Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής
Πρόγραμμα Μεταπτυχιακών Σπουδών
«Προηγμένα Συστήματα Πληροφορικής»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	***Εφαρμογή Android διαχείρισης και παροχής πληροφοριών και εργαλείων για ιστοσελίδες*** ***Android application for management, information and tools about web pages***
Ονοματεπώνυμο Φοιτητή	**Κωνσταντίνος Αδάμ**
Πατρώνυμο	**Πέτρος**
Αριθμός Μητρώου	**ΜΠΣΠ/ 17003**
Επιβλέπων	**Ευθύμιος Αλέπης, Επίκουρος Καθηγητής**

Ημερομηνία Παράδοσης **12 2018**

Τριμελής Εξεταστική Επιτροπή

Αλέπης Ευθύμιος Επίκουρος Καθηγητής	Πατσάκης Κωνσταντίνος Επίκουρος Καθηγητής	Βίρβου Μαρία Καθηγητής

ΠΕΡΙΛΗΨΗ

Η παρούσα μεταπτυχιακή διατριβή, ασχολείται με την ανάπτυξη λογισμικού ιστοσελίδας και Android εφαρμογής για την εύρεση, διαχείριση και παροχής πληροφοριών σχετικά με domains, IPs, πληροφορίες whois και SSL πιστοποιητικά. Γίνεται εκτενής παρουσίαση των υλοποιημένων εφαρμογών και σύγκριση αυτών με άλλες εφαρμογές τόσο web όσο και Android.

Στο πρώτο κεφάλαιο αναφέρονται τεχνικοί όροι που χρησιμοποιούνται στην παρούσα μεταπτυχιακή διατριβή μέσω βιβλιογραφικής ανασκόπησης, στο δεύτερο κεφάλαιο παρουσιάζονται, παρόμοιες, ήδη υλοποιημένες εφαρμογές. Στο τρίτο κεφάλαιο αναλύεται ο σκοπός, η μεθοδολογία και η αρχιτεκτονική των συστημάτων που υλοποιήθηκαν και στο τέταρτο κεφάλαιο γίνεται εκτενής παρουσίαση των εφαρμογών. Τέλος στο πέμπτο κεφάλαιο γίνεται σύγκριση των εφαρμογών με άλλες, παρουσιάζονται τα προβλήματα που προέκυψαν και πως επιλύθηκαν και αναφέρονται μελλοντικές προσθήκες και αναβαθμίσεις.

ABSTRACT

This present postgraduate dissertation concerns the development of the web and Android application for management, information and tools about web pages (domain names), IPs, whois information and SSL certificates. There is an extensive presentation of the developed applications and a comparison of them, with other applications (web and Android).

In the first chapter technical terms are mentioned that are used in the present postgraduate dissertation through bibliographic review, in the second chapter are presented similar developed applications. In the third chapter the purpose, methodology and systems architecture are analyzed and in the fourth chapter an extensive presentation is made of other applications. Finally, in the fifth chapter there is a comparison to the other applications, the problems that occurred and resolved are presented and new updates and additions are mentioned.

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΕΧΟΜΕΝΑ ΕΙΚΟΝΩΝ

Εισαγωγή

Η παρούσα μεταπτυχιακή διατριβή, με θέμα την ***διαχείριση και παροχή πληροφοριών και εργαλείων για ιστοσελίδες σε εφαρμογή Android***, δημιουργήθηκε προκειμένου να βοηθήσει όλους όσους επιθυμούν να αναζητήσουν πληροφορίες σχετικά με ένα όνομα χώρου στο διαδίκτυο (domain name).
Λόγω του χώρου εργασίας μου, υπήρξε μεγάλη ανάγκη για βελτιστοποίηση των εφαρμογών και αξιόπιστης αναζήτησης πληροφοριών σχετικά με domains, IPs, SSL, DNS κλπ και θέλησα να δημιουργήσω ένα πολυεργαλείο που θα συμπεριλάμβανε όλες τις διαφορετικές υπηρεσίες που έως τώρα χρησιμοποιούσα.
Η ανάπτυξη της ιστοσελίδας και της εφαρμογής Android ξεκίνησε τον Ιούνιο του 2018 και ολοκληρώθηκε τον Νοέμβριο του 2018.
Στο πρώτο μέρος της εργασίας γίνεται εκτενής βιβλιογραφική ανασκόπηση. Συγκεκριμένα στο 1ο κεφάλαιο εκθέτονται τεχνικοί όροι, σχετικά με κομμάτια τα οποία χρησιμοποιούνται ως εργαλεία στις εφαρμογές και αναφέρεται αναλυτικά το Λειτουργικό Σύστημα Android. Στο 2ο κεφάλαιο γίνονται αναφορές σε άλλες παρόμοιες εφαρμογές που ήδη υπάρχουν (τόσο ιστοσελίδες, όσο και Android applications). Στο δεύτερο μέρος, ξεκινώντας με το 3ο κεφάλαιο, παρουσιάζεται ο σκοπός, η δομή και η αρχιτεκτονική της εφαρμογής, τα εργαλεία ανάπτυξής της και η μεθοδολογία. Στο 4ο κεφάλαιο γίνεται λεπτομερής ανάλυση της εφαρμογής και όλων των δυνατοτήτων της (web και Android). Τέλος, στο 5ο κεφάλαιο, γίνεται σύγκριση αποτελεσμάτων, παρουσιάζονται τα προβλήματα που προέκυψαν και γίνονται αναφορές σε μελλοντικές επεκτάσεις και αναβαθμίσεις.

