνει μέσω της ανάπτυξης μιας εφαρμογής οι οποία θα δίνει τη δυνατότητα στο χρήστη να πάρει πληροφορίες για κάποιο θέμα που τον αφορά, να ενημερωθεί για όλες τις νέες τάσεις και δημοφιλή θέματα που αναφέρονται στο Twitter, μέσω του εργαλείου Splunk.

Ο χρήστης μπορεί μέσω των αποθηκευμένων αναζητήσεων να πάρει γενικές αναλύσεις σχετικά με τα top mentions και hashtags, να ενημερωθεί για το ποιοι είναι οι πιο δημοφιλείς χρήστες του κοινωνικού δικτύου για τη χρονική περίοδο που επιθυμεί. Επίσης έχει τη δυνατότητα να λάβει πληροφορίες και στατιστικά σχετικά με το μέσο με το οποίο μπαίνει κάποιος στο Twitter, καθώς και τη ζώνη ώρας στην οποία ανήκουν οι χρήστες. Με την επιλογή Alerts μπορεί να λάβει ενημέρωση σχετικά με κάποιο γεγονός το οποίο έχει ρυθμίσει ως σημαντικό και επιθυμεί να ενημερωθεί για οποιαδήποτε εξέλιξη το αφορά. Τέλος με την επιλογή New Search

μπορεί να πραγματοποιήσει και να περιορίσει μια αναζήτηση πραγματικού χρόνου πάνω σε πράγματα που τον ενδιαφέρουν πιο πολύ, τα οποία δεν υπάρχουν στον κατάλογο Saved Searches.

Η εν λόγω εφαρμογή μπορεί να χρησιμοποιηθεί από έναν απλό χρήστη του Twitter, ο οποίος χρησιμοποιεί το Twitter για την καθημερινή του ενημέρωση πάνω στις κοινωνικές και ψυχαγωγικές εξελίξεις, μπορεί όμως να αποδειχθεί και χρήσιμο εμπορικό αλλά και επιχειρηματικό εργαλείο. Παρόλο που το Twitter Splunk Mobile είναι μια σχετικά απλή εφαρμογή για κινητό τηλέφωνο, δεν παύει να επιστρέφει ακριβή δεδομένα, επεξεργασμένα από το έξυπνο και πανίσχυρο Splunk. Ιδιοκτήτες παντός είδους επιχειρήσεων μπορούν να επωφεληθούν από αυτό το μικρό εργαλείο, το οποίο μπορεί να τους ενημερώνει καθημερινά για τις νέες τάσεις του αγοραστικού κοινού, για την εμφάνιση ενός νέου προϊόντος ή υπηρεσίας δίνοντας τους την ευκαιρία να προσφέρουν «τη νέα αυτή ανάγκη» ταχύτερα και φθηνότερα από κάποιον άλλο. Ακόμα, άτομα του που το επάγγελμά τους βασίζεται στην προβολή και τη διαφήμιση, πραγματοποιώντας μια απλή αναζήτηση μπορούν να παρακολουθούν την εξέλιξη τους και την αποδοχή που έχουν από το κοινό, μέσω των αναφορών που γίνονται στο πρόσωπό τους από τους χρήστες του κοινωνικού αυτού δικτύου.

Αυτές είναι μερικές από τις πιο βασικές εφαρμογές του συγκεκριμένου app που καταφέρνει να παντρέψει την ανάγκη του κόσμου για σύντομη ενημέρωση με την ανάγκη να μπορεί να το κάνει οποιαδήποτε στιγμή μέσα από την οθόνη του κινητού του τηλεφώνου.

Ανάπτυξη εφαρμογής Twitter-Splunk Mobile

I.Ανάπτυξη στο Splunk

Για τη δημιουργία της εφαρμογής Twitter-Splunk Mobile για Twitter αναζητήσεις χρησιμοποιήθηκε το εργαλείο αναζήτησης και ανάλυσης δεδομένων Splunk και η εφαρμογή του Splunk με όνομα Splunk Mobile.

Το Splunk Mobile είναι μια εφαρμογή σχεδιασμένη για έξυπνα κινητά τηλέφωνα και tablets, τα οποία υποστηρίζουν διάφορα είδη σύγχρονων λειτουργικών συστημάτων (Android, IOS, Blackberry, Windows Mobile) με φιλικό και εύχρηστο μενού ακόμα και για την πιο μικρή οθόνη. Η εφαρμογή αυτή επιτρέπει στους χρήστες του Splunk web να βλέπουν στατιστικά και αναλύσεις με την μορφή λίστας events, πινάκων και γραφικών αναπαραστάσεων προερχόμενες από το δίκτυο τους .

Εικόνα 5 Splunk Mobile Print Screens

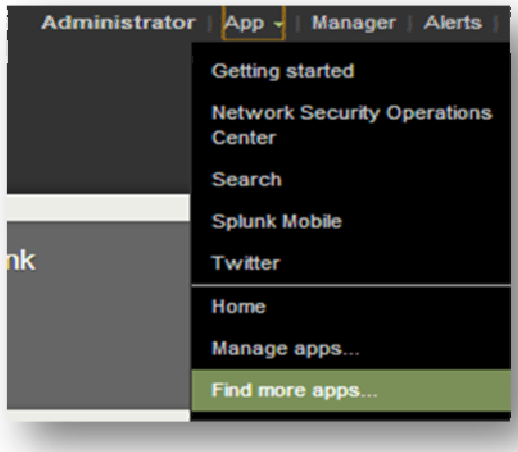
Το Splunk Mobile παρέχει τη δυνατότητα δημιουργίας αποθηκευμένων αναζητήσεων από το χρήστη ανάλογα με τις απαιτήσεις και τις ανάγκες του. Επίσης το μενού προσφέρει στο χρήστη την επιλογή και δημιουργία νέας αναζήτησης σε πραγματικό χρόνο, κρατώντας τον διαρκώς ενημερωμένο για οτιδήποτε θέλει να ελέγξει, το οποίο ίσως να μην καλύπτουν οι αποθηκευμένες αναζητήσεις του μενού Searches.

Εικόνα 6 Splunk Mobile Interface

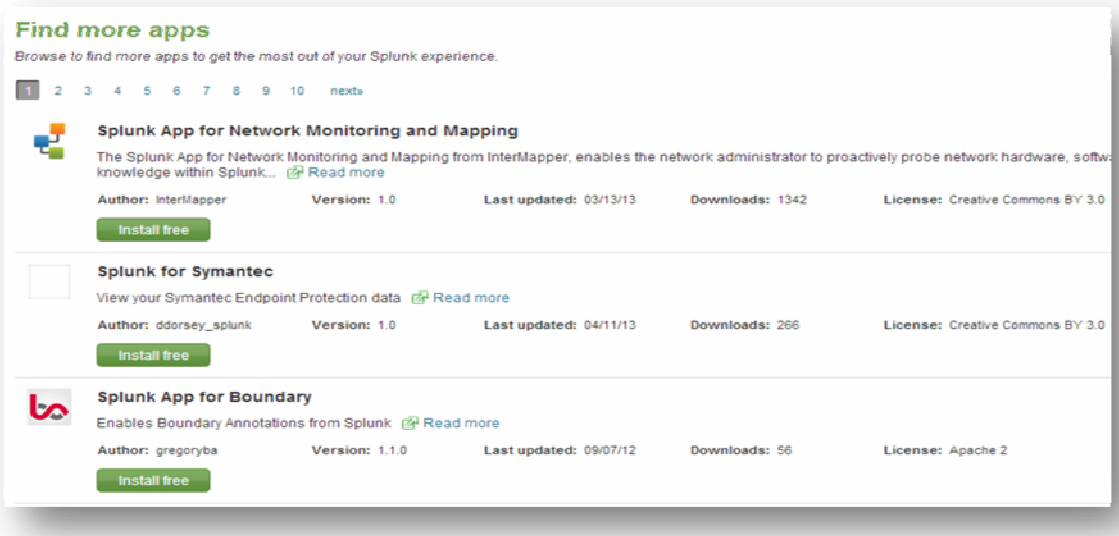
Τρόπος εγκατάστασης Splunk Mobile στο Splunk

Το Splunk διαθέτει μια μεγάλη ποικιλία εφαρμογών οι οποίες επεκτείνουν τις δυνατότητες του . Οι εφαρμογές αυτές είναι διαθέσιμες από το χρήστη και μπορούν να αποκτηθούν δωρεάν από κάποιον που διαθέτει άδεια χρήσης του εργαλείου. Η απόκτηση και εγκατάσταση μιας εφαρμογής στο Splunk γίνεται από το Interface του Splunk:

1. Πηγαίνουμε στο μενού App→Find more apps..

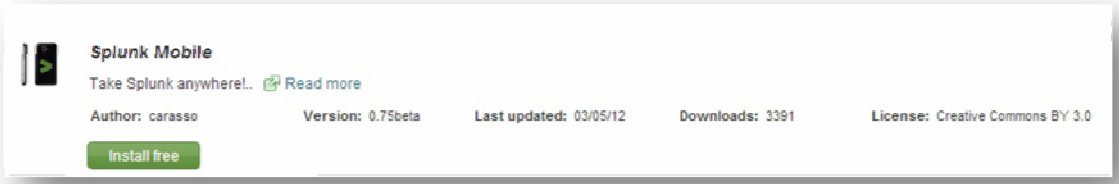


Εμφανίζεται η σελίδα που περιέχει τη λίστα με όλες τις εφαρμογές που είναι διαθέσιμες στη βάση δεδομένων του Splunk.

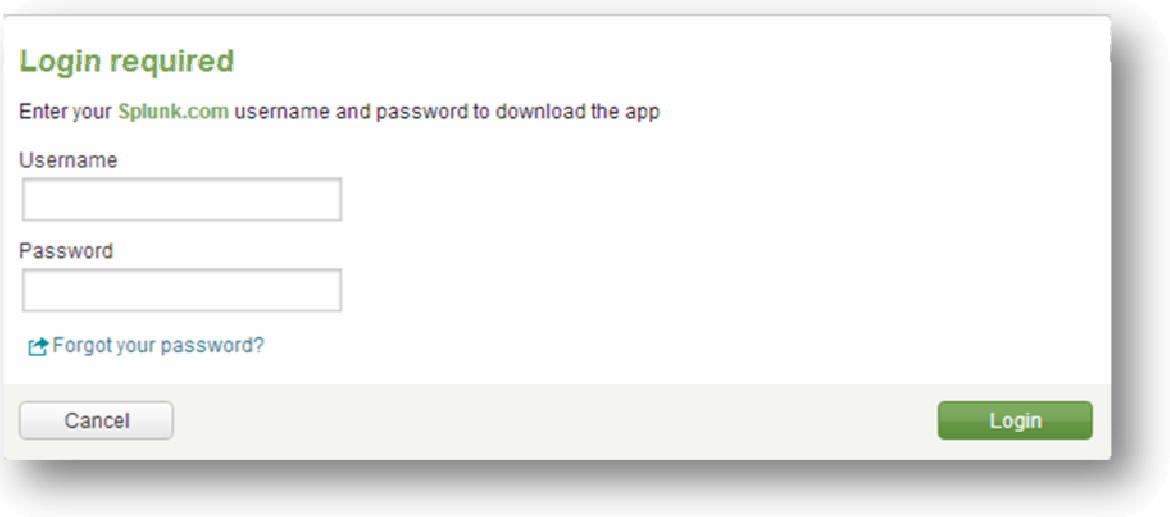


2. Πληκτρολογούμε στο πεδίο της αναζήτησης που βρίσκεται στην πάνω δεξιά πλευρά της σελίδας, Splunk Mobile και πατάμε Enter.

3. Εμφανίζεται η εφαρμογή Splunk Mobile. Πατάμε την επιλογή Install free.

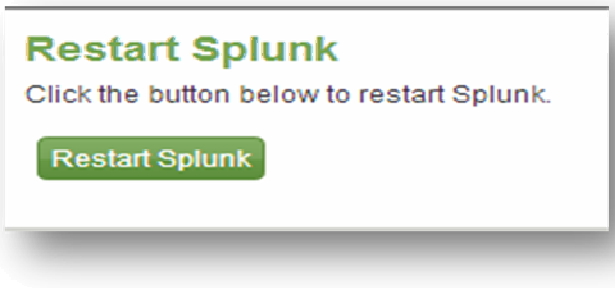


4. Πληκτρολογούμε το όνομα χρήστη και τον κωδικό μας στα πεδία Username και Password:

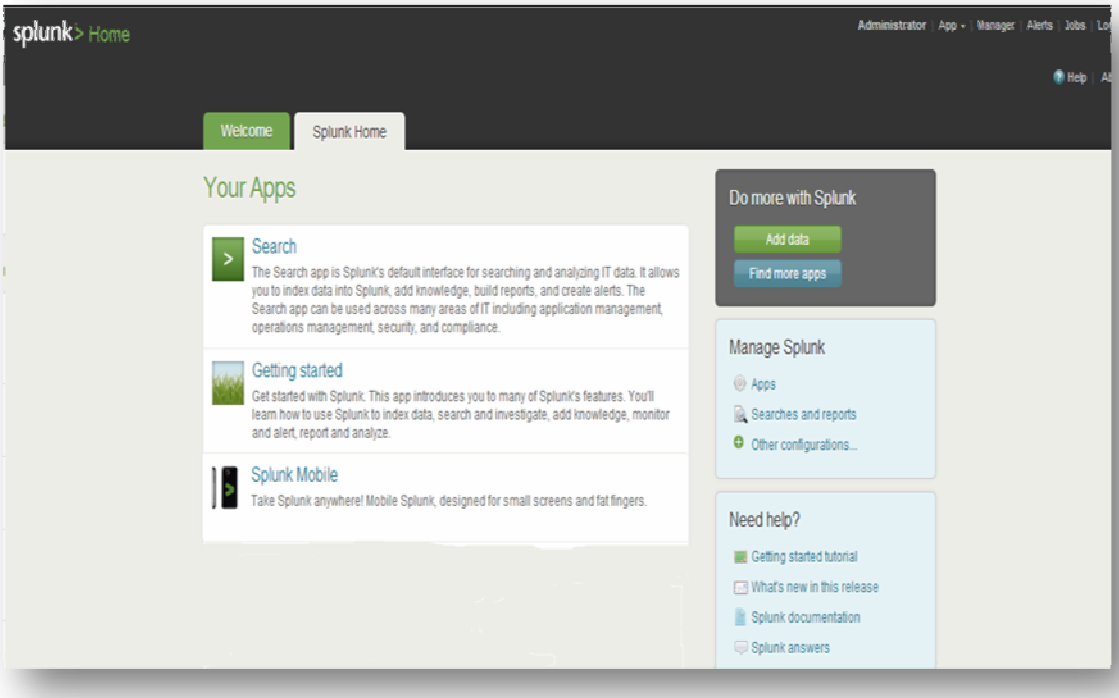


Το Splunk εγκαθιστά την εφαρμογή και απαιτείται επανεκκίνηση για να ολοκληρωθεί η διαδικασία.

5. Στη σελίδα του Manager επιλέγουμε Server Controls→ Restart Splunk.



6. Μόλις ολοκληρωθεί η επανεκκίνηση, το Splunk μας οδηγεί στην αρχική του σελίδα, όπου πλέον μπορούμε να δούμε στη λίστα των εφαρμογών την εφαρμογή Splunk Mobile.



Εισαγωγή Tweet data feeds στο Index

Το επόμενο βήμα της διαδικασίας δημιουργίας της εφαρμογής είναι να εισαχθούν δεδομένα από το Twitter στο Splunk Index. Αυτό θα γίνει με τη βοήθεια του Twitter API.

Το Twitter API

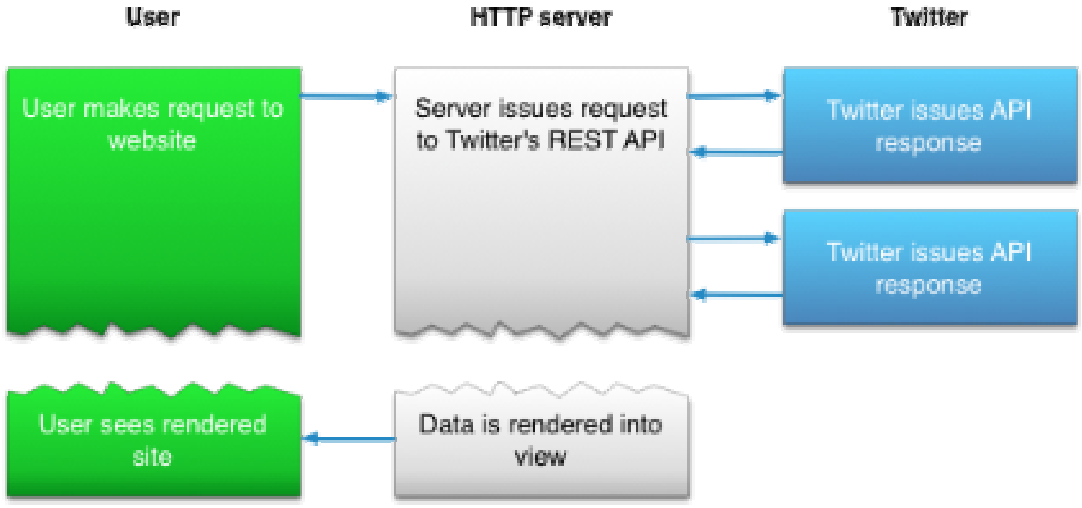
Το σύνολο των API'S που προσφέρονται από το Twitter, δίνουν τη δυνατότητα στους προγραμματιστές να αποκτήσουν πρόσβαση στην παγκόσμια ροή των δεδομένων που συρρέουν στο Twitter.

Το Twitter προσφέρει διαφορετικές επιλογές συλλογής δεδομένων από τις οποίες η καθεμία εξυπηρετεί διαφορετικό σκοπό. Πιο συγκεκριμένα προσφέρει:

Public streams	Streams από το συνολικό αριθμό δεδομένων που συλλέγονται

	από το Twitter. Κατάλληλο για την ακολούθηση συγκεκριμένων χρηστών, θεμάτων και συλλογή πληροφορίας.
User streams	Streams που αφορούν όλες τις ενέργειες που προέρχονται από ένα συγκεκριμένο χρήστη του Twitter.
Site streams	Η πολυχρηστική εκδοχή των User streams. Αφορά servers που πρέπει να συνδεθούν στο Twitter για λογαριασμό πολλών χρηστών.

Η σύνδεση με το streaming API απαιτεί μια μόνιμα ανοιχτή HTTP σύνδεση.



Η διαδικασία του streaming παίρνει ως είσοδο Tweets και εκτελεί οποιαδήποτε ανάλυση, φιλτράρισμα ή και συνάθροιση πριν αποθηκευτεί ένα αποτέλεσμα στη βάση δεδομένων. Η HTTP διαδικασία σαρώνει τη βάση δεδομένων για απαντήσεις που αφορούν τα αιτήματα χρηστών. Αυτή η διαδικασία είναι αρκετά περίπλοκη όμως εξυπηρετεί πολλούς τύπους εφαρμογών.

Παράδειγμα απάντησης αιτήματος χρήστη

"user":{

"followers_count":-1,

"friends_count":-1,

"listed_count":**null**,

"created_at":"Wed Sep 23 17:35:05 +0000 2009",

"favourites_count":-1,

"utc_offset":**null**,

"time_zone":**null**,

"geo_enabled":**false**,

"verified":**false**,

"statuses_count":-1,

"lang":"en",

...

}

Εισαγωγή Tweets στο Splunk

Για την εισαγωγή των twitter feeds στο Splunk στη συγκεκριμένη εργασία χρησιμοποιείται η scripting γλώσσα Python.