Κεφάλαιο 1

Στο παρόν κεφάλαιο, θα αναφερθούν αναλυτικά βάση βιβλιογραφικής ανασκόπησης, τεχνικοί όροι που χρησιμοποιούνται εκτενώς στην διπλωματική διατριβή. Γίνεται εκτενής αναφορά στο Λειτουργικό Σύστημα Android, που είναι και το κύριο θέμα της διατριβής, ενώ αναφέρονται, μεταξύ άλλων, οι όροι domain και DNS, SSL και IPs (RIPE).

1.1 Domain name + DNS:

Τα domain names παρέχονται στους χρήστες μέσω κάποιων εταιριών που λειτουργούν ως καταχωρητές γι' αυτά τα ονόματα και που αναλαμβάνουν να επικοινωνήσουν με το σωστό μητρώο για να ολοκληρωθεί η κατοχύρωση του domain. Επιπλέον, μέσω του Καταχωρητή ορίζονται στο domain, ένας ή περισσότεροι DNS servers[1]. Ένας DNS server περιέχει πληροφορίες σχετικά με το domain και αυτόν συμβουλεύεται το διαδίκτυο όταν κάποιος χρήστης πληκτρολογήσει το domain στον browser του[2]. Το λεγόμενο resolving, πραγματοποιείται σε επίπεδο DNS και πάντα, τον / τους DNS που έχει / έχουν οριστεί από τον Καταχωρητή, στο μητρώο για ένα domain name. Μέσα από τον DNS server, λαμβάνουν πληροφορίες και οι Internet Service Providers (ISPs – πάροχοι internet όπως ο ΟΤΕ(Οργανισμός Τηλεπικοινωνιών Ελλάδος)) ανά τον κόσμο και αποθηκεύουν και εκείνοι αντίστοιχα records - εγγραφές, ώστε να γίνεται γρηγορότερα η δρομολόγηση του κάθε χρήστη στον οποίο παρέχουν internet, προς οποιοδήποτε domain[3].

1.2 Android

Το Android, είναι ένα Λειτουργικό Σύστημα που προορίζεται κυρίως για κινητές συσκευές και tablets. Υπάρχουν εκδόσεις του ΛΣ Android ακόμη και για τηλεοράσεις, ρολόγια (smartwatches – Android Wear) και αυτοκίνητα (Android Auto)[4]. Παρουσιάστηκε πρώτη φορά τον Νοέμβριο του 2007 από την Google[5]. Η πρώτη επίσημη έκδοση του Λειτουργικού Συστήματος κυκλοφόρησε τον Οκτώβριο του 2008. Σύμφωνα με την έκθεση της Strategy Analytics, το Android μέχρι τον Οκτώβριο του 2013, καταλάμβανε ποσοστό 81,3% από την παγκόσμια αγορά Smartphones, ενώ την ίδια στιγμή η Apple καταλάμβανε ποσοστό 13,4%, η Microsoft 4,1% και μόλις το 1% η blackberry[6].

Πλέον είναι το πιο διαδεδομένο λογισμικό για κινητές συσκευές, με ποσοστό 72% στην παγκόσμια αγορά, σύμφωνα με μετρήσεις του Νοεμβρίου 2018[7]. Το Android έχει βασιστεί στον πυρήνα του Λειτουργικού Linux, ενώ ο κώδικάς του, είναι διαθέσιμος κάτω από τους όρους της ελεύθερης άδειας λογισμικού, Apache License[8].

---

[1] Brain M. , Crawford S. – How Domain Name Servers Work. *howstuffworks*. Weblog.
Available from: https://computer.howstuffworks.com/dns.htm
[Accessed 3rd Dec 2018]

[2] How the Domain Name System (DNS) Works. *Verisign.* Weblog.
Available from: https://www.verisign.com/en_US/website-presence/online/how-dns-works/index.xhtml
[Accessed 3rd Dec 2018]

[3] Abrams L.- What is Domain Name Resolution. *bleepingcomputer.* Weblog.
Available from: https://www.bleepingcomputer.com/tutorials/what-is-domain-name-resolution/ [Accessed 3rd Dec 2018]

[4] ΓΑΒΑΛΑΣ Δ., ΚΑΣΑΠΑΚΗΣ Β., ΧΑΤΖΗΔΗΜΗΤΡΗΣ Θ., 2015. ΚΙΝΗΤΕΣ ΤΕΧΝΟΛΟΓΙΕΣ. εκδ. Νέων Τεχνολογιών. Αθήνα. σελ. 9