Παράδειγμα Twitter

Το script αρχείο του Twitter, το λεγόμενο tweepy διοχετεύει δεδομένα από μία Twitter πηγή στο Splunk για ανάλυση. Το tweety είναι διαθέσιμο στο σύνδεσμο: http://tweepy.github.com/

Το twitter.py αρχείο τοποθετείται στην ακόλουθη τοποθεσία του αρχείου εγκατάστασης του Splunk:

$SPLUNK_HOME/etc/apps/twitter/bin/twitter.py

twitter.py

```
import tweepy, sys
import xml.dom.minidom, xml.sax.saxutils
from tweepy.utils import import_simplejson
json = import_simplejson()
from tweepy.models import Status
import logging
import splunk.entity as entity

import httplib
from socket import timeout
from tweepy.auth import BasicAuthHandler
from tweepy.api import API

#set up logging suitable for splunkd comsumption
logging.root
logging.root.setLevel(logging.DEBUG)
formatter = logging.Formatter('%(levelname)s %(message)s')
handler = logging.StreamHandler()
handler.setFormatter(formatter)
```

```
logging.root.addHandler(handler)

SCHEME = """<scheme>
    <title>Twitter</title>
    <description>Get data from Twitter.</description>
    <use_external_validation>true</use_external_validation>
    <streaming_mode>simple</streaming_mode>
    <endpoint>
        <args>
            <arg name="name">
                <title>Twitter feed name</title>
                <description>Name of the current feed using the user credentials
supplied.</description>
            </arg>

            <arg name="username">
                <title>Twitter ID/Handle</title>
                <description>Your Twitter ID.</description>
            </arg>
            <arg name="password">
                <title>Password</title>
                <description>Your twitter password</description>
            </arg>
        </args>
    </endpoint>
</scheme>
"""

def do_scheme():
            print SCHEME
# prints XML error data to be consumed by Splunk
def print_error(s):
    print "<error><message>%s</message></error>" %
xml.sax.saxutils.escape(s)

class SplunkListener( tweepy.StreamListener ):

        def on_data(self, data):
            super( SplunkListener, self).on_data( data )
            twt = json.loads(data)
            if 'text' in twt:
                print json.dumps(twt)
```

```
            return True

        def on_error(self, status_code):
                """Called when a non-200 status code is returned"""
                print 'got error\n'
                print status_code
                        logging.error("got error: %s" %(status_code))
                return False

        def on_timeout(self):
                """Called when stream connection times out"""
                print 'got timeout'
                        logging.info("Got a timeout")
                return

def validate_conf(config, key):
    if key not in config:
        raise Exception, "Invalid configuration received from Splunk: key '%s' is
missing." % key

#read XML configuration passed from splunkd
def get_config():
    config = {}
    try:
        # read everything from stdin
        config_str = sys.stdin.read()

        # parse the config XML
        doc = xml.dom.minidom.parseString(config_str)
        root = doc.documentElement
        conf_node = root.getElementsByTagName("configuration")[0]
        if conf_node:
            logging.debug("XML: found configuration")
            stanza = conf_node.getElementsByTagName("stanza")[0]
            if stanza:
                stanza_name = stanza.getAttribute("name")
                if stanza_name:
                    logging.debug("XML: found stanza " + stanza_name)
                    config["name"] = stanza_name

                    params = stanza.getElementsByTagName("param")
                    for param in params:
```

```
                param_name = param.getAttribute("name")
                logging.debug("XML: found param '%s'" % param_name)
                if param_name and param.firstChild and \
                   param.firstChild.nodeType == param.firstChild.TEXT_NODE:
                    data = param.firstChild.data
                    config[param_name] = data
                    logging.debug("XML: '%s' -> '%s'" % (param_name, data))

        checkpnt_node = root.getElementsByTagName("checkpoint_dir")[0]
        if checkpnt_node and checkpnt_node.firstChild and \
          checkpnt_node.firstChild.nodeType ==
checkpnt_node.firstChild.TEXT_NODE:
            config["checkpoint_dir"] = checkpnt_node.firstChild.data

        if not config:
            raise Exception, "Invalid configuration received from Splunk."

        # just some validation: make sure these keys are present (required)
        validate_conf(config, "name")
        validate_conf(config, "username")
        validate_conf(config, "password")
        validate_conf(config, "checkpoint_dir")
    except Exception, e:
        raise Exception, "Error getting Splunk configuration via STDIN: %s" %
str(e)

    return config

def get_validation_data():
    val_data = {}

    # read everything from stdin
    val_str = sys.stdin.read()

    # parse the validation XML
    doc = xml.dom.minidom.parseString(val_str)
    root = doc.documentElement

    logging.debug("XML: found items")
    item_node = root.getElementsByTagName("item")[0]
    if item_node:
        logging.debug("XML: found item")
```

```
        name = item_node.getAttribute("name")
        val_data["stanza"] = name

        params_node = item_node.getElementsByTagName("param")
        for param in params_node:
            name = param.getAttribute("name")
            logging.debug("Found param %s" % name)
            if name and param.firstChild and \
              param.firstChild.nodeType == param.firstChild.TEXT_NODE:
               val_data[name] = param.firstChild.data

    return val_data

# parse the twitter error string and extract the message
def get_twitter_error(s):
    try:
        doc = xml.dom.minidom.parseString(s)
        root = doc.documentElement
        messages = root.getElementsByTagName("Message")
        if messages and messages[0].firstChild and \
          messages[0].firstChild.nodeType ==
messages[0].firstChild.TEXT_NODE:
            return messages[0].firstChild.data
        return ""
    except xml.parsers.expat.ExpatError, e:
        return s

def validate_config(username,password):
  try:
            auth = BasicAuthHandler(username,password)
            headers = {}
            host = 'stream.twitter.com'
            url = '/1/statuses/sample.json?delimited=length'
            body = None
            timeout = 5.0
            auth.apply_auth(None,None, headers, None)
            conn = httplib.HTTPSConnection(host)
            conn.connect()
            conn.sock.settimeout(timeout)
            conn.request('POST', url, body, headers=headers)
            resp = conn.getresponse()
```

```
            if resp.status != 200:
                        raise Exception,"HTTP request to Twitter returned with
status code %d (%s): %s" % (resp.status,resp.reason,
get_twitter_error(resp.read()))
                        logging.error("Invalid twitter credentials %s , %s" %
(username,password))
            conn.close()
  except Exception,e:
            print_error("Invalid configuration specified: %s" % str(e))
            sys.exit(1)

def run():
            config =get_config()

            username=config["username"]
            password=config["password"]

            # Validate username and password before starting splunk listener.
            logging.debug("Credentials found: username = %s, password
= %s" %(username,password))
            validate_config(username,password)

            listener = SplunkListener()
        stream = tweepy.Stream( username,password, listener )
        stream.sample()
if __name__ == '__main__':
    if len(sys.argv) > 1:
        if sys.argv[1] == "--scheme":
            do_scheme()
        elif sys.argv[1] == "--validate-arguments":
            if len(sys.argv)>3:
                        validate_config(sys.argv[2],sys.argv[3])
                else:
                        print 'supply username and password'
        elif sys.argv[1] == "--test":
            print 'No tests for the scheme present'
        else:
            print 'You giveth weird arguments'
    else:
        # just request data from Twitter
        run()
```

```
sys.exit(0)
```

Αρχείο ρυθμίσεων Twitter

Το παρακάτω αρχείο ρυθμίσεων τοποθετήθηκε στο ακόλουθη τοποθεσία του Splunk Directory:

$SPLUNK_HOME/etc/apps/twitter/README/inputs.conf.spec

inputs.conf.spec

[twitter://default]

*This is how the Twitter app is configured

username = <value>

*This is the user's twitter username/handle

password = <value>

*This is the user's password used for logging into twitter

Δείγμα εισόδου δεδομένων από το Twitter

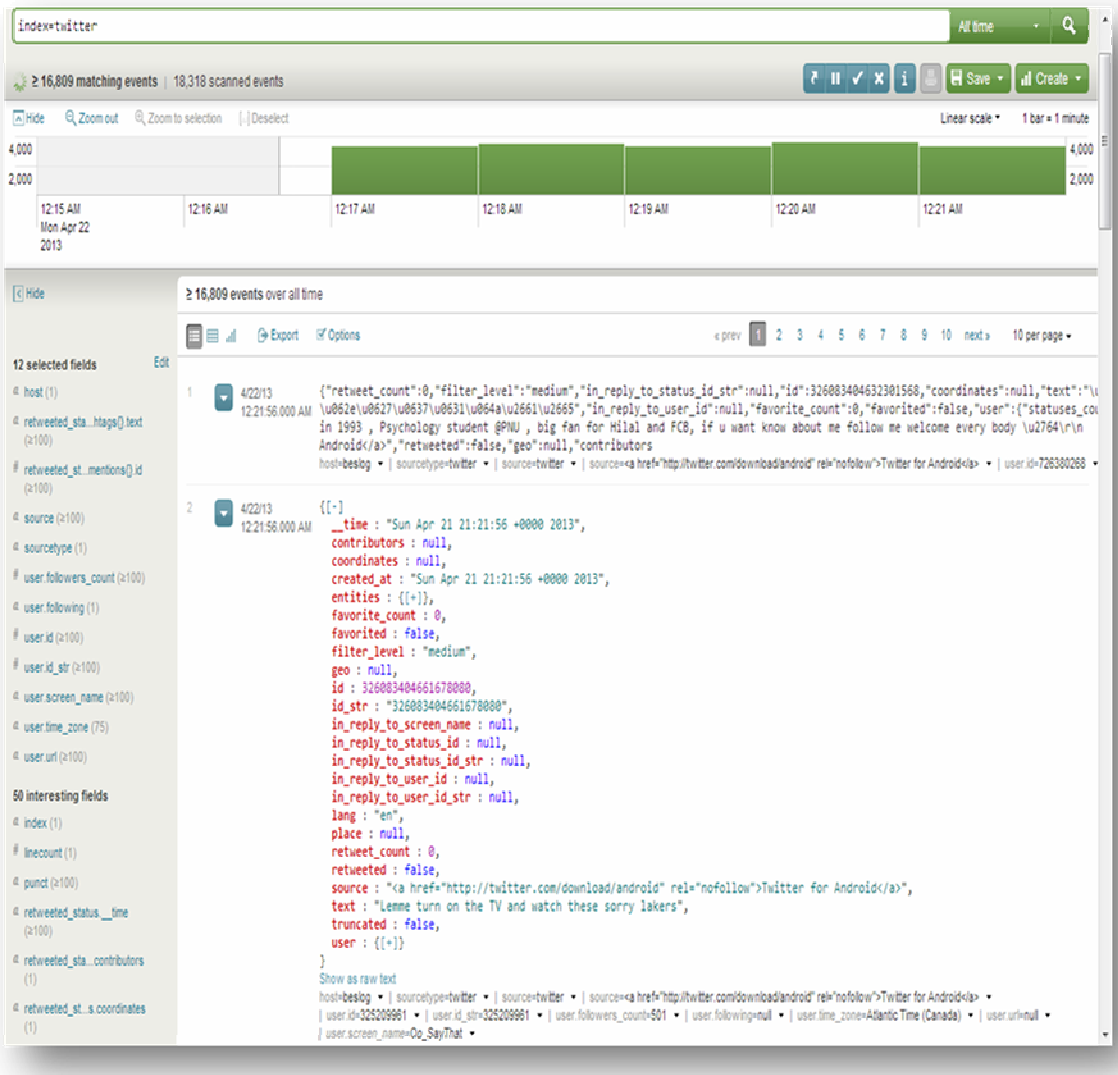
Ακολουθεί παράδειγμα εισόδου δεδομένων από το Twitter στο index του Splunk:

{"contributors":null,"text":"@CraZiiBoSSx3 Yea ... Lo_Okhttp://twitpic.com/19ksg2","created_at":"Fri Mar 19 18:41:17 +0000 2010","truncated":false,"coordinates":null,"in_reply_to_screen_name":"CraZiiBoSSx3","favorited":false,"geo":null,"in_reply_to_status_id":10735405186,"source":"Echofon","place":null,"in_reply_to_user_id":114199314,"user":{"created_at":"Mon Dec 21 23:01:05 +0000 2009","profile_background_color":"0099B9","favourites_count":0,"lang":"en","p

rofile_text_color":"3C3940","location":"iiN A Banqinq
Body !","following":null,"time_zone":"Central Time (US &
Canada)","description":"Da Names GiiqqL3z; Liqhtskin Beauty; FunSiized ;);
Brookyln Babe Witt Carribean Wayyz; Waht Mo Can Ya Ask 4 ? Follow A Bad
Chiq Buh Dnt Follow 2
Unfollow","statuses_count":1685,"profile_link_color":"0099B9","notifications":n
ull,"profile_background_image_url":"http://s.twimg.com/a/1268437273/images/
themes/theme4/bg.gif","contributors_enabled":false,"geo_enabled":false,"profi
le_sidebar_fill_color":"95E8EC","url":null,"profile_image_url":"http://a3.twimg.c
om/profile_images/703836981/PwettyChiQq_Kay_normal.jpg","profile_backgr
ound_tile":false,"protected":false,"profile_sidebar_border_color":"5ED4DC","s
creen_name":"PwettyChiQq_Kay","name":"~GLam DOll
GiiqqLez~","verified":false,"followers_count":77,"id":98491606,"utc_offset":-
21600,"friends_count":64},"id":10735704604}

Για να ελέγξουμε ότι τα δεδομένα εισήχθησαν σωστά στο Index πληκτρολογούμε στην μπάρα αναζήτησης του Splunk την αναζήτηση:

Index=twitter



Εικόνα 7 Αποτελέσματα αναζήτησης tweet feeds στο Splunk

Δημιουργία αποθηκευμένων αναζητήσεων για την εφαρμογή

Όπως αναφέρθηκε στο κεφάλαιο 1 πραγματοποιώντας μια αναζήτηση στο Splunk μπορούμε να εξάγουμε χρήσιμες πληροφορίες και πεδία τα οποία μας εξυπηρετούν σε μελλοντικές αναζητήσεις. Στην εφαρμογή Twitter-Splunk Mobile

θέλουμε να εισάγουμε αναζητήσεις οι οποίες θα επιστρέφουν τα πιο διαδεδομένα hashtags και mentions στο Twitter.

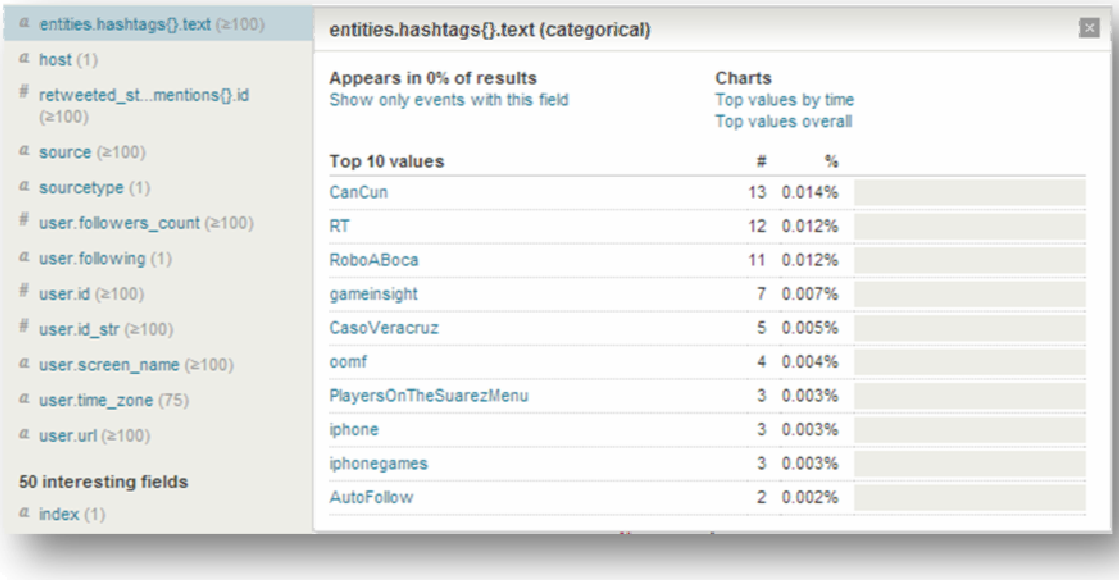
Δημιουργία αναζήτησης για επιστροφή Top Hashtags

Αυτή η αναζήτηση θα επιστρέφει αποτελέσματα που αφορούν τα κορυφαία Hashtags που αναφέρονται στο Twitter.

1. Τρέχουμε την αναζήτηση **index=twitter** και μελετάμε τα πλαϊνά πεδία. Σκοπός μας είναι να εντοπίσουμε κάποιο πεδίο του οποίου το όνομα να περιέχει τη λέξη-κλειδί hashtag.

2. Με μια γρήγορη αναζήτηση στα Interesting fields της πλαϊνής μπάρας εντοπίζουμε το πεδίο **entities.hashtags{}.text.**

3. Το μετακινούμε στη λίστα Selected Fields.

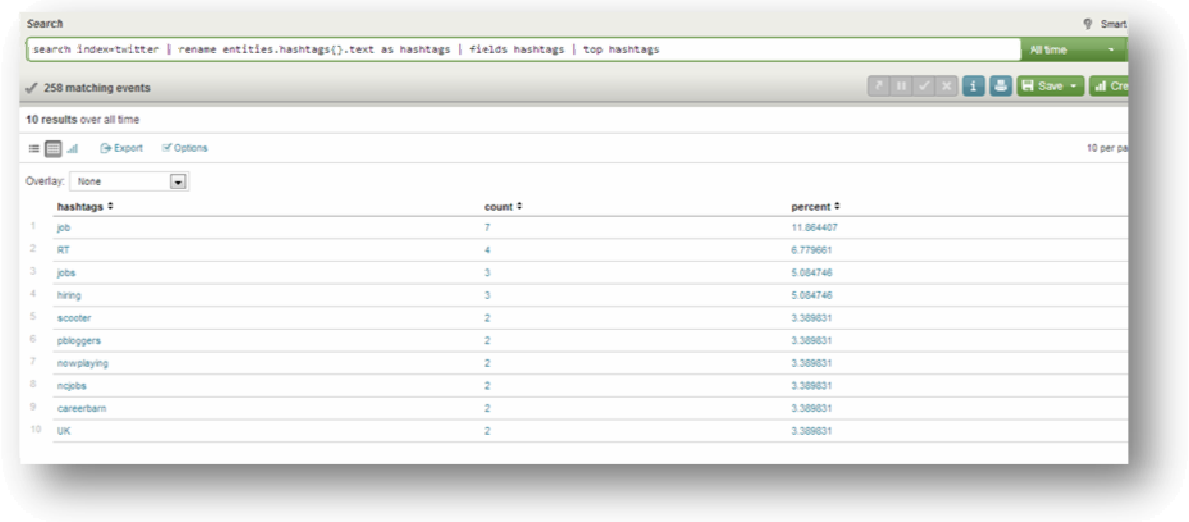


Εικόνα 8 Hashtags field

4. Για να δημιουργήσουμε την αποθηκευμένη αναζήτηση για τα κορυφαία hashtags λοιπόν πληκτρολογούμε την εξής αναζήτηση για χρόνο All time:

search index=twitter | rename entities.hashtags{}.text as hashtags | fields hashtags | top hashtags

5. Πατάμε Enter.



Το Splunk φέρνει πίσω ένα πίνακα που εμφανίζει το ποσοστό και τον αριθμό των κορυφαίων hashtags.

6. Αποθηκεύουμε την αναζήτηση με όνομα Top Hashtags.

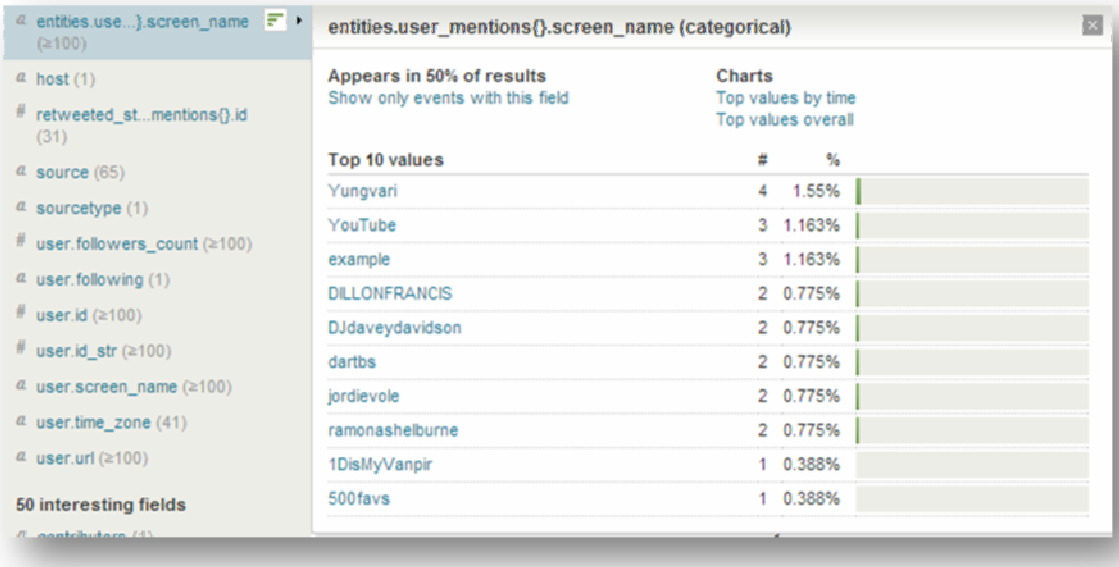
Δημιουργία αναζήτησης για επιστροφή Top Mentions

Σκοπός αυτής της αναζήτησης είναι να επιστρέψει αποτελέσματα που αφορούν τα πιο δημοφιλή Mentions στο Twitter.

1. Τρέχουμε την αναζήτηση **index=twitter** και μελετάμε τα πλαϊνά πεδία. Σκοπός μας είναι να εντοπίσουμε κάποιο πεδίο του οποίου το όνομα να περιέχει τη λέξη-κλειδί mentions.

2. Με μια γρήγορη αναζήτηση στα Interesting fields της πλαϊνής μπάρας εντοπίζουμε το πεδίο ***entities.user_mentions{}.screen_name***

3. Το μετακινούμε στη λίστα Selected Fields όπως προηγουμένως.

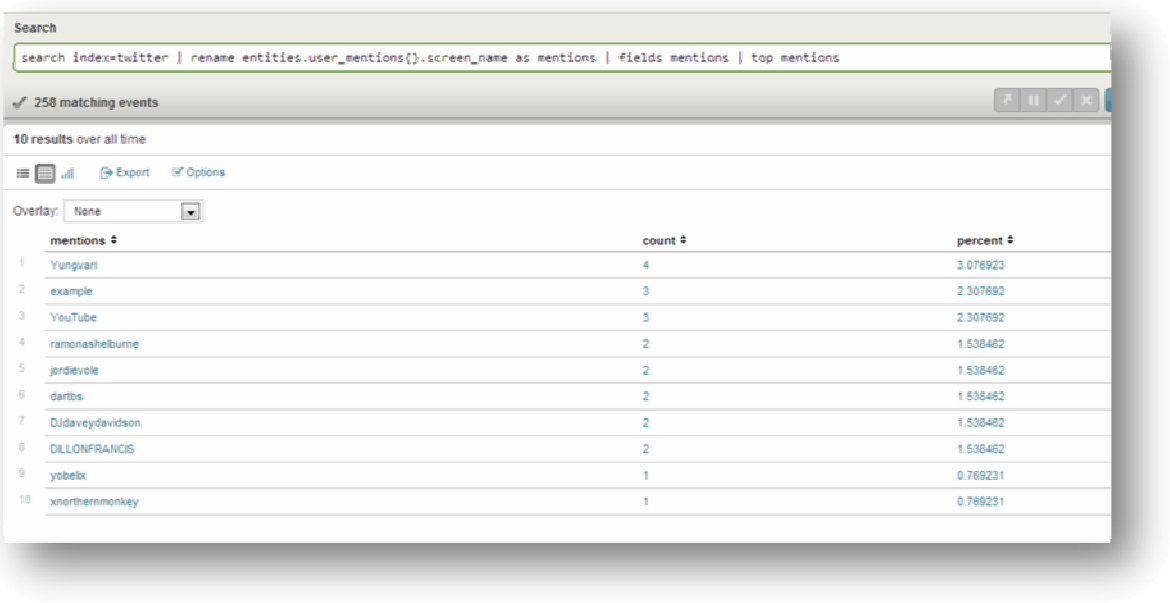


9 Mentions field

4. Για να δημιουργήσουμε την αποθηκευμένη αναζήτηση για τα κορυφαία mentions πληκτρολογούμε την εξής αναζήτηση με επιλογή χρόνου All time:

search index=twitter | rename entities.user_mentions{}.screen_name as mentions | fields mentions | top mentions

5. Πατάμε Enter.



Η αναζήτηση στο Splunk επιστρέφει ένα πίνακα με τον αριθμό και το ποσοστό των top mentions στο Twitter.

6. Αποθηκεύουμε την αναζήτηση με όνομα Top Mentions.

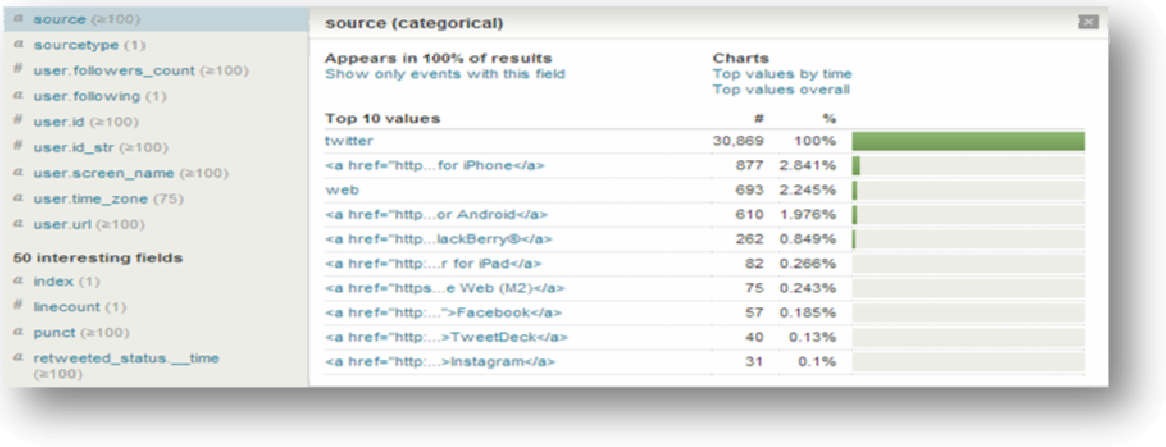
Κοιτώντας τη λίστα των διαθέσιμων πεδίων παρατηρούνται διάφορα πεδία που παρουσιάζουν ενδιαφέρον σχετικά με τις πληροφορίες που επιστρέφουν. Ακολουθώντας λοιπόν την ίδια διαδικασία θα γίνει εισαγωγή μερικών ακόμα αποθηκευμένων αναζητήσεων στην εφαρμογή.

Δημιουργία αναζήτησης για επιστροφή Top User Agents

Αυτή η αναζήτηση θα αναφέρεται στις πηγές από τις οποίες έχουν πρόσβαση οι χρήστες στο Twitter

1. Τρέχουμε την αναζήτηση **index=twitter** και μελετάμε τα πλαϊνά πεδία. Σκοπός μας είναι να εντοπίσουμε κάποιο πεδίο του οποίου το όνομα να περιέχει τη λέξη-κλειδί source.

2. Από προεπιλογή το Splunk τοποθετεί το πεδίο source στα Selected Fields της πλαϊνής μπάρας πεδίων οπότε δεν είναι δύσκολο να εντοπιστεί.



Εικόνα 10 Source Field

3. Για να δημιουργήσουμε την αποθηκευμένη αναζήτηση για τα μέσα από τα οποία έχουν πρόσβαση οι χρήστες, πληκτρολογούμε την εξής αναζήτηση, για χρόνο All Time:

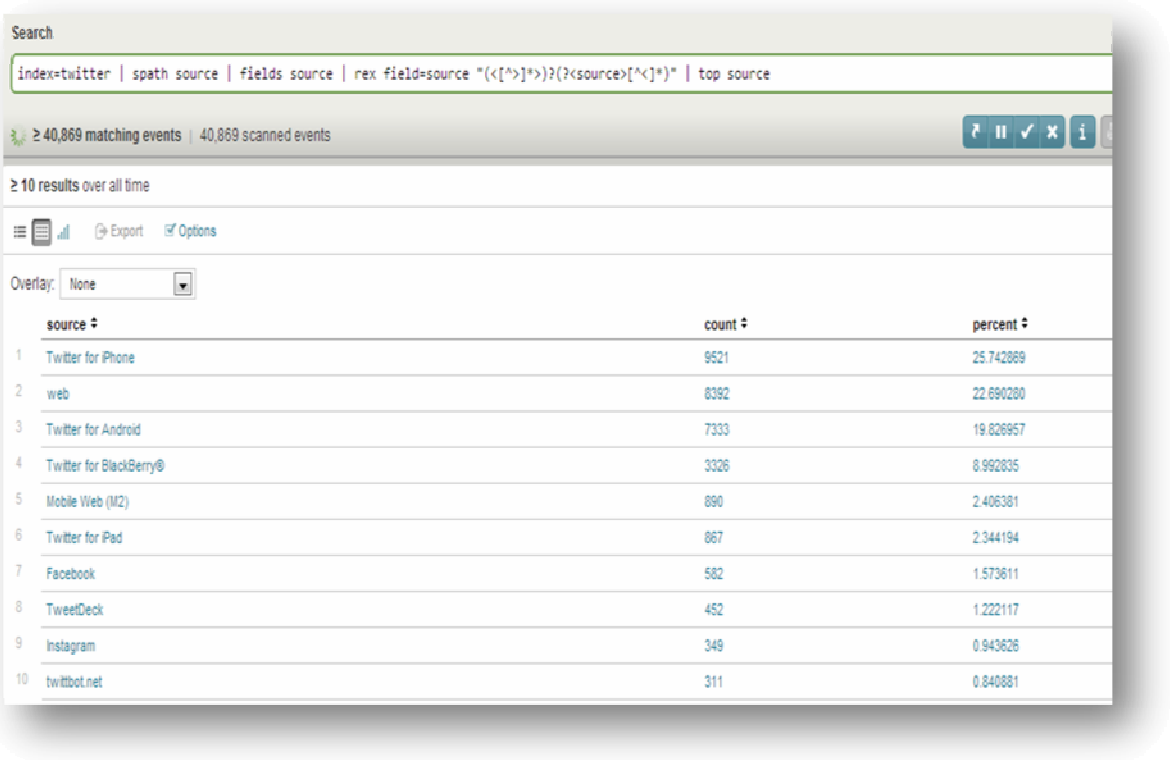
index=twitter | spath source | fields source | rex field=source "(<[^>]*>)?(?<source>[^<]*)" | top source

**Κάνουμε χρήση των χαρακτήρων (<[^>]*>)?(?<>[^<]*) ώστε να εμφανιστεί μόνο το όνομα του μέσου στα αποτελέσματα, χωρίς το html πρόθεμα*

* *

*** Δεν μπορεί να γίνει μετονομασία του πεδίου Source γι' αυτό το λόγο το αφήνουμε ως έχει.*

4. Πατάμε Enter.



	source	count	percent
1	Twitter for iPhone	9521	25.742889
2	web	8382	22.660280
3	Twitter for Android	7333	19.826957
4	Twitter for BlackBerry®	3326	8.992835
5	Mobile Web (M2)	890	2.406381
6	Twitter for iPad	867	2.344194
7	Facebook	582	1.573611
8	TweetDeck	452	1.222117
9	Instagram	349	0.943626
10	twittbot.net	311	0.840881

Στον πίνακα αποτελεσμάτων παρουσιάζονται τα 10 πιο δημοφιλή μέσα που χρησιμοποιούν οι χρήστες του Twitter για να εισέλθουν στην υπηρεσία.

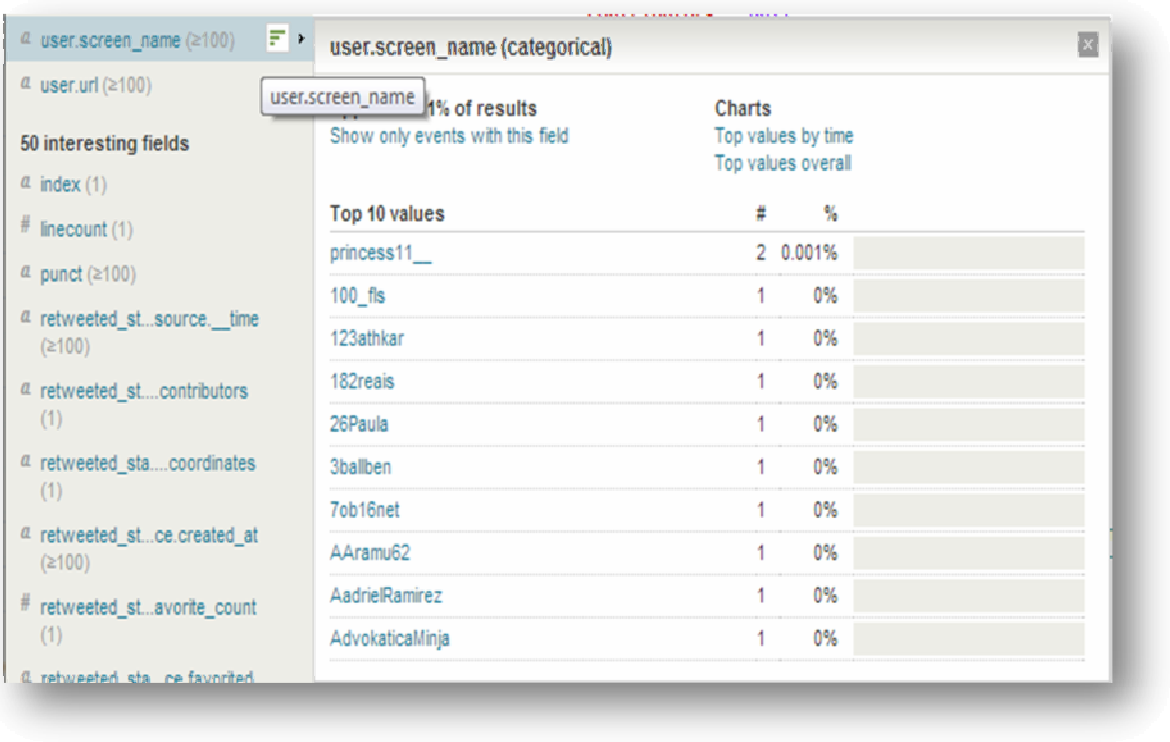
5. Αποθηκεύουμε την αναζήτηση με όνομα Top User Agents.

Δημιουργία αναζήτησης για επιστροφή Top Users

Αυτή η αναζήτηση εμφανίζει τους χρήστες που χρησιμοποιούν περισσότερο το Twitter.

1. Τρέχουμε την αναζήτηση **index=twitter** και μελετάμε τα πλαϊνά πεδία. Σκοπός μας είναι να εντοπίσουμε κάποιο πεδίο του οποίου το όνομα να περιέχει τη λέξη-κλειδί user.

2. Στα Interesting Fields εντοπίζουμε το πεδίο με όνομα ***user.screen_name*** και το τοποθετούμε στη λίστα Selected Fields.

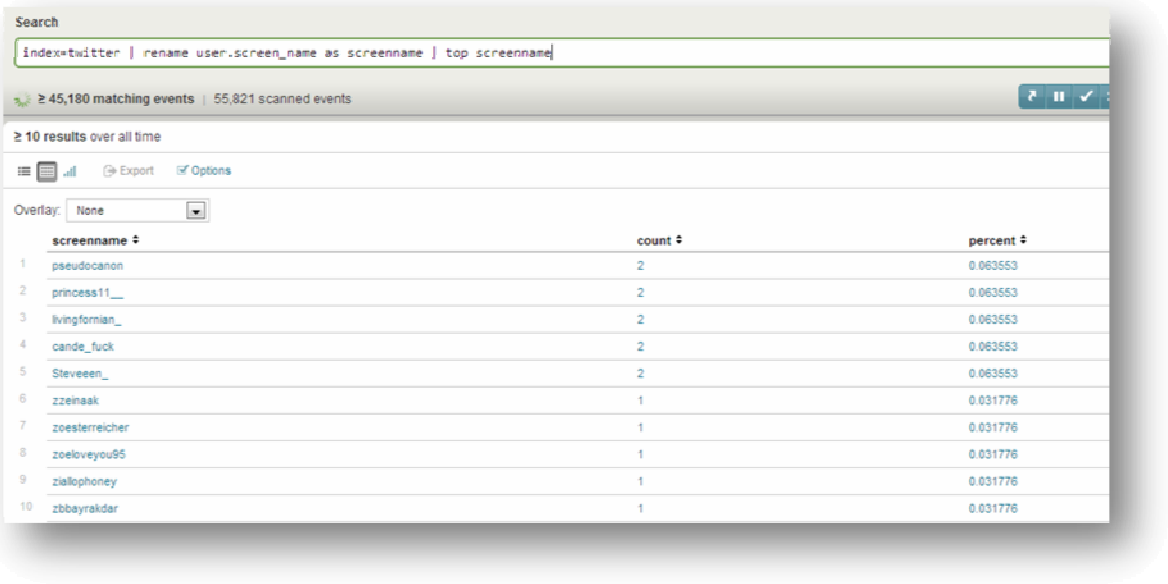


Εικόνα 11 User screen name Field

3. Πληκτρολογούμε την αναζήτηση με επιλογή χρόνου All Time:

index=twitter | rename user.screen_name as screenname | top screenname

4. Πατάμε Enter.



Το Splunk επιστρέφει τη λίστα με τους πιο δημοφιλείς χρήστες του κοινωνικού δικτύου.

5. Αποθηκεύουμε την αναζήτηση με όνομα Top Users.

Δημιουργία αναζήτησης για επιστροφή Tweet Time Zones

Αυτή η αναζήτηση εμφανίζει τους χρήστες που χρησιμοποιούν περισσότερο το Twitter.

1. Τρέχουμε την αναζήτηση **index=twitter** και μελετάμε τα πλαϊνά πεδία. Σκοπός μας είναι να εντοπίσουμε κάποιο πεδίο του οποίου το όνομα να περιέχει τη λέξη-κλειδί time.

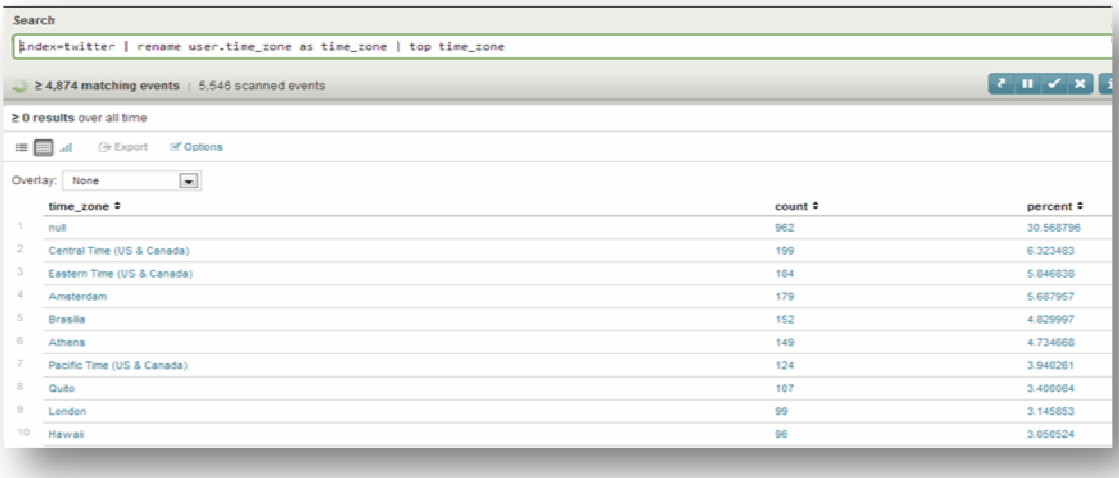
2. Στα Interesting Fields εντοπίζουμε το πεδίο με όνομα ***user.time_zone*** και το τοποθετούμε στη λίστα Selected Fields.

Εικόνα 12 Time zone Field

3. Πληκτρολογούμε την αναζήτηση:

index=twitter | rename user.time_zone as time_zone | top time_zone

4. Πατάμε Enter.



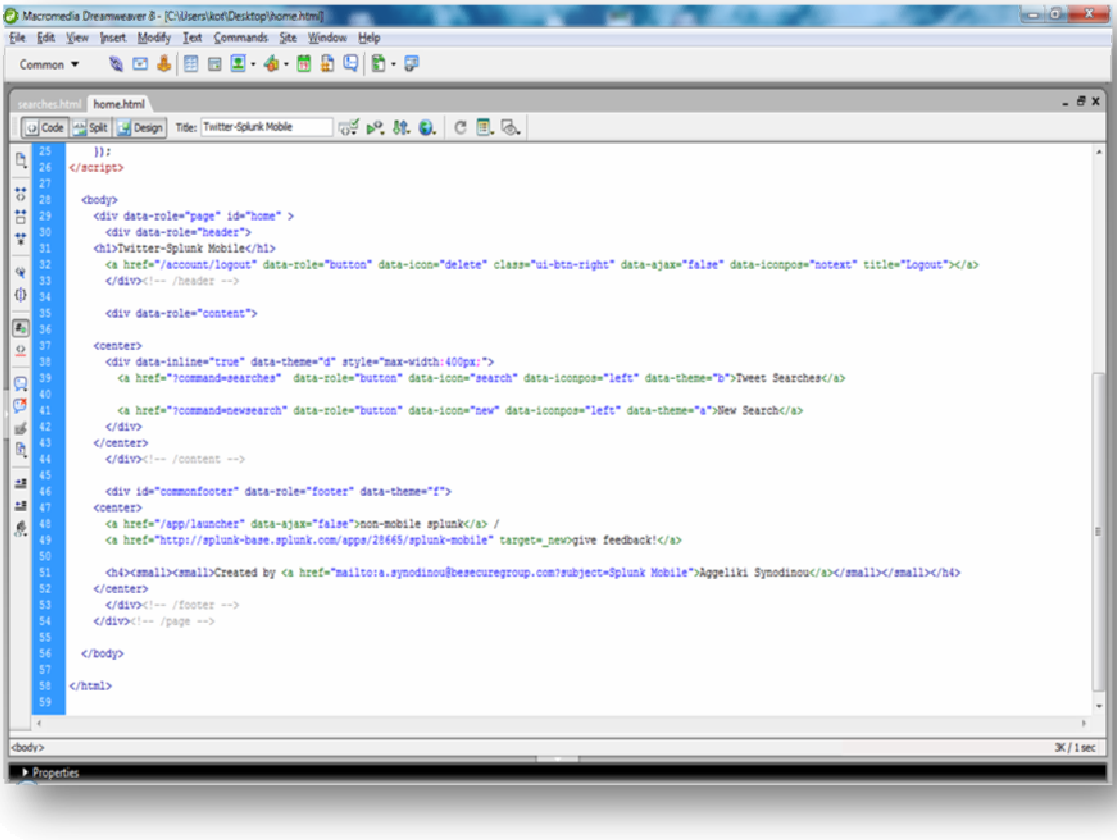
Το Splunk επιστρέφει τη λίστα με τις χώρες που οι χρήστες τους παρουσιάζονται ως πιο ενεργοί στο Twitter

5. Αποθηκεύουμε την αναζήτηση με όνομα Tweet Time Zones.

Αλλαγές στα αρχεία του Splunk Mobile

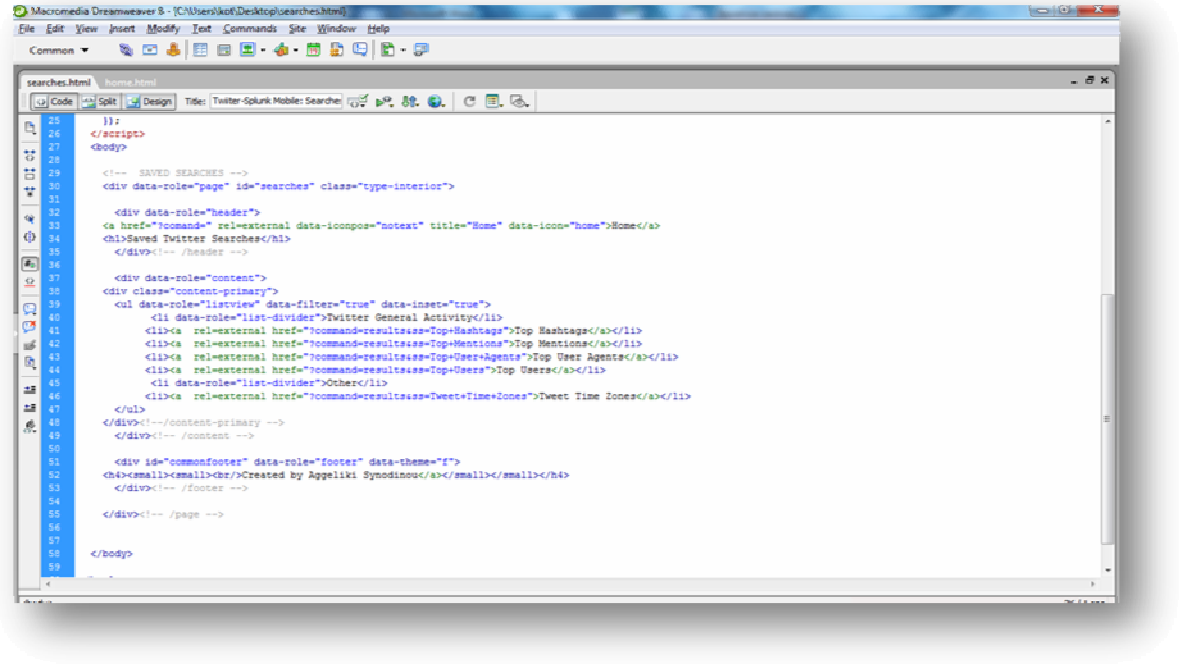
Αφού ολοκληρώθηκε η διαδικασία δημιουργίας των αποθηκευμένων αναζητήσεων της εφαρμογής Twitter-Splunk Mobile μένει να γίνουν αλλαγές στα αρχεία του κώδικα της εφαρμογής Splunk Mobile ώστε να οριστούν τα ονόματα των αναζητήσεων για να εμφανίζονται στο Interface της εφαρμογής.