[5] Wikipedia - Android. Weblog.
Available from: https://el.wikipedia.org/wiki/Android
[Accessed 4th Dec 2018]

[6] DEITEL P. DEITEL H.DEITEL A. , 2014. ANDROID ΠΡΟΓΡΑΜΜΑΤΙΣΜΟΣ. Μτφρ. Σαμαράς Γ. εκδ. Γκιούρδας. Αθήνα. σελ. 3

[7] Statcounter - Mobile Operating System Market Share Worldwide. Weblog.
Available from: http://gs.statcounter.com/os-market-share/mobile/worldwide
[Accessed 4th Dec 2018]

[8] Apache – Apache License.
Available from: https://www.apache.org/licenses/LICENSE-2.0
[Accessed 5th Dec 2018]

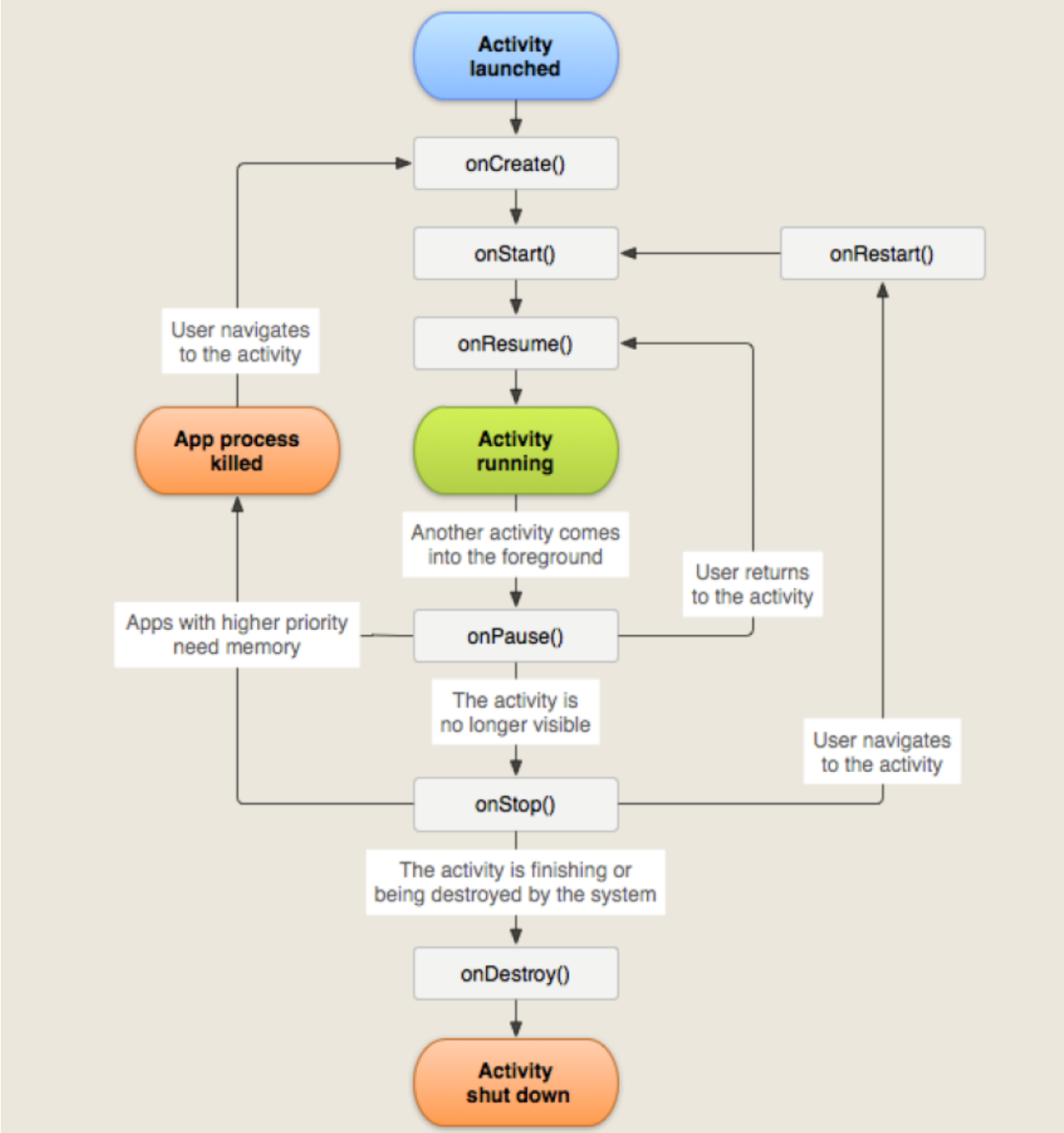
1.2.1 Δομικά στοιχεία εφαρμογών Android

Κάποια βασικά δομικά στοιχεία που εμπεριέχονται σε όλες τις εφαρμογές Android είναι τα παρακάτω:

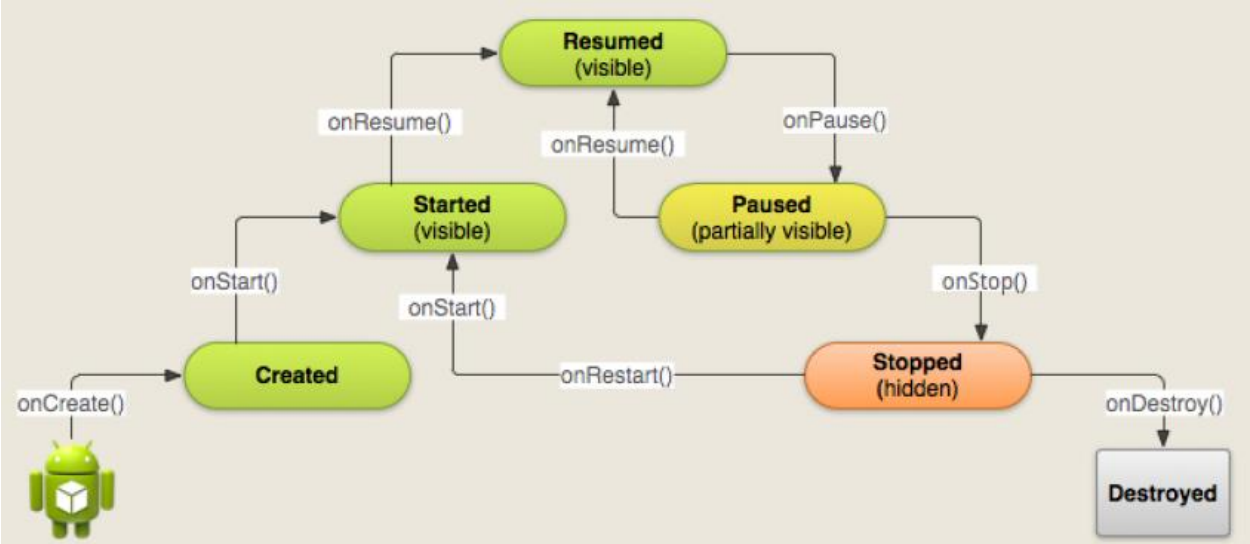
- Δραστηριότητες (Activities)
  - Είναι το πιο σύνηθες δομικό στοιχείο σε μια εφαρμογή Android καθώς αντιπροσωπεύουν διαφορετικές οθόνες διεπαφής της εφαρμογής με τον χρήστη. Όλες οι εφαρμογές έχουν ένα βασικό activity που ονομάζεται Main Activity
- Κύκλος ζωής μιας δραστηριότητας
  - Όλες οι δραστηριότητες έχουν συγκεκριμένο κύκλο ζωής στον οποίο μπορούν να βρεθούνε. Υπάρχουν 3 πιθανές καταστάσεις για κάθε δραστηριότητα:
    - Ενεργή
    - Παύση (αδράνεια)
    - Σταματημένη

    Σε κάθε εναλλαγή κατάστασης, η δραστηριότητα ειδοποιείται μέσω της αντίστοιχης ρουτίνας:
    - onCreate (δημιουργία δραστηριότητας)
    - onStart (εκκίνηση δραστηριότητας)
    - onResume (όταν επαναφερθεί η συγκεκριμένη δραστηριότητα από αδράνεια)
    - onPause (όταν καλείται άλλη δραστηριότητα)
    - onStop (τελειώνει η δραστηριότητα)
    - onDestroy (τερματισμός δραστηριότητας)[9]

[9] Αλέπης Ευ. – Activity Lifecycle and States. Πανεπιστημιακές Σημειώσεις. Πανεπιστήμιο Πειραιώς 12-07-2017



Εικόνα 1: Activity basic states



Εικόνα 2: Activity Lifetime methods

- **Υπηρεσίες (services)**
  - Ένα service εκκινείται από μια δραστηριότητα και τρέχει στο παρασκήνιο ακόμη και όταν η δραστηριότητα σταματήσει να λειτουργεί. Η λειτουργία των υπηρεσιών συνήθως εκτελούν πιο “βαριές” και χρονοβόρες εργασίες, ενώ δεν παρέχουν κάποιο γραφικό περιβάλλον στον χρήστη.
- **Μανιφέστο εφαρμογών (Android Manifest)**
  - Στο αρχείο manifest δηλώνονται και καταγράφονται όλα τα δομικά στοιχεία της εφαρμογής, το οποίο εμπεριέχεται σε όλες τις εφαρμογές Android (συμπεριλαμβάνεται στο .apk της εφαρμογής). Η μορφή του αρχείου manifest είναι σε xml και έχει την ονομασία AndroidManifest.xml. Επιπλέον στο συγκεκριμένο αρχείο, γίνεται δήλωση όλων των δικαιωμάτων που ζητά η εφαρμογή[10] από τον χρήστη μόλις έχει εγκατασταθεί και εκκινήσει[11].