1. Στο αρχείο Home.html του Splunk Mobile πληκτρολογούμε την ονομασία που θέλουμε να έχουν οι επιλογές στο αρχικό μενού της εφαρμογής στο κομμάτι του κώδικα όπως παρατίθεται παρακάτω. Οι δύο αυτές επιλογές θα ονομαστούν στην προκειμένη περίπτωση Tweet Searches και New Search.



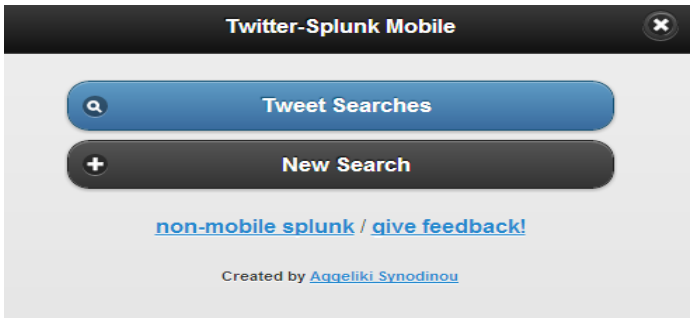
Εικόνα 13 Αλλαγές στο αρχείο Home.html του Splunk Mobile

2. Στο αρχείο Searches.html όπως παρουσιάζεται στην εικόνα προσθέτουμε τα ονόματα των αποθηκευμένων αναζητήσεων που δημιουργήσαμε για να εμφανίζονται στο μενού επιλογών αναζητήσεων.



Εικόνα 14 Αλλαγές στο αρχείο Searches.html του Splunk Mobile

3. Αφού αποθηκεύσουμε τις αλλαγές και πραγματοποιήσουμε επανεκκίνηση στο Splunk, ανοίγουμε την εφαρμογή Splunk Mobile και όπως αυτή έχει διαμορφωθεί ύστερα από τις αλλαγές που πραγματοποιήσαμε.



Εικόνα 15 Twitter-Splunk Mobile Interface Main Menu

Εικόνα 16 Twitter-Splunk Mobile Interface Μενού επιλογών

II.Ανάπτυξη σε Android

Για την ανάπτυξη και εξομοίωση της εφαρμογής στη συσκευή χρησιμοποιήθηκε το περιβάλλον ανάπτυξης Eclipse με το ADT (Android Development Toolkit) plugin. Η εφαρμογή αναπτύχθηκε για την έκδοση 4.2.2 του Android, στη συσκευή Nexus 7(7.27'' 800x1280 tvdpi).

Εργαλεία συστήματος

Eclipse

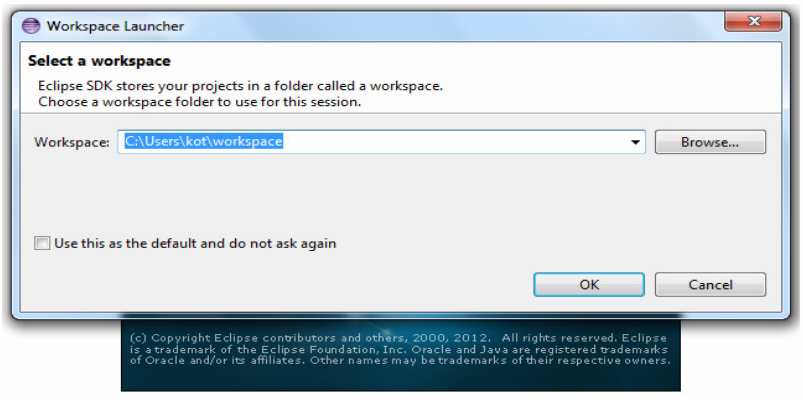
Το Eclipse είναι το εργαλείο με τη χρήση του οποίου έγινε η ανάπτυξη της εφαρμογής στην φορητή συσκευή. Αρχικά ο χρήστης πρέπει να «κατεβάσει» το ολοκληρωμένο σύστημα ανάπτυξης (έκδοση 4.2) από τον παρακάτω σύνδεσμο:

http://www.eclipse.org/downloads/

Για να λειτουργήσει το Eclipse χρειάζεται να υπάρχει εγκατεστημένο το JDK (Java Development Kit). Αν ο χρήστης δεν έχει κάποιο JDK (τρέχουσα έκδοση 7) εγκατεστημένο στον υπολογιστή του μπορεί να το κατεβάσει από το σύνδεσμο:

http://www.oracle.com/technetwork/java/javase/downloads/index.html

Το σύστημα δεν απαιτεί κάποιου είδους εγκατάσταση. Αρκεί ο χρήστης να τρέξει το εκτελέσιμο αρχείο για να γίνει η εκκίνησή του. Τη στιγμή της εκκίνησης ζητείται από τον χρήστη να επιλέξει τον χώρο εργασίας (workspace) δηλαδή το φάκελο του συστήματος μέσα στον οποίο θα αποθηκεύονται τα projects που δημιουργεί όπως φαίνεται και στο παρακάτω σχήμα:



Εικόνα 17 Οθόνη Εκκίνησης Eclipse

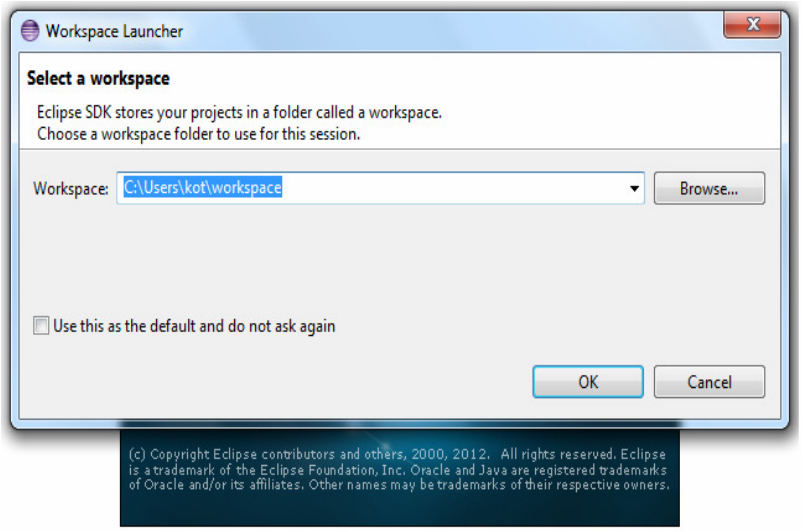
ADT και Android SDK

Μετά την επιλογή του χώρου εργασίας το Eclipse ολοκληρώνει την εκκίνησή του. Προκειμένου ο χρήστης να μπορέσει να αναπτύξει κάποια εφαρμογή για το Android πρέπει να εγκαταστήσει το plugin ADT ενώ πρέπει να «κατεβάσει» και το SDK του Android. Το SDK είναι διαθέσιμο από το σύνδεσμο:

http://developer.android.com/sdk/index.html

Σε ότι αφορά το Android, το plugin που χρησιμοποιείται ονομάζεται **Android Developers Tools** ***(ADT)*** και προσφέρει ένα ισχυρό περιβάλλον στο οποίο οικοδομούνται οι Android εφαρμογές. Το ADT επεκτείνει τις δυνατότητες του Eclipse, προκειμένου να επιτρέπεται στους προγραμματιστές να ρυθμίζουν εύκολα νέα έργα Android, να δημιουργούν UIs, να προσθέτουν στοιχεία βασισμένα στο Android API, να διορθώνουν τα σφάλματα χρησιμοποιώντας τα εργαλεία του Android SDK και τέλος να εξάγουν τα **apk** αρχεία προκειμένου να διανείμουν την εφαρμογή τους.

Ο χρήστης πρέπει να αποσυμπιέσει το συμπιεσμένο αρχείο σε κάποια τοποθεσία και να προσθέσει την τοποθεσία του φακέλου *platform-tools/* του SDK στο PATH του συστήματος. Προσθέτοντας τον φάκελο *platform-tools/* στο PATH του συστήματος ο χρήστης έχει τη δυνατότητα να εκτελέσει το Android Debug Bridge (adb) και άλλα εργαλεία της γραμμής εντολών χωρίς να είναι απαραίτητο να παρέχει κάθε φορά όλο το μονοπάτι στον φάκελο *platform-tools/*. Το σημείο προσθήκης του φακέλου εξαρτάται από την προτίμηση του χρήστη.



Εικόνα 18 Οθόνη εκκίνησης Eclipse

Στη συνέχεια ο χρήστης καλείται να εγκαταστήσει το ADT plugin στο Eclipse ακολουθώντας τα παρακάτω βήματα:

1. Στο μενού του Eclipse, επιλογή **Help → Install New Software…**

2. Επιλογή **Add** στην πάνω δεξιά γωνία.

3. Στο παράθυροο διαλόγου Add Repository που θα ανοίξει εισαγωγή "ADT Plugin" στο πεδίο *Name* και του ακόλουθου συνδέσμου στο πεδίο *Location:*

https://dl-ssl.google.com/android/eclipse/

4. Επιλογή **OK.**

5. Στο παράθυρο διαλόγου Available Software που εμφανίζεται, επιλογή του κουτιού δίπλα στο Developer Tools και επιλογή **Next**.

6. Επιλογή **Next** στο επόμενο παράθυρο, όπου παρουσιάζεται μία λίστα με τα εργαλεία προς εγκατάσταση.

7. Προσεκτικό διάβασμα και αποδοχή των συμφωνιών παραχώρησης άδειας και επιλογή **Finish**.

8. Όταν η εγκατάσταση ολοκληρωθεί, αποδοχή για επανεκκίνηση του Eclipse.

Το επόμενο βήμα είναι η τροποποίηση των ρυθμίσεων του ADT στο Eclipse ώστε να εμφανίζεται ο φάκελος του Android SDK:

1. Επιλογή **Window →Preferences** για το άνοιγμα του πίνακα ρυθμίσεων.

2. Επιλογή **Android** από την αριστερή στήλη.

3. Στο πεδίο *SDK Location* στο κύριο παράθυρο, επιλογή **Browse** για εντοπισμό του φακέλου του SDK.

4. Επιλογή **Apply** και έπειτα **OK**.

Αν μέχρι εδώ δεν έχουν προκύψει προβλήματα, τότε η εγκατάσταση του plugin έχει ολοκληρωθεί με επιτυχία. Μετά την ολοκλήρωση των παραπάνω διαδικασιών μένει ένα ακόμα βήμα ώστε να μπορέσει ο προγραμματιστής να αρχίσει την ανάπτυξη εφαρμογών σε Android.

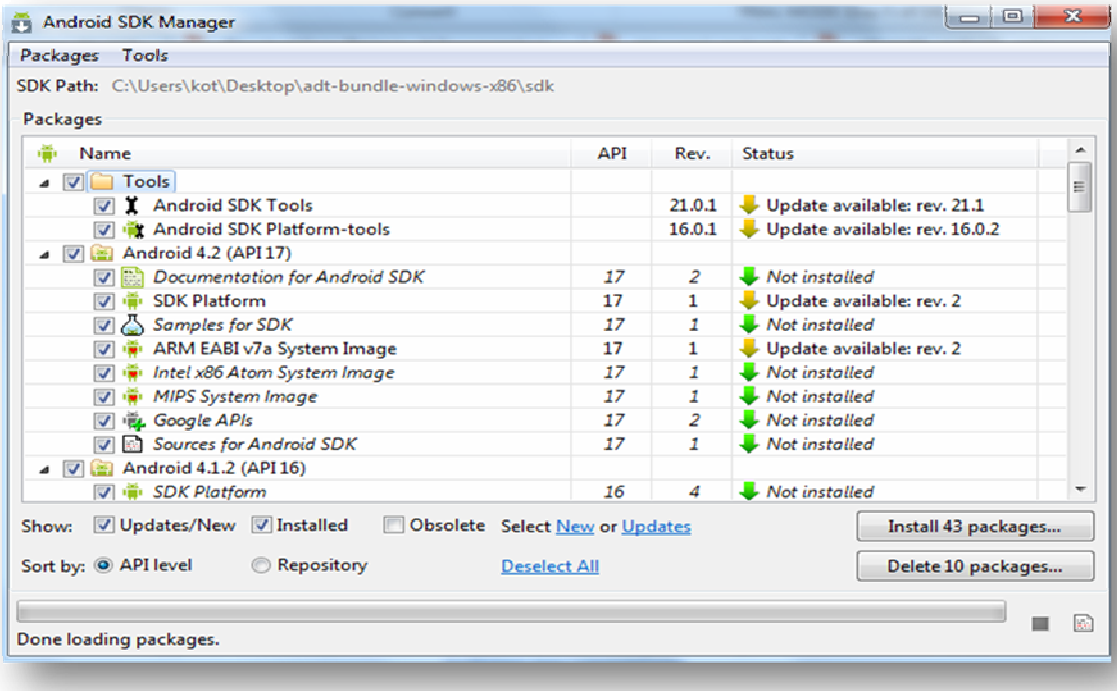
Ο χρήστης πρέπει να ρυθμίσει κατάλληλα το SDK μέσω του εργαλείου Android SDK Manager και να εγκαταστήσει τα απαραίτητα πακέτα στο περιβάλλον ανάπτυξης. Το SDK είναι δομημένο έτσι ώστε να μπορεί να ξεχωρίζει τα κύρια τμήματά του – τις εκδόσεις της πλατφόρμας, τα add-ons, τα εργαλεία, τον κώδικα και τις οδηγίες για την χρήση των APIs – σε ένα σύνολο ξεχωριστών προς εγκατάσταση πακέτων. Όταν ο χρήστης κατεβάζει το SDK πακέτο, αυτό περιλαμβάνει μόνο την τελευταία έκδοση των εργαλείων του Android. Για την ανάπτυξη οποιασδήποτε εφαρμογής για το Android ο χρήστης πρέπει να έχει εγκατεστημένη μια τουλάχιστον έκδοσης της πλατφόρμας στο περιβάλλον ανάπτυξης. Το SDK παρέχει τους παρακάτω τύπους πακέτων:

- **SDK εργαλεία** – Περιέχει εργαλεία για την αποσφαλμάτωση και τη δοκιμή του κώδικα καθώς και άλλα χρήσιμα εργαλεία. Τα εργαλεία λαμβάνουν συνεχείς ενημερώσεις ανά τακτά χρονικά διαστήματα.
- **SDK εργαλεία πλατφόρμας** – Περιέχει εργαλεία, που εξαρτώνται από την πλατφόρμα, για την ανάπτυξη και αποσφαλμάτωση της εφαρμογής. Αυτά τα εργαλεία υποστηρίζουν τα πιο πρόσφατα χαρακτηριστικά της πλατφόρμας Android και ενημερώνονται όταν μία καινούρια έκδοση γίνει διαθέσιμη.
- **Πλατφόρμες Android** – Κάθε πλατφόρμα περιλαμβάνει μία πλήρως συμβατή βιβλιοθήκη του Android μαζί με ένα αρχείο εικόνας του συστήματος, δείγματα κώδικα και έναν εξομοιωτή. Μία πλατφόρμα του SDK είναι διαθέσιμη για κάθε έκδοση του Android που έχει παραχθεί για φορητές συσκευές που βασίζονται σε αυτό.
- **Πρόγραμμα οδήγησης USB για Windows** – Περιέχει αρχεία οδήγησης τα οποία εγκαθίστανται σε έναν υπολογιστή έτσι ώστε να μπορεί να εκτελέσει αποσφαλμάτωση και άλλες λειτουργίες των εφαρμογών σε πραγματική συσκευή.
- **Δείγματα κώδικα** – Περιέχει δείγματα κώδικα και εφαρμογές διαθέσιμες για κάθε έκδοση του Android, ώστε να μπορεί να τις χρησιμοποιεί ο χρήστης σαν οδηγό για τη δημιουργία της δικής του εφαρμογής.
- **Documentation** – Περιέχει ένα τοπικό αντίγραφο των τελευταίων οδηγιών για την χρήση του πλαισίου των APIs για όλες τις εκδόσεις του Android.
- **Add-ons –** Περιέχει πακέτα ανεπτυγμένα από τρίτους, τα οποία επιτρέπουν τη δημιουργία περιβάλλοντος ανάπτυξης που χρησιμοποιεί μία εξωτερική Android βιβλιοθήκη ή ένα προσαρμοσμένο σύστημα Android.

Υπάρχουν 3 τρόποι για να αποκτήσει κάποιος πρόσβαση στο εργαλείο Android SDK Manager:

Για να μεταβεί ο χρήστης στο εργαλείο Android SDK Manager ακολουθεί το εξής βήμα:

- Από το περιβάλλον ανάπτυξης Eclipse, επιλογή **Window > Android SDK Manager**.


Android SDK Manager
Packages Tools
SDK Path: C:\Users\kot\Desktop\adt-bundle-windows-x86\sdk
Packages
Name API Rev. Status
Tools
Android SDK Tools 21.0.1 Update available: rev. 21.1
Android SDK Platform-tools 16.0.1 Update available: rev. 16.0.2
Android 4.2 (API 17)
Documentation for Android SDK 17 2 Not installed
SDK Platform 17 1 Update available: rev. 2
Samples for SDK 17 1 Not installed
ARM EABI v7a System Image 17 1 Update available: rev. 2
Intel x86 Atom System Image 17 1 Not installed
MIPS System Image 17 1 Not installed
Google APIs 17 2 Not installed
Sources for Android SDK 17 1 Not installed
Android 4.1.2 (API 16)
SDK Platform 16 4 Not installed
Show: Updates/New Installed Obsolete Select New or Updates
Install 43 packages...
Sort by: API level Repository
Deselect All
Delete 10 packages...
Done loading packages.

Δημιουργία Εξομοιωτή και νέου project

Σε αυτήν την ενότητα παρουσιάζεται ο τρόπος εκτέλεσης μίας εφαρμογής στον Εξομοιωτή (emulator) της πλατφόρμας Android. Αρχικά, πρέπει να γίνει η δημιουργία ενός Android Virtual Device (AVD) που εξομοιώνει το σύστημα στο οποίο θα τρέξει η εφαρμογή μαζί με τις ρυθμίσεις της συσκευής. Η δημιουργία ενός AVD γίνεται ως εξής:

1. Στο περιβάλλον Eclipse, επιλογή **Window > AVD Manager**.

2. Επιλογή **New** πάνω δεξιά στο παράθυρο με τη λίστα των AVDs που άνοιξε.

3. Επιλογή ονόματος του AVD, όπως “splunk_mobile”.

4. Επιλογής πλατφόρμας, δηλαδή επιλογή έκδοσης του Android που θα τρέχει στον εξομοιωτή.

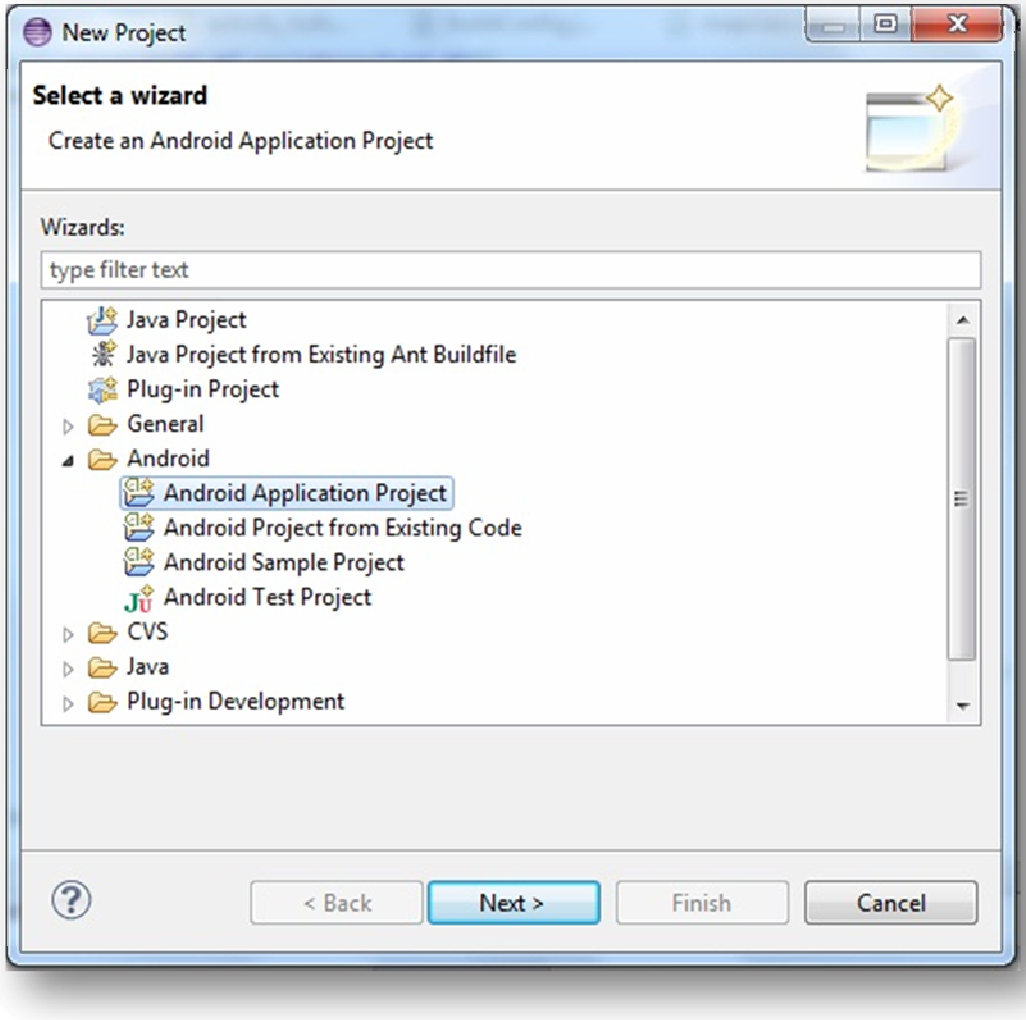
5. Προαιρετικά, επιλογή μεγέθους της εξωτερικής (SD) κάρτας και της ανάλυσης της οθόνης.

6. Επιλογή του υλικού (hardware) που θα υποστηρίζει ο εξομοιωτής.

7. Επιλογή **Create AVD**.

Αφού έχει δημιουργηθεί το AVD, το επόμενο βήμα είναι η δημιουργία ενός νέου Android project στο Eclipse:

1. Στο Eclipse, επιλογή **File > New > Project** Αν το ADT Plugin έχει εγκατασταθεί σωστά, το παράθυρο διαλόγου που θα εμφανιστεί θα πρέπει να έχει έναν φάκελο ονομαζόμενο *Android* που θα περιέχει την επιλογή *Android Application Project*.

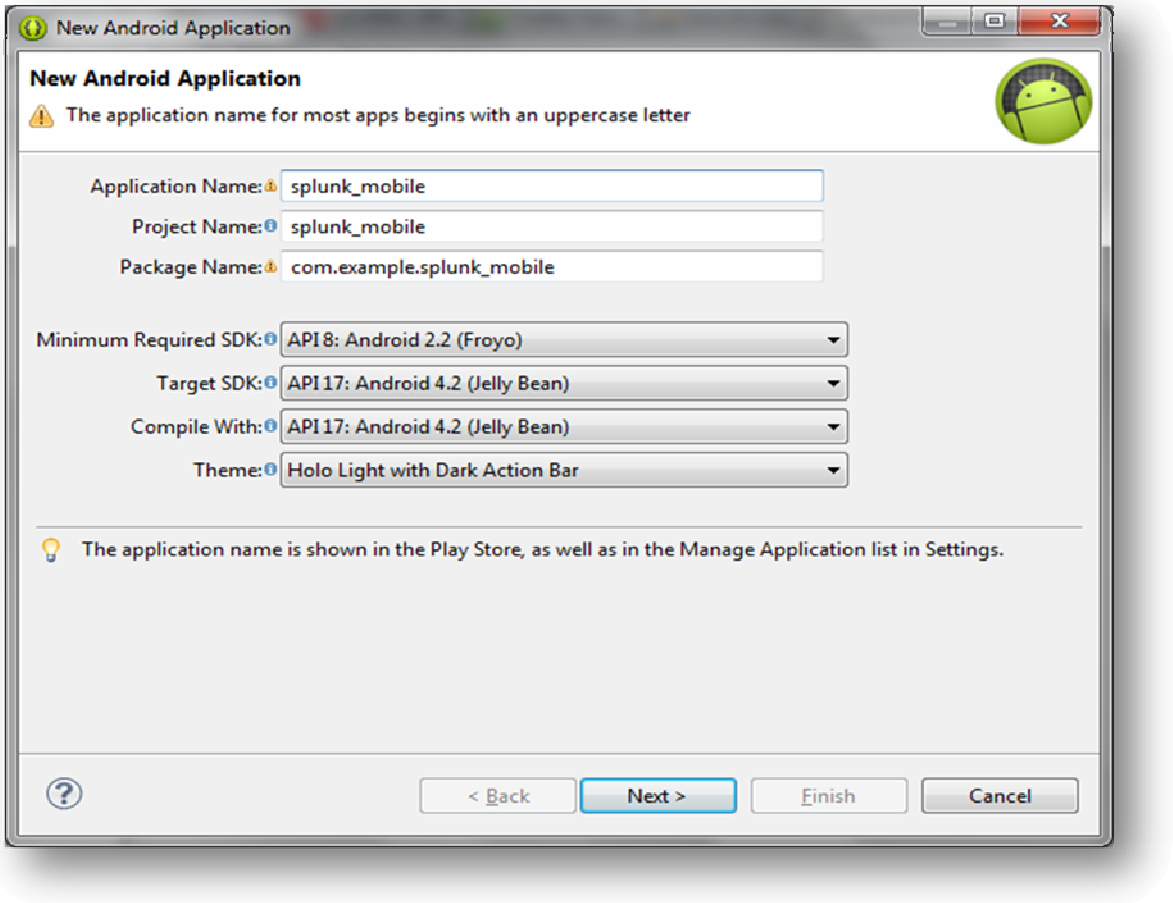


2. Επιλογή *Android Application Project* και **Next**.

3. Αν ο χρήστης επιθυμεί να δημιουργήσει ένα καινούριο project (create new project in workspace) τότε πρέπει να συμπληρώσει το πεδίο *Project Name*, στη συνέχεια να επιλέξει **Next,** να επιλέξει το *Target Name* (έκδοση της πλατφόρμας του Android), να επιλέξει πάλι **Next** και να συμπληρώσει τα ακόλουθα πεδία στο νέο παράθυρο:

- Application Name
- Package Name
- Create Activity

Το πεδίο Minimum SDK συμπληρώνεται σύμφωνα με την επιλογή του *Target Name* στο προηγούμενο παράθυρο. Τέλος, επιλέγοντας **Finish** ολοκληρώνεται η δημιουργία του project.



Ακολουθεί επεξήγηση του κάθε πεδίου:

Application Name

Αυτός είναι ο τίτλος της εφαρμογής.

Project Name

Αυτό είναι το όνομα του project στο Eclipse – το όνομα του φακέλου που περιέχει τα αρχεία του project.

Package Name

Αυτός είναι ο χώρος ονομάτων του πακέτου που θα έχουν όλα τα αρχεία του πηγαίου κώδικα. Το όνομα του πακέτου πρέπει να είναι μοναδικό ανάμεσα σε όλα τα πακέτα που είναι αποθηκευμένα στο σύστημα Android. Γι' αυτόν το λόγο είναι σημαντικό να διατηρείται ένα συγκεκριμένο πλαίσιο ονομάτων για τις εφαρμογές.

Create Activity

Αυτό είναι το όνομα της κλάσης που θα παραχθεί από το plugin και θα είναι μία υποκλάση της κλάσης *Activity* του Android. Συνήθως αποτελεί την αρχική οθόνη της εφαρμογής.

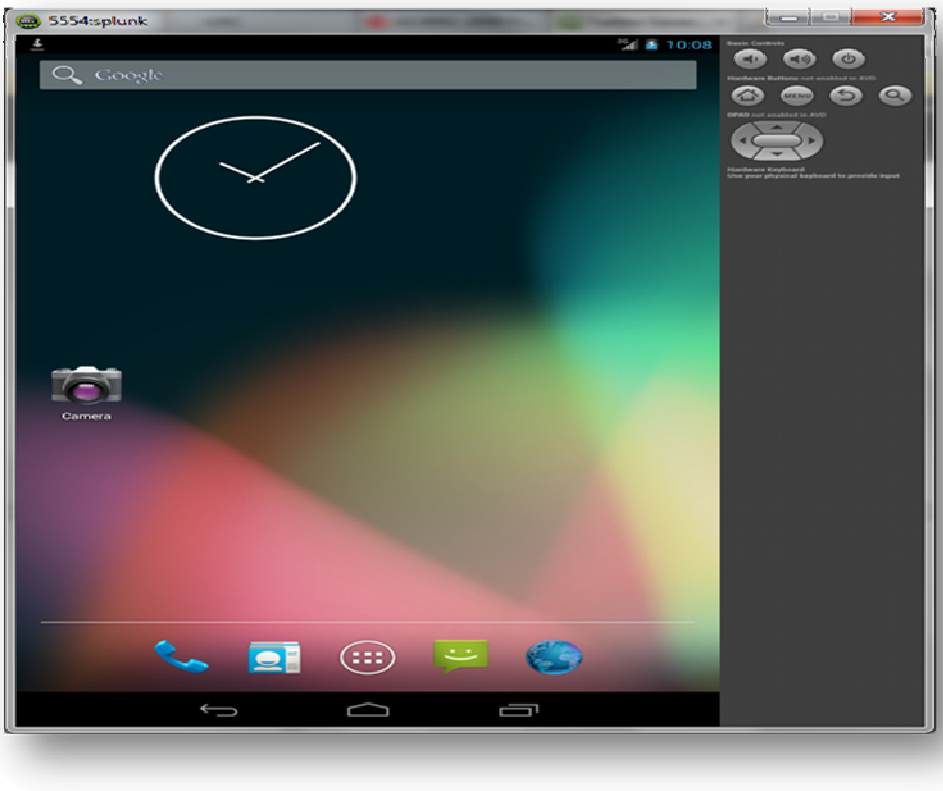
Min SDK Version

Προσδιορίζει τη μικρότερη δυνατή έκδοση του API που απαιτείται για να εκτελεστεί η εφαρμογή. Αφού η εφαρμογή έχει δημιουργηθεί και έχει μεταφραστεί χωρίς λάθη, είναι έτοιμη να τρέξει. Για να πραγματοποιηθεί αυτό ο χρήστης πρέπει να ακολουθήσει τα παρακάτω βήματα:

1. Επιλογή του project στην αριστερή στήλη του Eclipse.

2. Δεξί κλικ στο project, επιλογή **Run As > Android Application**.

Πραγματοποιείται εκκίνηση του εξομοιωτή, ο οποίος χρειάζεται μερικά λεπτά (ανάλογα με τις δυνατότητες κάθε υπολογιστή) για να φορτώσει όλες τις ρυθμίσεις και να είναι έτοιμος προς χρήση. Παρακάτω απεικονίζεται ένα στιγμιότυπο του:



Ανάπτυξη εφαρμογής

Οι εφαρμογές Android αναφορικά με λειτουργίες και δεδομένα ορίζουν ένα πρόγραμμα και δεν διαφέρουν. Παρακάτω αναφέρονται τα σημαντικότερα στοιχεία κατασκευής εφαρμογών Android και επισημαίνεται η ορολογία Android.

- ***Activity (Δραστηριότητα):*** *Αποτελεί θεμέλιο λίθο σε μια εφαρμογή Android.* Η Activity μέσα σε μία εφαρμογή έχει ένα και μοναδικό σκοπό ή αναλαμβάνει μια μοναδική εργασία. Ένα σύνολο εργασιών εμπεριέχονται σε μία εφαρμογή Android. Μάλιστα τις περισσότερες φορές, για κάθε οθόνη στην εφαρμογή μας, ορίζεται και υλοποιείται μια κλάση Activity.
- ***Intent (Πρόθεση):*** Προκειμένου να ανταπεξέλθει, με την κατάλληλη Activity, σε αιτήσεις εργασιών ,το λειτουργικό σύστημα Android χρησιμοποιεί ένα ασύγχρονο μηχανισμό αποστολής/παραλαβής μηνυμάτων. Ως μια Intent νοείται κάθε αίτηση, την οποία μπορείτε να εκλάβετε ως ένα μήνυμα που δηλώνει μία πρόθεση για να συμβεί κάτι.
- ***Service (Υπηρεσία):*** Μία υπηρεσία μπορεί να εκτελέσει εργασίες που δεν απαιτούν την αλληλεπίδραση με τον χρήστη. Όσο περισσότερο διαρκούν οι λειτουργίες, χωρίς βέβαια να συνυπολογίζεται ο χρόνος επεξεργασίας ή πραγματοποιούνται τακτικά, όπως ο έλεγχος διακομιστών για νέα αλληλογραφία, τόσο πιο χρήσιμη είναι η υπηρεσία.

Context – Activity

Η διαχείριση λεπτομερειών ρύθμισης παραμέτρων για συγκεκριμένες εφαρμογές, οι λειτουργίες και τα δεδομένα για μια ολόκληρη εφαρμογή αναλαμβάνονται από την κλάση Context. Επίσης με χρήση αυτής προσπελαύνονται ρυθμίσεις και πόροι που μοιράζονται σε πολλαπλά στιγμιότυπα Activity. Όμως η κλάση Activity προέρχεται από την κλάση Context και έτσι μπορούμε να χρησιμοποιήσουμε την Activity αντί να ανακτήσουμε με ρητό τρόπο το Context της

εφαρμογής. Ωστόσο αν το χρησιμοποιήσετε πολλές φορές αυτό, υπάρχει κίνδυνος διαρροών μνήμης

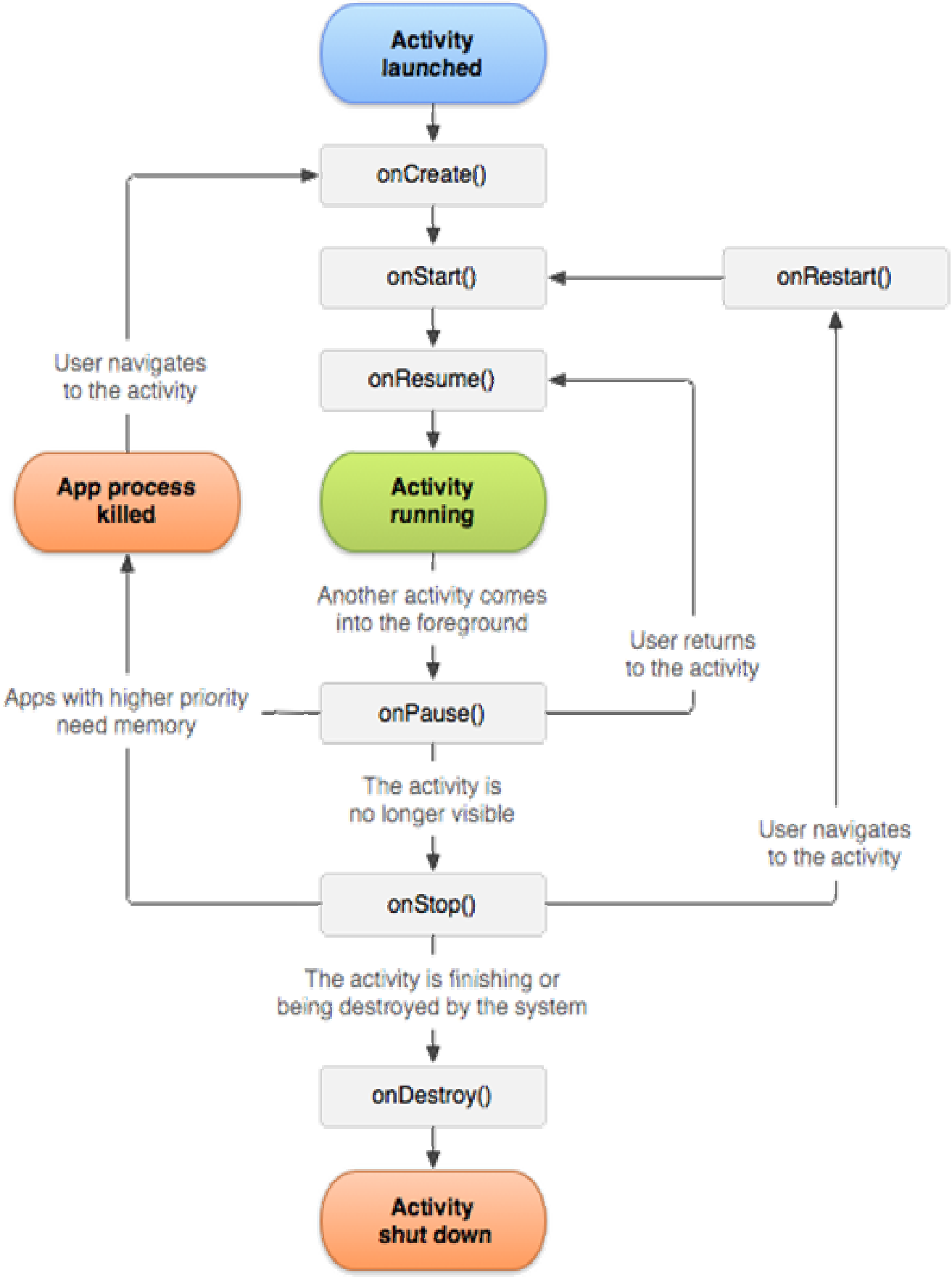
Κύκλος ζωής μίας Activity του Android

Το λειτουργικό σύστημα Android επιτρέπει σε διαφορετικές εφαρμογές να εκτελούνται ταυτόχρονα , οι οποίες περιλαμβάνουν διαφορετικές διεργασίες εφόσονβέβαια υπάρχει επεξεργαστική ισχύς και διαθέσιμη μνήμη. Στο προσκήνιο στο χρήστη κάθε φορά υπάρχει ορατή μόνο μία ενεργή εφαρμογή - Activity. Παρ' όλα αυτά στο παρασκήνιο μπορούν να υπάρχουν άλλες διεργασίες και όταν υπάρχουν συμβάντα οι εφαρμογές μπορούν να παύονται και να διακόπτονται, όπως για παράδειγμα μ' ένα εισερχόμενο μήνυμα.

Όλα τα αντικείμενα Activity παρακολουθούνται και τοποθετούνται σε μια στοίβα από το λειτουργικό σύστημα Android. Ανάστροφες κλίσεις μεθόδων προκαλούν αλλαγές κατάστασης μέσα στον κύκλο ζωής μίας Activity.

Οι πιο βασικές μέθοδοι για την ανάστροφη κλήση Activity είναι:

```
public class MyActivity extends Activity {
protected void onCreate(Bundle savedInstanceState);
    protected void onStart();
    protected void onRestart();
    protected void onResume();
    protected void onPause();
    protected void onStop();
                        protected void onDestroy();
                                }
```



Εικόνα 19 Ο κύκλος ζωής μιας Activity στο Android

Επεξήγηση

Καλείται η μέθοδος onCreate(), όταν μία Activity ξεκινά για πρώτη φορά. Σε αυτή την φάση που μόλις πρωτοξεκινά το Bundle, το οποίο έχει την τιμή null είναι η μόνη παράμετρος της onCreate(). Σε περίπτωση που για λόγους απελευθέρωσης μνήμης σταματήσει και ανακινηθεί η Activity, το Bundle της περιέχει πληροφορίες της προηγούμενης κατάστασης προκειμένου να μπορεί να ξεκινήσει πάλι. Η ρύθμιση παραμέτρων, όπως για τη σύνδεση δεδομένων και για τη διάταξη – κλήσεις στη μέθοδο setContentView() μπορεί να γίνει στη μέθοδο onCreate(). Με την onResume() γίνεται αρχικοποίηση και ανάκτηση δεδομένων δραστηριοτήτων και είναι το κατάλληλο σημείο για έναρξη βίντεο, ήχου και κινήσεων. Με την onPause() γίνεται διακοπή, αποθήκευση και απελευθέρωση δεδομένων δραστηριοτήτων. Με την μέθοδο ανάστροφης κλήσης onSaveInstanceState(), η Activity μπορεί να αποθηκεύσει πληροφορίες κατάστασης σ' ένα αντικείμενο Bundle. Ωστόσο, για ουσιαστικές επιβολές δεδομένων πρέπει να χρησιμοποιείται η μέθοδος onPause() καθώς δεν είναι εγγυημένη σε όλες τις περιπτώσεις η κλήση της onSaveInstanceState(). Με την onDestroy() γίνεται καταστροφή στατικών δεδομένων δραστηριότητας δηλαδή όταν η Activity καταστρέφεται, γίνεται κλήση της μεθόδου αυτής. Με τις μεθόδους startActivity() και finish() ο χρήστης μπορεί να επιστρέψει σε στιγμιότυπα Activity που εμφανίζονται και έπειτα καταργούνται μόνιμα όταν εκτελείται η δραστηριότητα της οθόνης χωρίς να επανεκκινήσεις την εφαρμογή.

Τέτοιο παράδειγμα Activity είναι η οθόνη εκκίνησης της εφαρμογής. Ένας τρόπος για να ξεκινήσουμε διάφορες δραστηριότητες είναι με την μέθοδο startActivity(new Intent(getApplicationContext()), MyaDrawActivity.class). Αναφορικά, διατίθεται η δυνατότητα, μέσω Intent για παράδειγμα, εκκίνηση μιας δραστηριότητας που ανήκει σε άλλη εφαρμογή ενώ εκτελείται η δικιά μας. Επίσης η εφαρμογή μας θα μπορούσε να στέλνει και να ανιχνεύει αντικείμενα Intent για την ενημέρωση του γενικότερου συστήματος, πχ η μπαταρία εξαντλείται, ήρθε ένα email.

Κλάσεις Activity και View

Τα βασικά δομικά υλικά οποιασδήποτε εφαρμογής Android είναι οι κλάσεις Activity και View. Με μια οθόνη διεπαφής χρήστη, η οποία αποτελείται από αντικείμενα όψης View, η κάθε Activity εκτελεί μία συγκεκριμένη εργασία μέσα στην εφαρμογή.

Το αρχείο manifest

Προτού το σύστημα μπορέσει να εκκινήσει ένα συστατικό μίας εφαρμογής, πρέπει να γνωρίζει την ύπαρξη του συστατικού. Γι' αυτό, οι εφαρμογές δηλώνουν τα συστατικά τους σε ένα αρχείο που καλείται manifest και συμπεριλαμβάνεται στο Android πακέτο, δηλαδή στο .apk αρχείο που περιέχει τον πηγαίο κώδικα, τα αρχεία και τους άλλους πόρους της εφαρμογής. Το manifest είναι ένα δομημένο XML αρχείο που πάντα έχει την ονομασία AndroidManifest.xml για όλες τις εφαρμογές. Πέρα από το να δηλώνει τα συστατικά της εφαρμογής χρησιμοποιείται για τη δήλωση των βιβλιοθηκών που χρειάζεται η εφαρμογή για να λειτουργήσει ενώ προσδιορίζει και τα δικαιώματα πρόσβασης που αναμένει να έχει.