1.3 DIG

Η λειτουργία του dig, είναι μια διαδικασία κατά την οποία αναζητούμε συγκεκριμένες εγγραφές από τους δηλωμένους DNS ενός domain. Υπάρχουν πολλοί και διάφοροι τρόποι να υλοποιηθεί μια εφαρμογή εύρεσης DNS records, ωστόσο η ορθή διαδικασία είναι αυτή που περιγράφεται σε επόμενο κεφάλαιο.

[10] Felt AP, Chin E, Hanna S, Song D, Wagner D. Android permissions demystified. In: Proceedings of the 18th ACM conference on Computer and communications security - CCS ’11 [Internet]. Chicago, Illinois, USA: ACM Press; 2011 [cited 2018 Dec 12]. p. 627. Available from: http://dl.acm.org/citation.cfm?doid=2046707.2046779

[11] ΓΑΒΑΛΑΣ Δ., ΚΑΣΑΠΑΚΗΣ Β., ΧΑΤΖΗΔΗΜΗΤΡΗΣ Θ., 2015. ΚΙΝΗΤΕΣ ΤΕΧΝΟΛΟΓΙΕΣ. εκδ. Νέων Τεχνολογιών. Αθήνα. σελ. 200-204

1.4 SSL

Το SSL είναι ένα πιστοποιητικό το οποίο εκδίδει μια εταιρία για κάποιο συγκεκριμένο domain. Υπάρχουν πολλά και διάφορα είδη πιστοποιητικών SSL, τα οποία προκειμένου να εκδοθούν, απαιτούν διαφορετική διαδικασία. Τα πιστοποιητικά που έχουν οι πιο απλές ιστοσελίδες και εφαρμογές είναι Domain Validation. Ουσιαστικά γίνεται μια επιβεβαίωση του domain μέσω:

a) Επιβεβαίωση μέσω συγκεκριμένου λογαριασμού email
b) Επιβεβαίωση μέσω CNAME record μέσα στους δηλωμένους DNS του domain
c) Επιβεβαίωση με το upload κάποιου αρχείο με συγκεκριμένο όνομα και περιεχόμενο και crawl αυτού του αρχείου από την εκδότρια αρχή

Το πιστοποιητικό συνδέεται άμεσα με ένα private key που βρίσκεται εγκατεστημένο στον server ο οποίος φιλοξενεί την υπηρεσία του domain (μπορεί να είναι emails, ιστοσελίδα, web application) και με βάση το private key εκδίδεται ένα αρχείο CSR που περιέχει κωδικοποιημένα τις απαραίτητες πληροφορίες. Το αρχείο που επιστρέφει η εκδότρια αρχή μετά την απαραίτητη επιβεβαίωση είναι της μορφής .crt και εγκαθίσταται στον web server, ο οποίος το κάνει attach στο domain και το αποστέλλει σε κάθε request που το απαιτεί (secure connection – https). Εναλλακτικά από το Domain Validation (DV) υπάρχει το Organization Validation (OV) και το Extended Validation (EV)[12] που είναι το πιο απαιτητικό από όλα. Γι' αυτά τα πιστοποιητικά, επιπλέον από την παραπάνω διαδικασία, απαιτούνται και κάποια έγγραφα πιστοποίησης της εταιρίας στην οποία ανήκει το domain, έγγραφα για την ιδιοκτησία του domain καθώς και τηλεφωνική επιβεβαίωση[13].

1.5 RIPE NCC (Réseaux IP Européens Network Coordination Centre)

Η RIPE NCC είναι η αρμόδια αρχή, απόδοσης IPv4 και IPv6 διευθύνσεων για την Ευρώπη, Δυτική Ασία και την πρώην Σοβιετική Ένωση. Τα κεντρικά γραφεία βρίσκονται στο Άμστερνταμ στην Ολλανδία, ενώ υπάρχουν και στο Ντουμπάι.
Υπάρχουν περισσότερα από 10000 μέλη (καταγραφή Μαρτίου 2014) και συνδρομητές στην RIPE σε πάνω από 76 χώρες από τις περιοχές για τις οποίες είναι αρμόδια (στοιχεία του Μαρτίου 2014). Οποιοδήποτε μπορεί να γίνει μέλος της, ωστόσο, τα μέλη της είναι ως επί το πλείστων πάροχοι internet στις χώρες αρμοδιότητάς της (όπως για παράδειγμα ο ΟΤΕ στην Ελλάδα).
Η δραστηριότητά της ξεκίνησε τον Απρίλιο του 1992 στο Άμστερνταμ στην Ολλανδία. Επίσημα εδραιώθηκε τον Νοέμβριο του 1997[14].