Επεξεργασία του αρχείου AndroidManifest

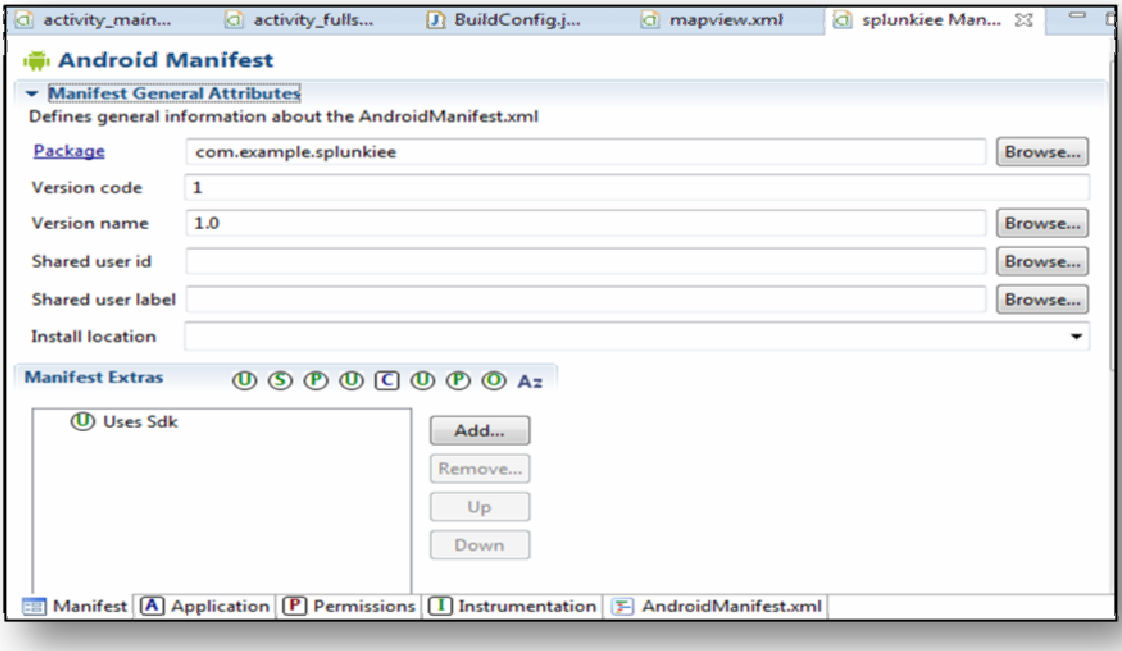
Μπορούμε τα τροποποιήσουμε το αρχείο manifest είτε χειροκίνητα είτε χρησιμοποιώντας τον επεξεργαστή πόρων Eclipse Manifest. Ο επεξεργαστή πόρων Eclipse Manifest χωρίζει της πληροφορίες του manifest ανά κατηγορία. Έτσι έχουμε τις εξής καρτέλες:

1. Manifest
2. Application (Εφαρμογή)
3. Permissions (Δικαιώματα)

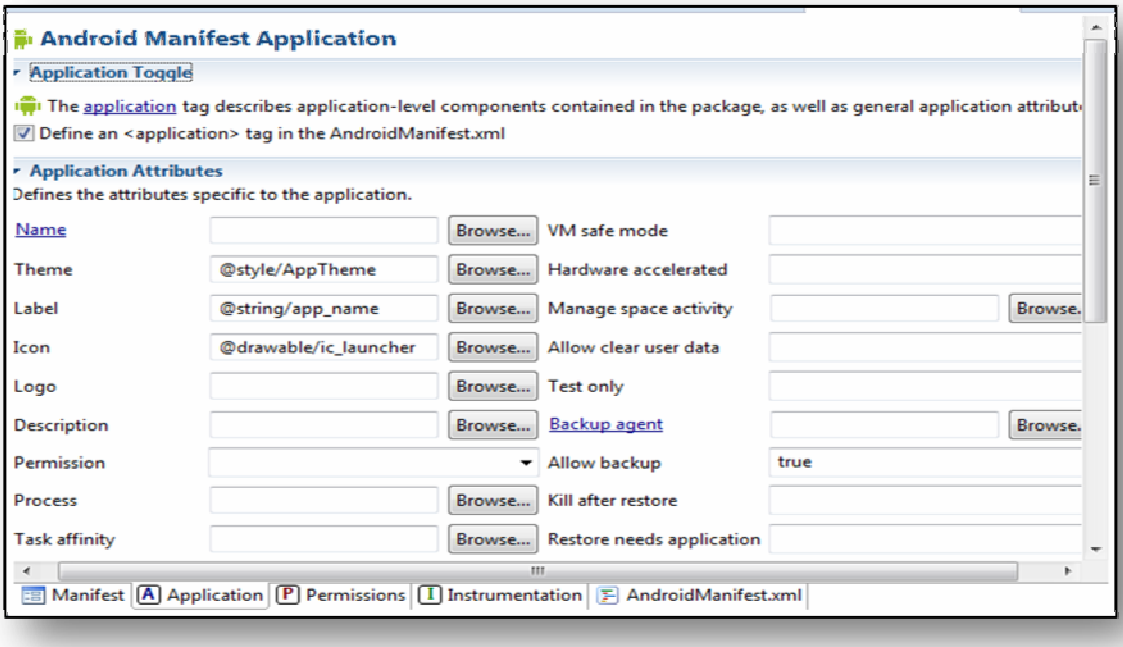
4. Instrumentation(Συσκευές)

5. AndroidManifest.xml

Όπως γίνεται φανερό από την εικόνα2.3 η καρτέλα Manifest εμπεριέχει πληροφορίες για ρυθμίσεις που επεκτείνονται σε όλο το πακέτο σχετικά με το όνομα του, με την έκδοση, με το Android SDK που υποστηρίζεται. Επιπλέον μπορούμε να ορίσουμε εδώ απαιτήσεις για το υλικό ή τα χαρακτηριστικά.



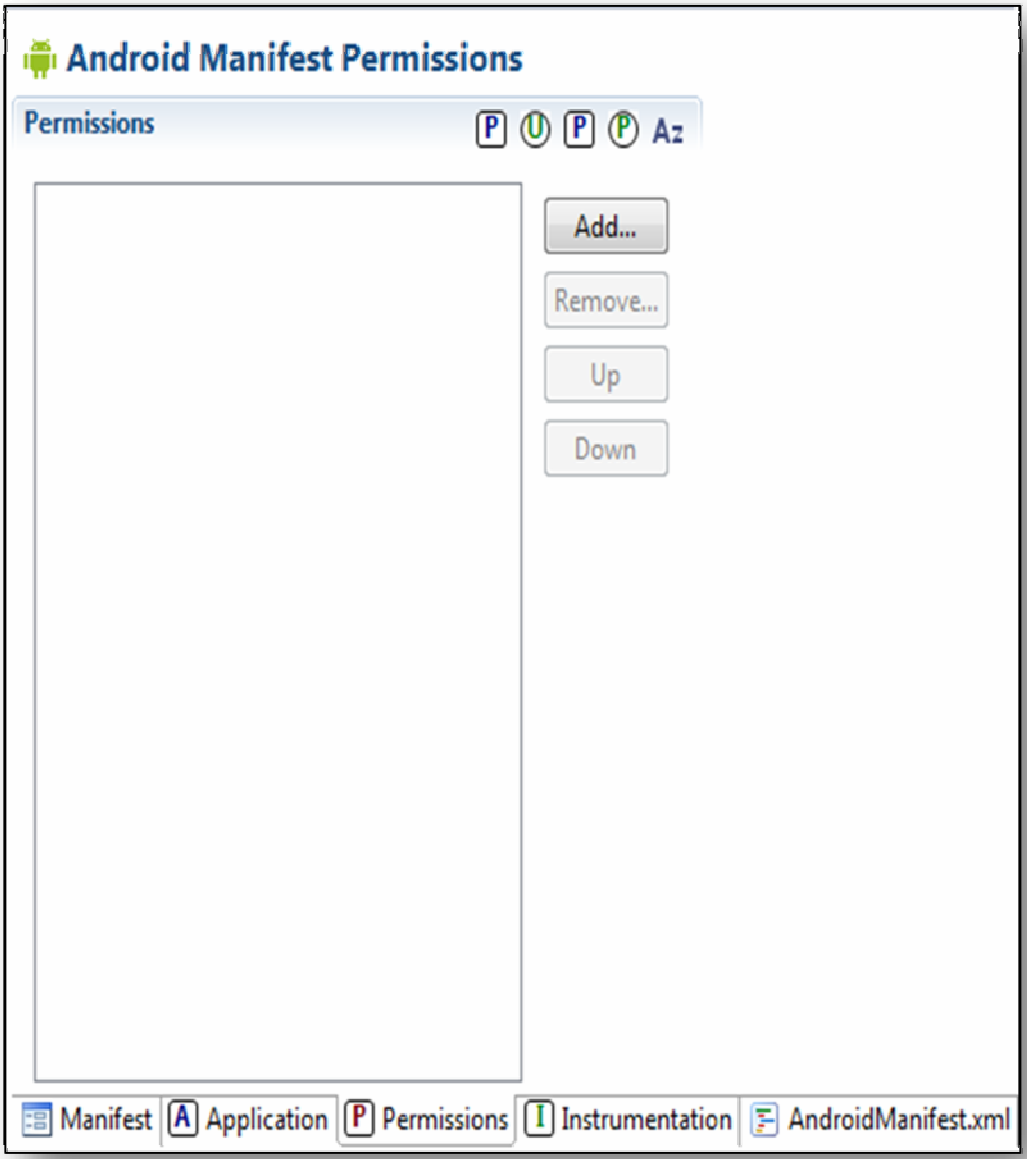
Εικόνα 10 Η καρτέλα του Manifest



Εικόνα 21 Η καρτέλα του Application

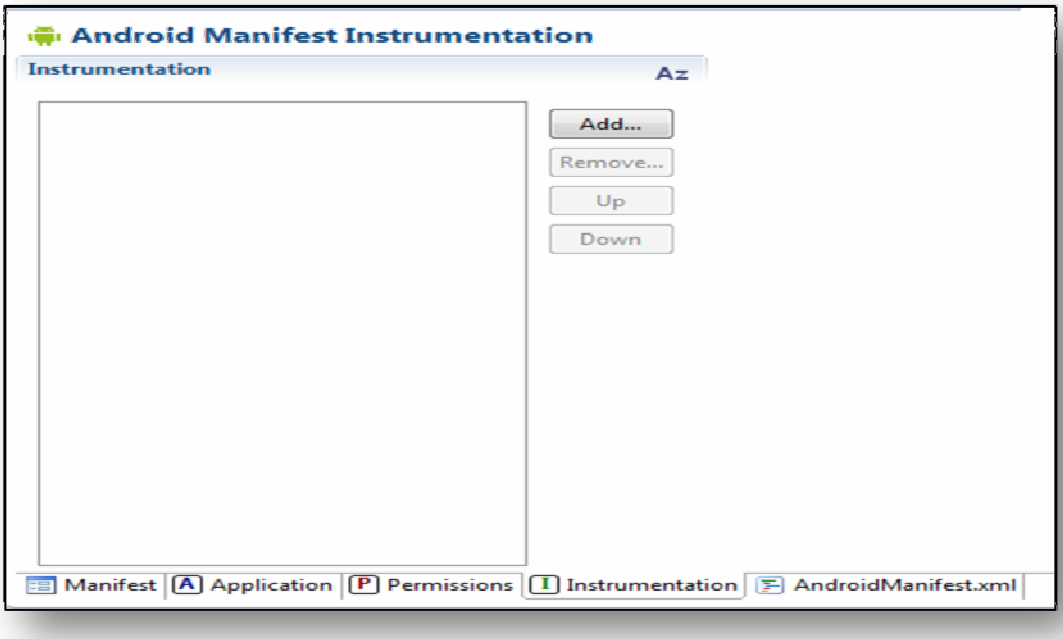
Η καρτέλα Application εμπεριέχει πληροφορίες για ρυθμίσεις που επεκτείνονται σε ολόκληρη την εφαρμογή σχετικά με την ετικέτα και το εικονίδιό της, με τα στοιχεία της εφαρμογής (πάροχοι υλικού, φίλτρα προθέσεων, δραστηριότητες, ρυθμίσεις για

υπηρεσίες).



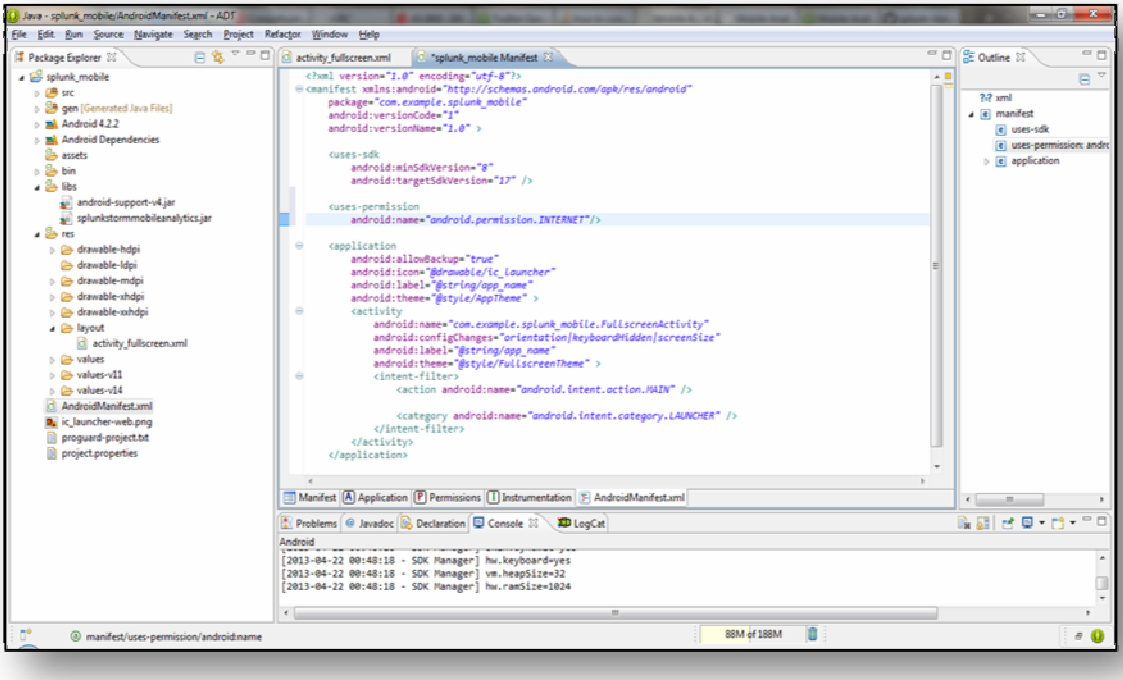
Εικόνα 21 Η καρτέλα Permissions

Η καρτέλα Permissions εμπεριέχει κανόνες δικαιωμάτων για την εκτέλεση από την εφαρμογή μας και μπορεί επίσης να χρησιμοποιηθεί για την επιβολήπροσαρμοσμένων δικαιωμάτων για την εφαρμογή.



Εικόνα 22 Η καρτέλα Instrumentation (Eclipse)

Η καρτέλα Instrumentation παρέχει στον προγραμματιστή την δυνατότητα να δηλώνει κατηγορίες συσκευών για την παρακολούθηση της εφαρμογής.



Εικόνα 23 Η καρτέλα AndroidManifest.xml (Eclipse)

Η καρτέλα AndroidManifest παρέχει την δυνατότητα χειροκίνητης επεξεργασίας του manifest του Android. Ας δούμε πιο αναλυτικά στο παρακάτω αρχείο της εφαρμογής Twitter-Splunk Mobile:

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="com.example.splunk_mobile"
    android:versionCode="1"
    android:versionName="1.0" >

    <uses-sdk
        android:minSdkVersion="8"
        android:targetSdkVersion="17" />

<uses-permission
        android:name="android.permission.INTERNET"/>

    <application
        android:allowBackup="true"
        android:icon="@drawable/ic_launcher"
        android:label="@string/app_name"
        android:theme="@style/AppTheme" >
        <activity
            android:name="com.example.splunk_mobile.MainActivity"
            android:label="@string/app_name" >
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />

                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
    </application>
</manifest>
```

Όπως παρατηρούμε:

- Το αρχείο manifest περιλαμβάνει μια μόνο ετικέτα, <manifest> και <application>.

- Το όνομα πακέτου της εφαρμογής είναι *com.example.splunk_mobile*

- Η εφαρμογή έχει κωδικό έκδοσης 1.

- Η εφαρμογή έχει έκδοση 1.0.

- Στον κατάλογο */res/android*, όπου στην πραγματικότητα υπάρχουν πολλαπλές εκδόσεις για διαφορετικές πυκνότητες pixel, αποθηκεύεται το εικονίδιο της εφαρμογής που είναι ένα εικονίδιο γραφικών icon. Το εικονίδιο αυτό μπορεί να είναι ένα αρχείο PNG,JPG ή GIF.
- Η δραστηριότητα, η οποία ξεκινά όταν ο χρήστης κάνει κλικ στο εικονίδιο της εφαρμογής είναι η *.splunk_mobile.*Αυτό ορίζεται αφού ρυθμίσουμε το φίλτρο προθέσεων χρησιμοποιώντας την ετικέτα <intent-filter> με τον τύπο ενέργειας MAIN και την κατηγορία LAUNCHER.

Συνοπτικά λοιπόν, θα μπορούσαμε να πούμε ότι μέσω του manifest του Android, οι προγραμματιστές μπορούν να ορίσουν τα εξής:

- Τις υποστηριζόμενες από την εφαρμογή εκδόσεις Android SDK.
- Τα χρησιμοποιούμενα από την εφαρμογή χαρακτηριστικά της πλατφόρμας Android.
- Με ποιες βιβλιοθήκες συνδέεται η εφαρμογή.
- Τις απαιτούμενες από την εφαρμογή ρυθμίσεις υλικού Android.
- Τα υποστηριζόμενα από την εφαρμογή μεγέθη οθονών και πυκνότητες pixel.

Τα βήματα που πρέπει να ακολουθήσουμε για τη δημιουργία της εφαρμογής σε Android είναι απλά. Στο αρχείο Manifest του Project προσθέτουμε σύμφωνα με τις οδηγίες εγκατάστασης του Splunk Mobile την εντολή για να επιτρέπεται η πρόσβαση της εφαρμογής στο Internet:

```
<uses-permission

android:name="android.permission.INTERNET"/>
```

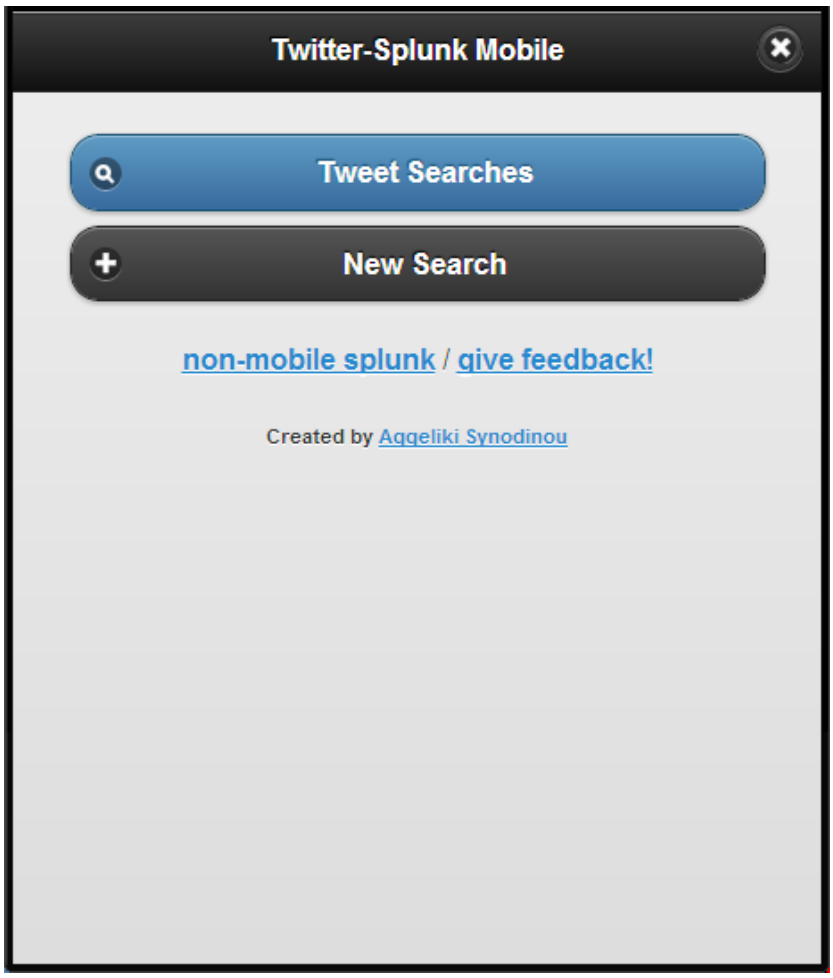
Στη MainActivity του Project εισάγουμε την εντολή:

```
import com.splunk.android.Splunk;
```

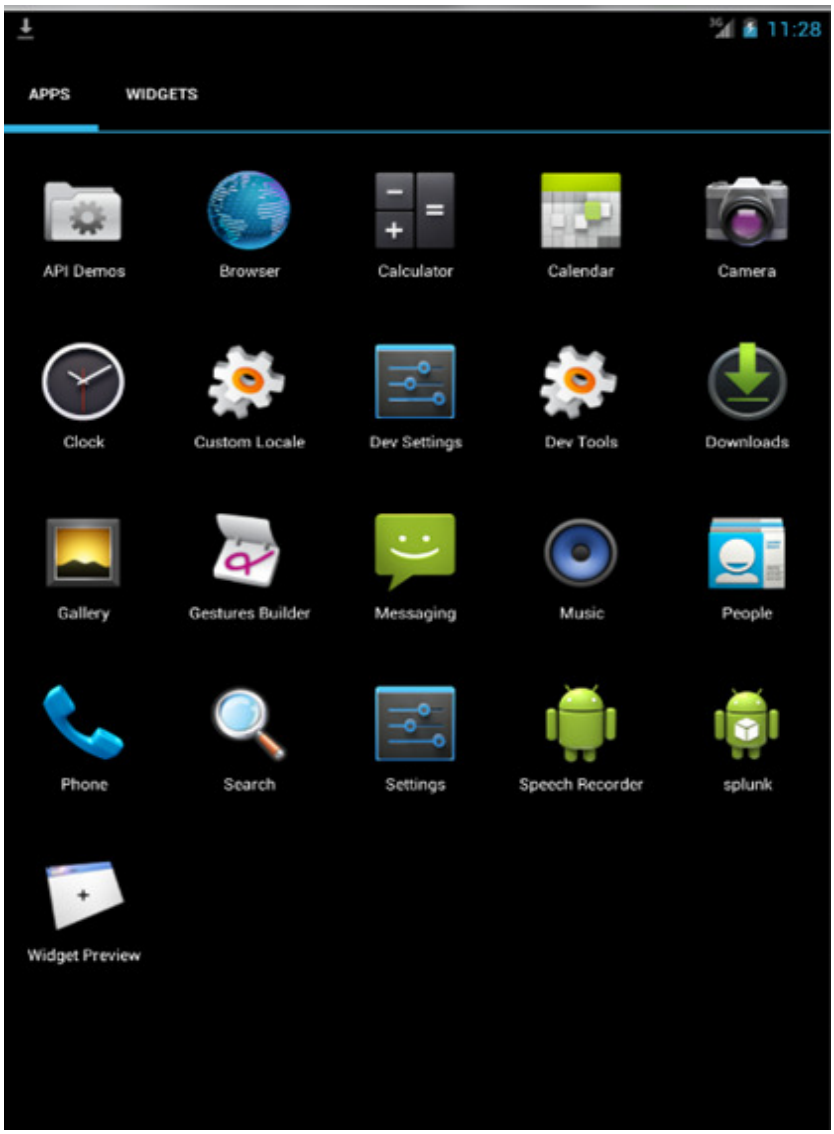
Στη MainActivity προσθέτουμε τη μέθοδο OnCreate() για να συνδεθεί η εφαρμογή μας με το Twitter-Splunk Mobile:

```
protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main);
    Splunk.connect("https://192.168.132.68:8032", "admin",
"passcode", getApplicationContext());
```

Αφού ολοκληρώσουμε αυτές τις αλλαγές επιλέγουμε την εφαρμογή ,κάνουμε δεξί κλικ→Run as→ Android Application και η εφαρμογή αρχίζει να τρέχει με τη βοήθεια της εικονικής μηχανής AVD όπως βλέπουμε στην εικόνα παρακάτω.



Εικόνα 24 Εκτέλεση Twitter-Splunk Moblie με το ADV

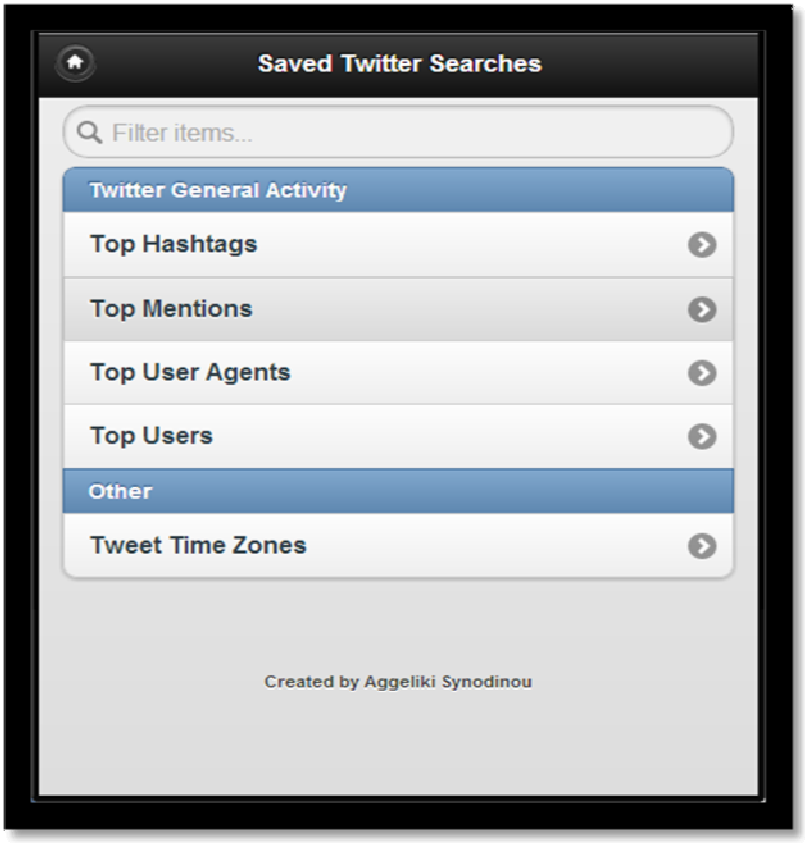


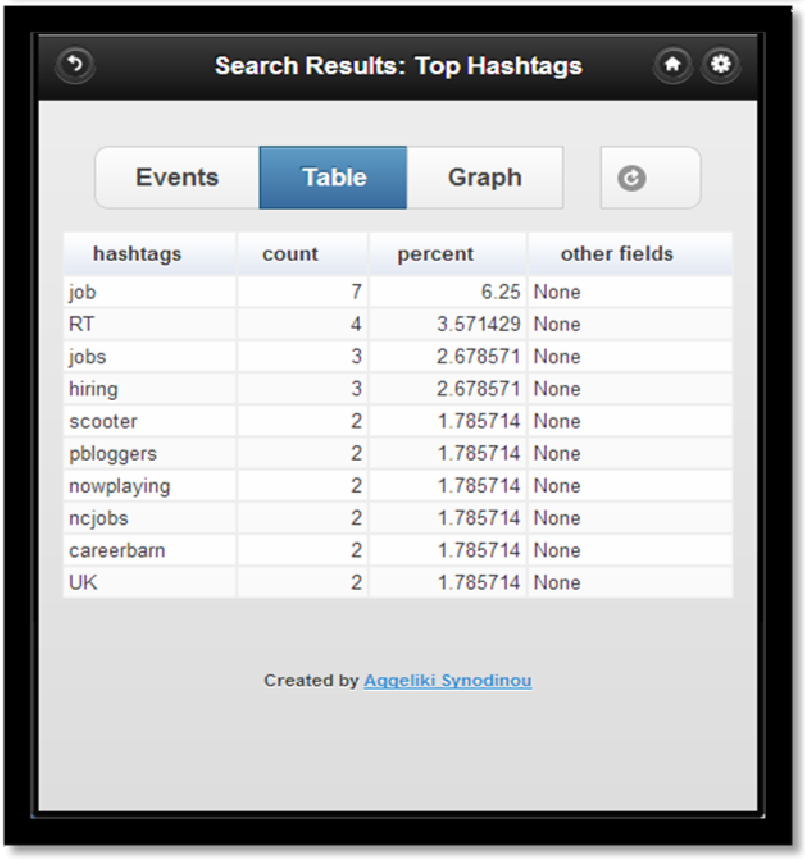
Εικόνα 25 Μενού εφαρμογών εξομοιωτή-Εικονίδιο Εφαρμογής

Εφαρμογή Twitter-Splunk Mobile

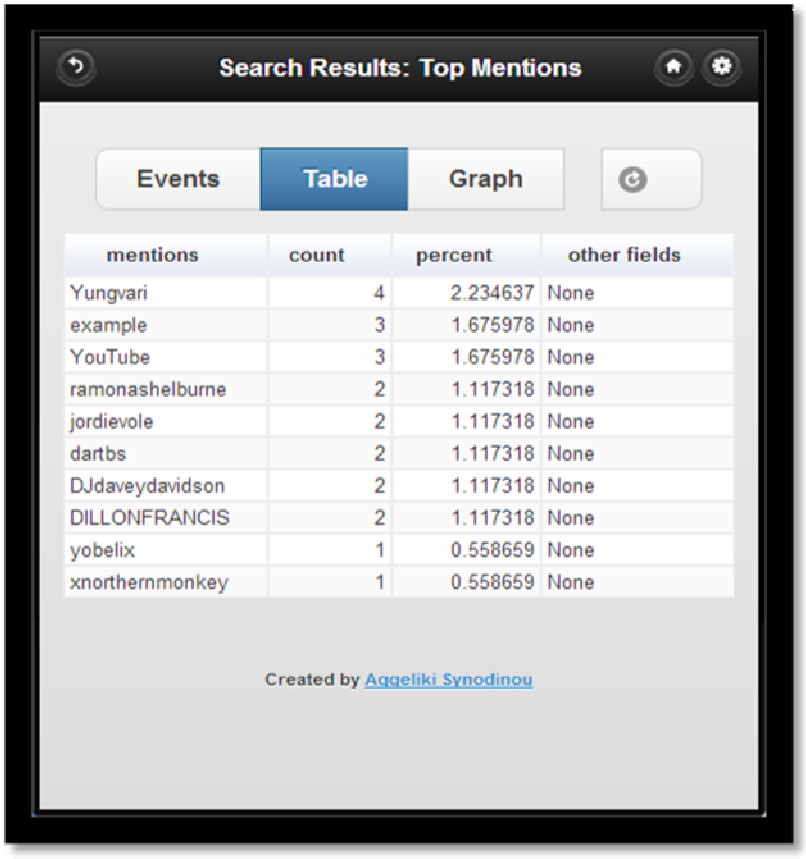
Αυτή η εφαρμογή που υλοποιήθηκε κατά τη διάρκεια εκπόνησης της πτυχιακής επικοινωνεί με το εργαλείο Splunk κάνοντας ανταλλαγή δεδομένων μέσω web σε ένα Android app προκειμένου να έχει πρόσβαση ο χρήστης στο app που έχει δημιουργηθεί πάνω στην πλατφόρμα ανάλυσης και να μπορεί να τη χρησιμοποιεί ώστε να λαμβάνει αναλύσεις και γραφικά σχετικά με data feeds του Twitter.

Ακολουθούν εικόνες της εφαρμογής:





hashtags	count	percent	other fields
job	7	6.25	None
RT	4	3.571429	None
jobs	3	2.678571	None
hiring	3	2.678571	None
scooter	2	1.785714	None
pbloggers	2	1.785714	None
nowplaying	2	1.785714	None
ncjobs	2	1.785714	None
careerbarn	2	1.785714	None
UK	2	1.785714	None

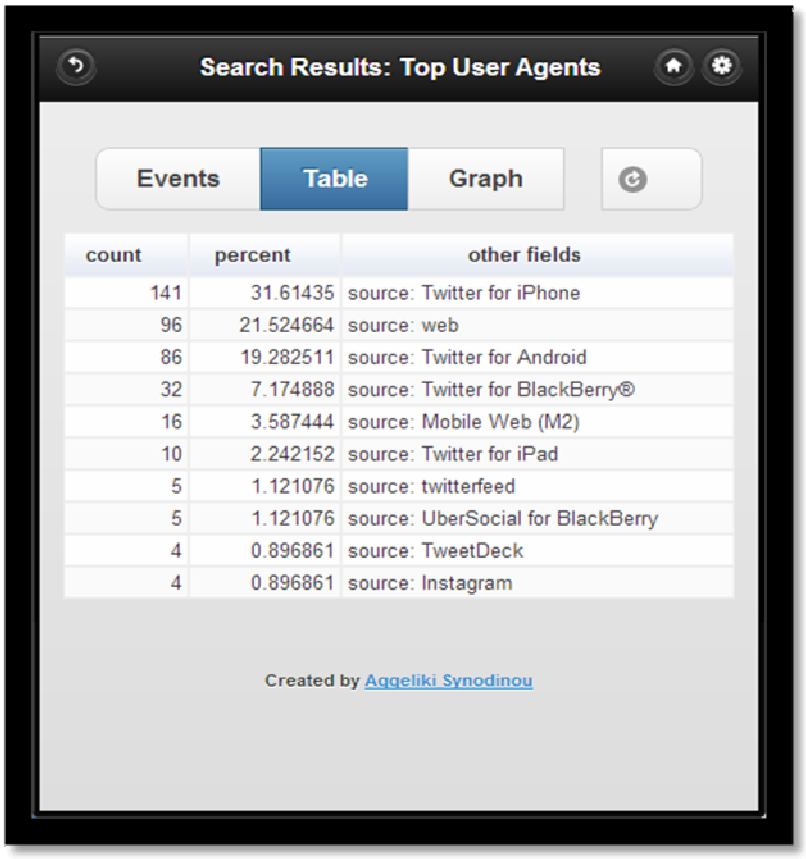


Search Results: Top Mentions

Events | Table | Graph

mentions	count	percent	other fields
Yungvari	4	2.234637	None
example	3	1.675978	None
YouTube	3	1.675978	None
ramonashelburne	2	1.117318	None
jordievole	2	1.117318	None
dartbs	2	1.117318	None
DJdaveydavidson	2	1.117318	None
DILLONFRANCIS	2	1.117318	None
yobelix	1	0.558659	None
xnorthernmonkey	1	0.558659	None

Created by Aggeliki Synodinou

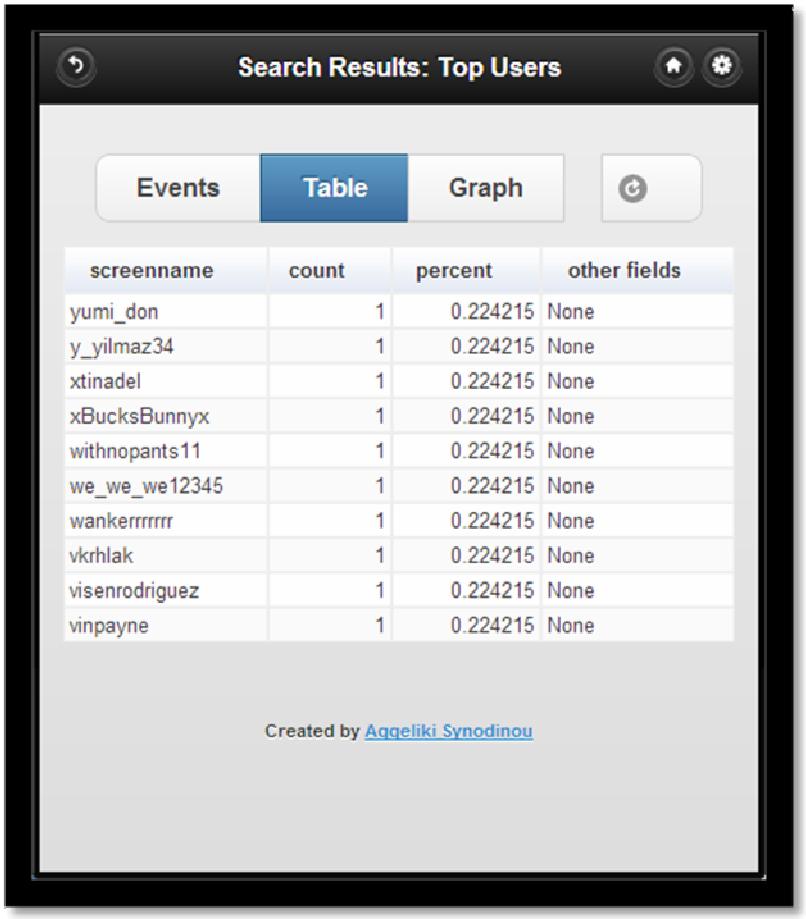


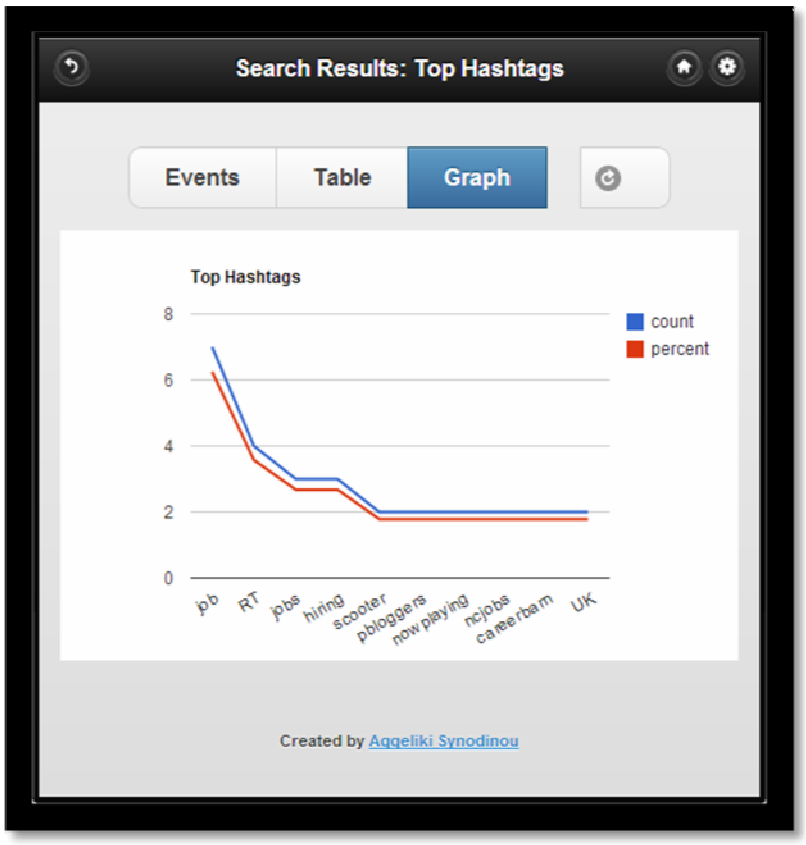
Search Results: Top User Agents

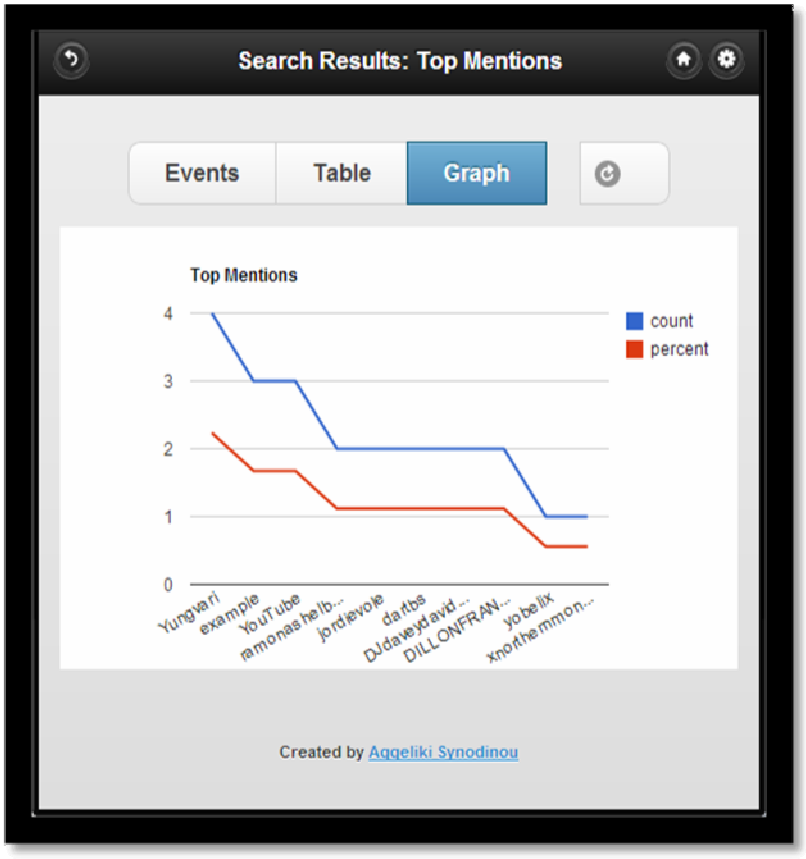
Events | Table | Graph

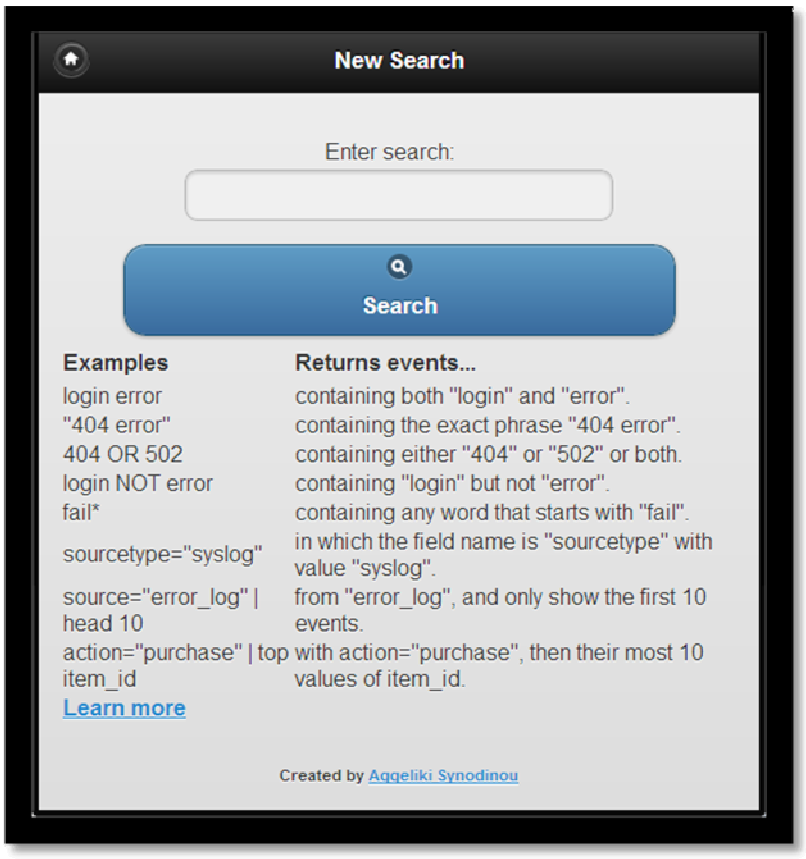
count	percent	other fields
141	31.61435	source: Twitter for iPhone
96	21.524664	source: web
86	19.282511	source: Twitter for Android
32	7.174888	source: Twitter for BlackBerry®
16	3.587444	source: Mobile Web (M2)
10	2.242152	source: Twitter for iPad
5	1.121076	source: twitterfeed
5	1.121076	source: UberSocial for BlackBerry
4	0.896861	source: TweetDeck
4	0.896861	source: Instagram

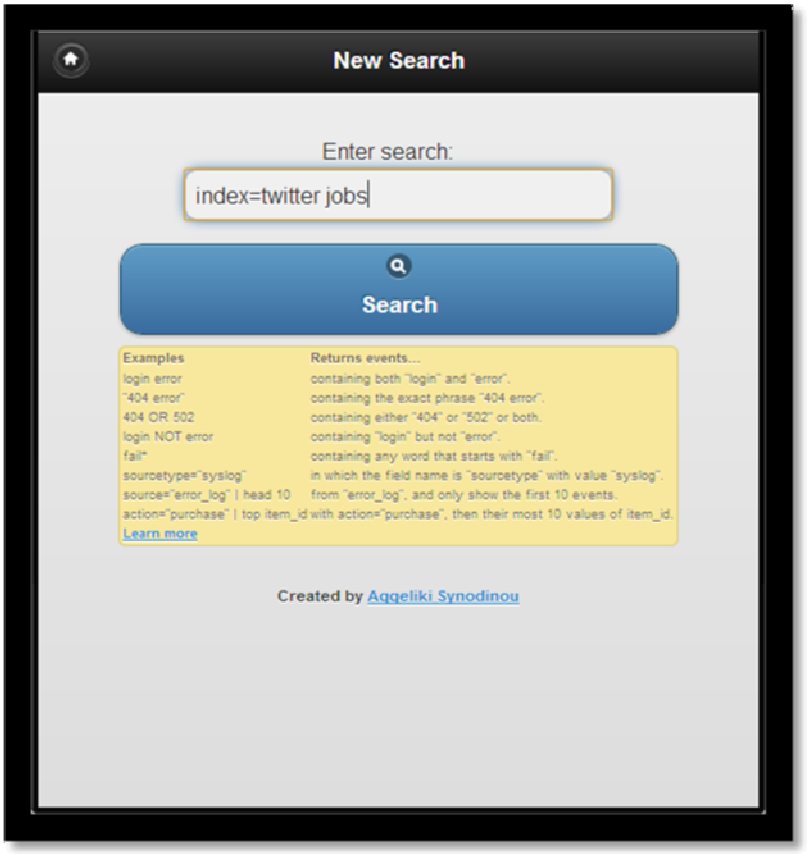
Created by Aggeliki Synodinou

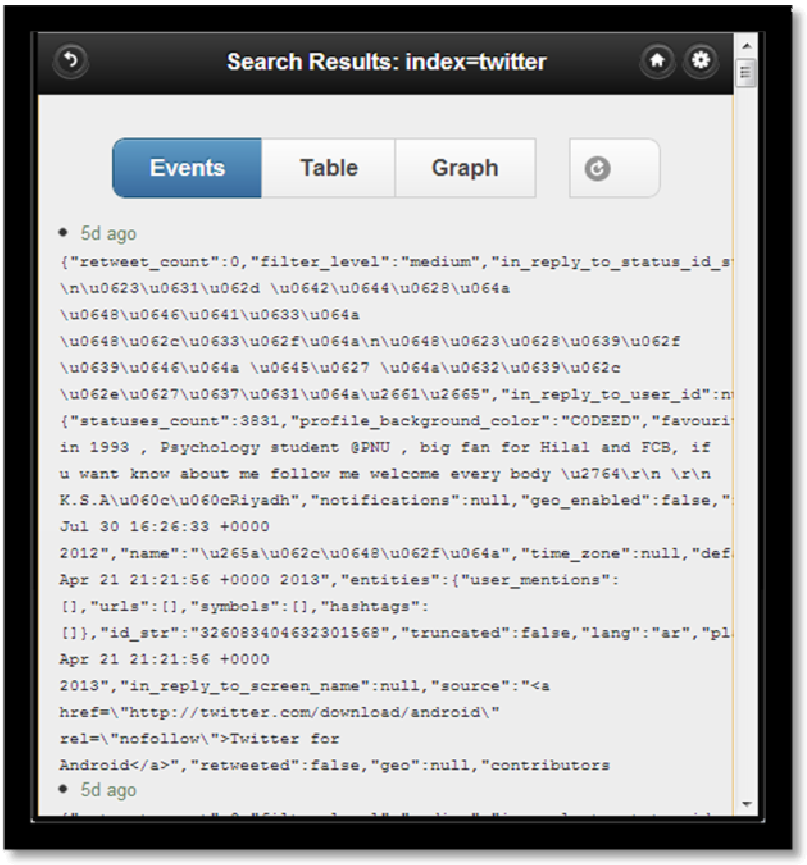

Search Results: Top Users
Events
Table
Graph
screenname
count
percent
other fields
yumi_don 1 0.224215 None
y_yilmaz34 1 0.224215 None
xtinadel 1 0.224215 None
xBucksBunnyx 1 0.224215 None
withnopants11 1 0.224215 None
we_we_we12345 1 0.224215 None
wankerrrrrrr 1 0.224215 None
vkrhlak 1 0.224215 None
visenrodriguez 1 0.224215 None
vinpayne 1 0.224215 None
Created by Aggeliki Synodinou


Search Results: Top Hashtags
Events
Table
Graph
Top Hashtags
count
percent
8
6
4
2
0
job
RT
jobs
hiring
scooter
pbloggers
now playing
ncjobs
careerbarn
UK
Created by Aggeliki Synodinou


Search Results: Top Mentions
Events
Table
Graph
Top Mentions
count
percent
4
3
2
1
0
Yungvari
example
YouTube
ramonashelb...
jordievole
darbs
DJdaweydavid...
DILLONFRAN...
yobelix
xnorthernmon...
Created by Aggeliki Synodinou


New Search
Enter search:
Search
Examples
Returns events...
login error
containing both "login" and "error".
"404 error"
containing the exact phrase "404 error".
404 OR 502
containing either "404" or "502" or both.
login NOT error
containing "login" but not "error".
fail*
containing any word that starts with "fail".
sourcetype="syslog"
in which the field name is "sourcetype" with value "syslog".
source="error_log" | head 10
from "error_log", and only show the first 10 events.
action="purchase" | top item_id
with action="purchase", then their most 10 values of item_id.
Learn more
Created by Aggeliki Synodinou


New Search
Enter search:
index=twitter jobs
Search
Examples
Returns events...
login error
containing both "login" and "error".
"404 error"
containing the exact phrase "404 error".
404 OR 502
containing either "404" or "502" or both.
login NOT error
containing "login" but not "error".
fail*
containing any word that starts with "fail".
sourcetype="syslog"
in which the field name is "sourcetype" with value "syslog".
source="error_log" | head 10
from "error_log", and only show the first 10 events.
action="purchase" | top item_id
with action="purchase", then their most 10 values of item_id.
Learn more
Created by Aggeliki Synodinou


Search Results: index=twitter
Events
Table
Graph
5d ago
{"retweet_count":0,"filter_level":"medium","in_reply_to_status_id_s
\n\u0623\u0631\u062d \u0642\u0644\u0628\u064a
\u0648\u0646\u0641\u0633\u064a
\u0648\u062c\u0633\u062f\u064a\n\u0648\u0623\u0628\u0639\u062f
\u0639\u0646\u064a \u0645\u0627 \u064a\u0632\u0639\u062c
\u062e\u0627\u0637\u0631\u064a\u2661\u2665","in_reply_to_user_id":n
{"statuses_count":3831,"profile_background_color":"C0DEED","favouri
in 1993 , Psychology student @PNU , big fan for Hilal and FCB, if
u want know about me follow me welcome every body \u2764\r\n \r\n
K.S.A\u060c\u060cRiyadh","notifications":null,"geo_enabled":false,"
Jul 30 16:26:33 +0000
2012","name":"\u265a\u062c\u0648\u062f\u064a","time_zone":null,"def
Apr 21 21:21:56 +0000 2013","entities":{"user_mentions":
[],"urls":[],"symbols":[],"hashtags":
[]},"id_str":"326083404632301568","truncated":false,"lang":"ar","pl
Apr 21 21:21:56 +0000
2013","in_reply_to_screen_name":null,"source":"<a
href=\"http://twitter.com/download/android\"
rel=\"nofollow\">Twitter for
Android","retweeted":false,"geo":null,"contributors
5d ago

Κεφάλαιο 5

Συμπεράσματα και προτάσεις για μελλοντική ανάπτυξη

Το κοινωνικό δίκτυο Twitter έχει γνωρίσει μεγάλη ανάπτυξη και αποτελεί μια από τις πιο κορυφαίες σελίδες κοινωνικής δικτύωσης. Η επίδραση που είχε στην κοινωνία αποτελεί απόδειξη για το πόσο δημοφιλές είναι. Λόγω λοιπόν αυτής της μαζικής προτίμησης και χρήσης του, τα δεδομένα που διακινούνται στην υπηρεσία είναι πάρα πολλά αλλά συγχρόνως πολύ σημαντικά.

Η άμεση πρόσβαση σε επίκαιρες πληροφορίες καθιστά αναγκαία την συνεχή ενημέρωση των χρηστών δικτύων κοινωνικών δικτύων όπως το twitter, γεγονός που έχει οδηγήσει πάρα πολλούς κατασκευαστές smart phones, να ενσωματώσουν εφαρμογές κοινωνικών δικτύων στα κινητά τους.

Η εφαρμογή κινούμενη προς αυτή την κατεύθυνση έχει σκοπό να συλλέξει δεδομένα από το Twitter μέσω του εργαλείου αναζήτησης και ανάλυσης Splunk και να τα επιστρέψει στην οθόνη της φορητής συσκευής του χρήστη, κρατώντας τον διαρκώς ενημερωμένο για τις πιο ενδιαφέρουσες εξελίξεις και τάσεις που συμβαίνουν στο αγαπημένο του κοινωνικό δίκτυο.

Η εφαρμογή Twitter -Splunk Mobile παρόλο που είναι μια ολοκληρωμένη εφαρμογή έχει ακόμα πολλά περιθώρια ανάπτυξης. Μερικές κατευθύνσεις για μελλοντική της επέκταση είναι:

- Πρώτον να δημιουργηθεί προσαρμογή οριζόντιου προσανατολισμού της οθόνης ώστε να εμφανίζονται μεγαλύτερα τα γραφήματα.

- Προσθήκη alerts σύμφωνα με προκαθορισμένα κριτήρια όπως λέξεις-κλειδιά.

- Μια ακόμα ενδιαφέρουσα επέκταση της εφαρμογής θα ήταν να επεκταθεί το μενού και να προσφέρει τη δυνατότητα επιλογής κοινωνικού δικτύου. Παραδείγματα τέτοιας επέκτασης θα μπορούσαν να είναι το Facebook, το οποίο είναι εξίσου δημοφιλές με το Twitter καθώς και το LinkedIn, το οποίο είναι ιδιαίτερα διαδεδομένο

στον επιχειρηματικό κόσμο. Η λήψη δεδομένων και η δημιουργία αποθηκευμένων αναζητήσεων μπορεί να υλοποιηθεί εύκολα βάση των ήδη υπαρχόντων πόρων.

Παράρτημα

Παρακάτω παρατίθενται οι εντολές αναζήτησης του Splunk που χρησιμοποιήθηκαν στα κεφάλαια 2 & 4 και εξηγούνται:

Εντολή	**Περιγραφή**
chart	Επιστρέφει τα αποτελέσματα αναζήτησης σε πίνακα.
eval	Υπολογίζει μια έκφραση και τοποθετεί την τιμή της σε ένα πεδίο.
stats	Παρέχει στατιστικά, προαιρετικά κατηγοριοποιημένα σε πεδία.
round(X,Y)	Απαιτεί ένα ή δύο αριθμητικά αθροίσματα. Επιστρέφει μια στρογγυλοποιημένη τιμή για το X η οποία καθορίζεται από το Y.
sum(X)	Επιστρέφει το άθροισμα των τιμών του πεδίου X.
usenull(X)	Επιστρέφει μη μηδενικές τιμές του πεδίου X.
timechart	Επιστρέφει τα αποτελέσματα αναζήτησης σε μορφή διαγράμματος χρονοσειράς.
top	Εμφανίζει τις πιο κοινές τιμές ενός πεδίου.
lookup	Προσθέτει πεδία που προέρχονται από εξωτερικό αρχείο.
fields	Αφαιρεί πεδία από τα αποτελέσματα αναζήτησης.
table	Επιστρέφει αποτελέσματα σε μορφή πίνακα.
sort	Κατηγοριοποιεί τα αποτελέσματα αναζήτησης σύμφωνα με καθορισμένα πεδία.

dc(X)	Επιστρέφει μόνο τις διακριτές τιμές ενός πεδίου X.
values(X)	Επιστρέφει τη λίστα όλων των διαφορετικών τιμών του πεδίου X.
spath	Εξάγει τιμές κλειδιά σε XML μορφή.
search	Πραγματοποιεί αναζήτηση στο Index για να επιστρέψει αποτελέσματα.

Status	**Περιγραφή**
200	Επιτυχής παραλαβή αιτήματος από το διακομιστή.
404	Το αντικείμενο που ζητήθηκε δεν υπάρχει.
500	Εσωτερικό σφάλμα διακομιστή.
503	Ο διακομιστής δεν είναι διαθέσιμος.

Παρατίθενται τα αρχεία κώδικα του Twitter-Splunk Mobile που τροποποιήθηκαν:

Home.html