[12] What is an Extended Validation (EV SSL) Certificate? [Internet]. [cited 2018 Dec 16]. Available from: https://www.globalsign.com/en/ssl-information-center/what-is-an-extended-validation-certificate/
[13] The SSL Store™ is here to help you validate your SSL Certificates quickly & easily. Breeze through the SSL valiation process by following our validation checklist. [Internet]. Knowledge Base. [cited 2018 Dec 15]. Available from: https://www.thesslstore.com/knowledgebase/ssl-validation/
[14] Réseaux IP Européens Network Coordination Centre. In: Wikipedia [Internet]. 2018 [cited 2018 Dec 15]. Available from: https://en.wikipedia.org/w/index.php?title=R%C3%A9seaux_IP_Europ%C3%A9ens_Network_Coordination_Centre&oldid=845590576

Κεφάλαιο 2

Στο κεφάλαιο 2 γίνεται παρουσίαση των εφαρμογών που προσφέρουν παρόμοια εργαλεία, όπως και η παρούσα μεταπτυχιακή διατριβή. Καθώς δεν υπάρχει αντίστοιχο εργαλείο που έχει ενσωματωμένες όλες τις λειτουργίες, έχουν επιλεγεί 2 πλατφόρμες από κάθε λειτουργία.

2.1 Υπάρχουσες εφαρμογές

Η ιδέα της παρούσας διπλωματικής εργασίας είναι καινοτόμα όσον αφορά τα εργαλεία που προσφέρει, σε σχέση με παρόμοια που υπάρχουν στο διαδίκτυο. Υπάρχουν πολλά αντίστοιχα εργαλεία τα οποία αναφέρουμε στο παρόν κεφάλαιο. Εκτενέστερη ανάλυση και σύγκριση θα γίνει στα επόμενα κεφάλαια.

2.1.1 Web εφαρμογή

Η web εφαρμογή περιλαμβάνει αρκετά εργαλεία. Δεν υπάρχει αντίστοιχη εφαρμογή η οποία να περιέχει τόσες πολλές λειτουργίες μαζεμένες σε μια. Ενδεικτικά αναφέρουμε παρόμοια εργαλεία τα οποία περιλαμβάνονται στην web εφαρμογή.

- DIG
  - G Suite Toolbox DIG (https://toolbox.googleapps.com/apps/dig/)
  - DigWebInterface (https://www.digwebinterface.com/)
- Password
  - Password Generator (https://my.norton.com/extspa/idsafe?path=pwd-gen)
  - Random Password Generator (https://www.roboform.com/password-generator)
- Whois
  - whois (https://www.whois.com/)
  - ICANN WHOIS (https://whois.icann.org/en)

- Check port – port scan
  - you get signal (https://www.yougetsignal.com/tools/open-ports/)
  - Online Port Scan (http://www.t1shopper.com/tools/port-scan/)
- SSL Tools
  - DigiCert® SSL Installation Diagnostics Tool (https://www.digicert.com/help/)
  - SSL Checker (https://www.thesslstore.com/ssltools/ssl-checker.php)
- IP
  - IP Lookup (https://whatismyipaddress.com/ip-lookup)
  - IP Address Lookup (https://www.whatismyip.com/ip-address-lookup/)

2.1.2 Android Apps

Εφαρμογές για Android συσκευές, υπάρχουν σαφώς λιγότερες από ότι web εφαρμογές και ιστοσελίδες.

- Domain Analyzer (https://play.google.com/store/apps/details?id=uk.co.bocc.domain_analyser)
- WhoIs, DNS lookup Domain Tools (https://play.google.com/store/apps/details?id=pryc.domain.tools.app)
- Domain Server IP (https://play.google.com/store/apps/details?id=com.pingresponsetime)
- Whois & DNS Lookup - Domain/IP (https://play.google.com/store/apps/details?id=com.xsprice.nettools)
- MyDIG (https://play.google.com/store/apps/details?id=at.tripwire.mydig)

Κεφάλαιο 3

Στο παρόν κεφάλαιο αναφέρεται ο σκοπός για τον οποίο αναπτύχθηκαν οι εφαρμογές και η μεθοδολογία που ακολουθήθηκε προκειμένου να παραχθεί το τελικό αποτέλεσμα. Τέλος παρουσιάζεται λεπτομερώς η αρχιτεκτονική των συστημάτων που χρησιμοποιούνται από τις εφαρμογές, ο τρόπος εγκατάστασης και παραμετροποίησής τους.

3.1 Σκοπός

Προκειμένου, όποιος ενδιαφέρεται να μάθει πληροφορίες σχετικά με την IP από την οποία λειτουργεί μια ιστοσελίδα ή υπηρεσία, θα πρέπει να χρησιμοποιήσει διάφορα εργαλεία. Ο σκοπός για την εφαρμογή της παρούσας μεταπτυχιακής διατριβής είναι να αναλάβει να εξαλείψει αυτά τα βήματα και να εμφανίσει ολόκληρη την πληροφορία, μέσω ενός κουμπιού. Συγκεντρωμένα σε μια web και Android εφαρμογή, μπορεί ο χρήστης να αναζητήσει πληροφορίες που σχετίζονται με domain, IP, SSL, βελτίωση απόδοσης της ιστοσελίδας του και πολλά άλλα μέσα από τον υπολογιστή ή την κινητή του συσκευή.

3.2 Μεθοδολογία

Η ορθή διαδικασία εύρεσης της διεύθυνσης IP για ένα domain στο διαδίκτυο, είναι να ρωτήσουμε τους root DNS, αυτοί απαντάνε με τους DNS του αρμόδιου μητρώου (παράδειγμα ITE (Ίδρυμα Τεχνολογίας και Έρευνας) για τα .gr) και από το αρμόδιο μητρώο μαθαίνουμε τους authoritative DNS για ένα domain. Αυτοί οι DNS είναι οι δηλωμένοι στο μητρώο και περιλαμβάνουν τις απαραίτητες εγγραφές που πρέπει να έχει το συγκεκριμένο domain και τις μοιράζονται με το διαδίκτυο. Όποιος αναζητήσει ένα domain σε οποιονδήποτε browser, ακολουθείται η παραπάνω διαδικασία. Αφού γνωρίζουμε τους DNS του domain που θέλουμε να μάθουμε πληροφορίες, τότε θα πρέπει να ρωτήσουμε τι ακριβώς πληροφορία χρειαζόμαστε να μάθουμε (ποιο record ικανοποιεί την αναζήτησή μας). Η IP που μας ενδιαφέρει, αφού την μάθουμε, θα πρέπει να αναζητήσουμε κάποιο άλλο εργαλείο που μπορεί από την IP να εμφανίσει πληροφορίες σχετικά με την χώρα στην οποία έχει απονεμηθεί, σε ποια εταιρία έχει μισθωθεί και άλλες διάφορες πληροφορίες. Τόσο η web εφαρμογή, όσο και η Android, έχουν συμπεριλάβει όλα τα παραπάνω βήματα και εμφανίζουν ολόκληρη την πληροφορία στον χρήστη, σαν να χρησιμοποιούσε όλα τα παραπάνω εργαλεία. Στην web εφαρμογή, υπάρχουν κουμπιά που μπορεί να εμφανιστεί επιπλέον πληροφορία όπως για παράδειγμα να μεταβεί ο χρήστης απευθείας στον έλεγχο της IP από την οποία λειτουργεί το domain που αναζητεί ή να ελέγξει πληροφορίες για το domain από το μητρώο (ισχύει για .com, .net και .edu domains μόνο).
Πολλές φορές κατά την αποστολή email, μπορεί να αντιμετωπιστεί πρόβλημα λήψης του μηνύματος από τον παραλήπτη. Είναι συχνό φαινόμενο, να λείπουν κρίσιμες εγγραφές από ένα domain, οι οποίες χρησιμοποιούνται στην επιβεβαίωση της ταυτότητας του αποστολέα, ώστε να θεωρηθεί το μήνυμά του ως έγκυρο και όχι ως SPAM (κακόβουλο μήνυμα). Αυτά τα records υπάρχουν μέσα στην ζώνη DNS του domain και ονομάζονται SPF[15] (Sender Policy

[15] What is an SPF record? - DNSimple Help [Internet]. [cited 2018 Dec 16]. Available from: https://support.dnsimple.com/articles/spf-record/

Framework), DKIM[16] (DomainKeys Identified Email) και DMARC[17] (Domain-based Message Authentication, Reporting & Conformance).

Μία SPF εγγραφή είναι σε μορφή txt record και περιλαμβάνει τις Authorized IPs που μπορούν να στέλνουν emails για το domain.
Για τις DKIM εγγραφές, γίνεται επιβεβαίωση ότι ο mail server έχει την απαραίτητη εξουσιοδότηση να αποστέλλει emails για το domain.
Τέλος, οι DMARC εγγραφές δηλώνει στον mail server του παραλήπτη ότι υπάρχει SPF και DKIM record ώστε να συμβουλευτεί και πως να ενεργήσει σε περίπτωση που δεν υπάρχουν τα προαναφερθέντα records.
Με την προσθήκη των 3 παραπάνω records, αυξάνεται αρκετά η πιθανότητα επιτυχημένη παράδοσης του email. Όλα τα παραπάνω, μπορούν να ελεγχθούν με την αντίστοιχη επιλογή της web εφαρμογής.

Από το Google Tools υπάρχουν υλοποιημένα τα Mobile Friendly και Google Page Speed, που εμφανίζει τις πληροφορίες μέσω API της Google.
Έχουν αναπτυχθεί 3 εργαλεία για έλεγχο πιστοποιητικών. Μπορεί ο χρήστης να ελέγξει το αρχείο crt ή csr, ώστε να επιβεβαιώσει τις πληροφορίες που υπάρχουν μέσα στο πιστοποιητικό ή να ελέγξει εάν σε κάποιο domain, είναι ενεργό κάποιο πιστοποιητικό SSL.