```
<!DOCTYPE html>
<html>
  <head>
    <title>Twitter-Splunk Mobile</title>
<meta name="viewport" content="initial-scale=1.0, width=device-width, user-
scalable=no" />
    <script type="text/javascript" src="${make_url("/static/js/i18n.js")}"></script>
    <link   rel="stylesheet"
href="${make_url('/static/app/mobile/jquery.mobile-1.0b3/jquery.mobile-
1.0b3.min.css')}" />
    <script type="text/javascript" src="${make_url('/static/app/mobile/jquery-
1.6.3.min.js')}"></script>
    <script type="text/javascript"
src="${make_url('/static/app/mobile/jquery.mobile-1.0b3/jquery.mobile-
1.0b3.min.js')}"></script>
<link rel="shortcut icon"    href="${make_url('/static/img/favicon.ico')}" />
    <link rel="apple-touch-icon"
href="${make_url('/static/app/mobile/splIcon57.png')}"  sizes="57x57"   />
    <link rel="apple-touch-icon"
href="${make_url('/static/app/mobile/splIcon72.png')}"  sizes="72x72"   />
    <link rel="apple-touch-icon"
href="${make_url('/static/app/mobile/splIcon114.png')}" sizes="114x114" />

  </head>
<script>
   $('body').live('pagecreate',function(event) {
     if (navigator.userAgent.match(/Android/i)) {
        window.scrollTo(0,0);
        window.scrollTo(0,1);
     }
    });
</script>
<body>
    <div data-role="page" id="home" >
      <div data-role="header">
          <h1>Twitter-Splunk Mobile</h1>
```

```
            <a href="/account/logout" data-role="button" data-icon="delete"
class="ui-btn-right" data-ajax="false" data-iconpos="notext"
title="Logout"></a>
      </div><!-- /header -->
<div data-role="content">
          <center>
            <div data-inline="true" data-theme="d" style="max-width:400px;">
              <a href="?command=searches"  data-role="button" data-
icon="search" data-iconpos="left" data-theme="b">Tweet Searches</a>

              <a href="?command=newsearch" data-role="button" data-
icon="new" data-iconpos="left" data-theme="a">New Search</a>
            </div>
          </center>
      </div><!-- /content -->
   <div id="commonfooter" data-role="footer" data-theme="f">
          <center>
            <a href="/app/launcher" data-ajax="false">non-mobile splunk</a> /
            <a href="http://splunk-base.splunk.com/apps/28665/splunk-mobile"
target=_new>give feedback!</a>
<h4><small><small>Created by <a
href="mailto:a.synodinou@besecuregroup.com?subject=Splunk
Mobile">Aggeliki Synodinou</a></small></small></h4>
          </center>
      </div><!-- /footer -->
    </div><!-- /page -->
</body>
</html>
Searches.html
<!DOCTYPE html>
<html>
  <head>
    <title>Twiiter-Splunk Mobile: Searches</title>

    <meta name="viewport" content="initial-scale=1.0, width=device-width,
user-scalable=no" />
    <script type="text/javascript" src="${make_url("/static/js/i18n.js")}"></script>
    <link   rel="stylesheet"
href="${make_url('/static/app/mobile/jquery.mobile-1.0b3/jquery.mobile-
1.0b3.min.css')}" />
    <script type="text/javascript" src="${make_url('/static/app/mobile/jquery-
1.6.3.min.js')}"></script>
```

```
    <script type="text/javascript"
src="${make_url('/static/app/mobile/jquery.mobile-1.0b3/jquery.mobile-
1.0b3.min.js')}"></script>
 <link rel="shortcut icon"    href="${make_url('/static/img/favicon.ico')}" />
    <link rel="apple-touch-icon"
href="${make_url('/static/app/mobile/splIcon57.png')}"  sizes="57x57"   />
    <link rel="apple-touch-icon"
href="${make_url('/static/app/mobile/splIcon72.png')}"  sizes="72x72"   />
    <link rel="apple-touch-icon"
href="${make_url('/static/app/mobile/splIcon114.png')}" sizes="114x114" />
 </head>
<script>
   $('body').live('pagecreate',function(event) {
     if (navigator.userAgent.match(/Android/i)) {
        window.scrollTo(0,0);
        window.scrollTo(0,1);
     }
    });
  </script>
  <body>

    <!--  SAVED SEARCHES -->
    <div data-role="page" id="searches" class="type-interior">
      <div data-role="header">
          <a href="?comand=" rel=external data-iconpos="notext" title="Home"
data-icon="home">Home</a>
          <h1>Saved Twitter Searches</h1>
      </div><!-- /header -->

      <div data-role="content">
          <div class="content-primary">
            <ul data-role="listview" data-filter="true" data-inset="true">
           <li data-role="list-divider">Twitter General Activity</li>
                <li><a  rel=external
href="?command=results&ss=Top+Hashtags">Top Hashtags</a></li>
                <li><a  rel=external
href="?command=results&ss=Top+Mentions">Top Mentions</a></li>
                <li><a  rel=external
href="?command=results&ss=Top+User+Agents">Top User Agents</a></li>
                <li><a  rel=external
href="?command=results&ss=Top+Users">Top Users</a></li>
            <li data-role="list-divider">Other</li>
```

```
                <li><a  rel=external
href="?command=results&ss=Tweet+Time+Zones">Tweet Time
Zones</a></li>
            </ul>
          </div><!--/content-primary -->
      </div><!-- /content -->

      <div id="commonfooter" data-role="footer" data-theme="f">
          <h4><small><small><br/>Created by Aggeliki
Synodinou</a></small></small></h4>
      </div><!-- /footer -->
        </div><!-- /page -->
   </body>
</html>
```

AndroidManifest

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="com.example.splunk_mobile"
    android:versionCode="1"
    android:versionName="1.0" >
<uses-sdk
        android:minSdkVersion="8"
        android:targetSdkVersion="17" />
<uses-permission
        android:name="android.permission.INTERNET"/>
<application
        android:allowBackup="true"
        android:icon="@drawable/ic_launcher"
        android:label="@string/app_name"
        android:theme="@style/AppTheme" >
        <activity
            android:name="com.example.splunk_mobile.MainActivity"
            android:label="@string/app_name" >
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
 <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
```

```
        </activity>
    </application>
</manifest>
```

MainActivity

```
package com.example.splunk_mobile;
                        import android.os.Bundle;
import android.app.Activity;
import android.view.Menu;
import android.webkit.WebView;
                      import com.splunk.android.Splunk;
public class MainActivity extends Activity {

        @Override
        protected void onCreate(Bundle savedInstanceState) {
                super.onCreate(savedInstanceState);
                setContentView(R.layout.activity_main);
                Splunk.connect("https://192.168.252.66:8089", "admin",
                        "Password", getApplicationContext());
                 WebView webview = new WebView(this);
                 setContentView(webview);
                 webview .getSettings().setJavaScriptEnabled(true);
                 webview.loadUrl("http:// 192.168.232.68:8032en-
US/custom/mobile/mobile");
                 }
@Override
        public boolean onCreateOptionsMenu(Menu menu) {
                // Inflate the menu; this adds items to the action bar if it is
present.
                getMenuInflater().inflate(R.menu.main, menu);
                return true;
        }
         />
```

Βιβλιογραφία – Πηγές

http://docs.splunk.com/Documentation/Splunk/latest/Tutorial/WelcometotheSplunkTutorial

http://docs.splunk.com/Documentation/Splunk/latest/Data/WhatSplunkcanmonitor

http://docs.splunk.com/Documentation/Splunk/latest/Search/Whatsinthismanual

http://docs.splunk.com/Documentation/Splunk/latest/Admin/Whatsinthismanual

http://dev.splunk.com/view/SP-CAAADQ8

http://www.adslgr.com/forum/archive/index.php/t-331275.html

http://dev.splunk.com/view/rest-api-overview/SP-CAAADP8

https://dev.twitter.com/docs/streaming-apis/processing

http://docs.splunk.com/Documentation/Splunk/5.0.2/AdvancedDev/ModInputsExample#Twitter_example

http://en.wikipedia.org/wiki/Splunk

http://www.splunk.com/view/big-data/SP-CAAAGFH

http://blogs.splunk.com/2010/06/23/track-twitter-world-cup-sentiment-with-splunk/

https://blogs.ischool.berkeley.edu/i290-abdt-s12/

http://www.ischool.berkeley.edu/node/22593

http://splunk-base.splunk.com/apps/28665/splunk-mobile

http://splunk-base.splunk.com/answers/28678/what-do-you-want-to-see-in-a-splunk-mobile-app

http://splunk-base.splunk.com/answers/31866/accessing-stuff-from-other-apps-using-splunk-mobile

http://splunkninja.ning.com/profiles/blogs/how-to-build-a-simple-app-in.

http://metasplunk.com/projects/particle

http://www.businesscoachinglab.gr/page.aspx?itemID=SPG59

http://www.splunk.com/view/benefits/SP-CAAACCS

http://blog.programmableweb.com/2012/12/18/splunk-digs-deep-into-big-data-application-development/

http://www.sepe.gr/files/pdf/sepenews/sepenews33/manpower.pdf

http://www.itu.int/ITU-D/treg/publications/trends12.html

http://twiplomacy.com/

http://social-net.gr/2012/11/auxisi-poliseos-pelatologiou-via-social-media/

http://www.digitaldaya.com/epetition.php?id_petition=69#/0

http://en.wikipedia.org/wiki/Main_Page

http://developer.android.com

http://developer.android.com/about/dashboards/index.html

http://www.openhandsetalliance.com

http://developer.android.com/guide/developing/device.html

http://developer.android.com/reference/android/content/Context.html

http://www.ibm.com/developerworks/opensource/library/xandroid/index.html?ca=dgr-lnxw82AndroidXML&S_TACT=105AGX59&S_CMP=grlnxw82

http://developer.android.com/guide/topics/security/security.html

http://developer.android.com/guide/topics/manifest/manifest-intro.html

http://developer.android.com/reference/android/app/Activity.html

http://developer.android.com/reference/android/app/Activity.html

http://www.android-app-market.com/android-activity-lifecycle.html

http://developer.android.com/guide/webapps/index.html