3.3 Αρχιτεκτονική Συστημάτων

3.3.1 Web εφαρμογή + Βάση Δεδομένων

Η web εφαρμογή και η βάση δεδομένων, φιλοξενούνται σε ένα Virtual Machine το οποίο παρέχει 2 CPU και 2GB RAM. Το Λειτουργικό Σύστημα του server είναι CentOS 7.6 Minimal με χρήση php 7.2.13 και MariaDB 10.3.11. Ως web server χρησιμοποιείται ο Nginx και γίνεται χρήση του php-fpm ως handler για την php. Με τον παραπάνω συνδυασμό, το αποτέλεσμα είναι αρκετά γρήγορο καθώς όλα τα προαναφερθέντα services είναι αρκετά ελαφριά και δεν απαιτούν πολλούς πόρους από το σύστημα, κατά συνέπεια, οι υπόλοιποι πόροι του server είναι διαθέσιμοι προς κατανάλωση από την ιστοσελίδα και την λειτουργία της. Η λειτουργία του handler php-fpm, λόγω του pool που δημιουργεί και έχει σε αναμονή για connections, καθώς και το ενεργοποιημένο http2 πρωτόκολλο του web server, καθιστούν την συγκεκριμένη εγκατάσταση, από τις πιο αποδοτικές σε ταχύτητα και αξιοπιστία[18].
Για λόγους εξοικονόμηση πόρων και άσκοπη χρήση στα I/O του δίσκου, δεν έχει εγκατασταθεί κάποιο panel ελέγχου και όλες οι ενέργειες ολοκληρώνονται χειροκίνητα, επικοινωνώντας απευθείας με το server μέσω τερματικού (SSH πρωτόκολλο).
Επιλέχτηκε η έκδοση 7.2 της php, καθώς είναι η πλέον ενημερωμένη και γρηγορότερη από όλες τις προηγούμενες εκδόσεις. Υποστηρίζονται αλγόριθμοι κρυπτογραφίας, που δεν υποστηρίζονται σε προηγούμενες εκδόσεις, καθιστώντας την έκδοση 7.2, πιο ασφαλή.
Όλα τα components και modules που έχουν χρησιμοποιηθεί, είναι στην τελευταία δυνατή έκδοση, έχοντας ήδη δοκιμαστεί σε demo περιβάλλον προκειμένου να είναι σε stable έκδοση, καθώς αφορά production servers.

Στον server έχουν εγκατασταθεί CSF Firewall και Fail2Ban. Με τις 2 υπηρεσίες, αυξάνεται αρκετά η ασφάλεια του server καθώς μέσω αυτοματοποιημένων διαδικασιών,

[16] What is a DKIM record? - DNSimple Help [Internet]. [cited 2018 Dec 16]. Available from: https://support.dnsimple.com/articles/dkim-record/
[17] What is a DMARC record and how do I create it on DNS server? | SonicWall [Internet]. [cited 2018 Dec 16]. Available from: https://www.sonicwall.com/en-us/support/knowledge-base/170504796167071
[18] JR – Install Nginx/PHP-FPM on Fedora 29/28, CentOS/RHEL 7.5/6.10. *if-not-true-then-false*. Weblog. Available from: https://www.if-not-true-then-false.com/2011/install-nginx-php-fpm-on-fedora-centos-red-hat-rhel/ [Accessed 20th Jun 2018]

ελέγχονται τα requests και οι προσπάθειες για login και σε περίπτωση που αναγνωριστούν ότι είναι κακόβουλα ή λανθασμένα πολλαπλές φορές, τότε γίνεται αποκλεισμός της IP σε επίπεδο Firewall.

Ο server καθώς δεν έχει εγκατεστημένο panel διαχείρισης, όλες οι ενέργειες ολοκληρώθηκαν με shell commands. Για να είναι ευκολότερη η ανάπτυξη του κώδικα, χρησιμοποιήθηκε το φοιτητικό πακέτο του προγράμματος της JetBrains, PHPStorm. Η σύνδεση του PHPStorm με τον server, έγινε με χρήση SFTP πρωτοκόλλου καθώς είναι πιο ασφαλές από ότι το plain FTP. Η ιστοσελίδα έχει εγκατεστημένο SSL πιστοποιητικό, συνεπώς οποιαδήποτε σύνδεση με τον server, ολοκληρωνόταν με κρυπτογραφημένη μεταφορά δεδομένων.
Για την αποτροπή αυξημένης χρήσης της εφαρμογής από κάποια αυτοματοποιημένη διαδικασία, γίνεται έλεγχος κάθε request προς την εφαρμογή και προσμετράτε σε έναν counter. Επιτρεπτό όριο που έχει τεθεί, είναι 100 requests σε περίοδο 30 λεπτών. Επιπλέον αυτού του ορίου και μέχρι τα 400 requests ανά 30 λεπτά, εμφανίζεται στον χρήστη ένα pop up παράθυρο ενημερώντας σχετικά με την αυξημένη χρήση της εφαρμογής.

```
$hostname = gethostbyaddr($_SERVER['REMOTE_ADDR']);
$date = date("Y-m-d H:i:s");
$datet = new DateTime();
$timestamp = $datet->getTimestamp();
$check = $timestamp - 1800; //30 minutes before current request

$result = "INSERT INTO `hitted_urls` ( `ip`, `hostname`, `link`,
`timestamp`, `date`) VALUES ('$ip', '$hostname', '$actual_link',
'$timestamp', '$date')";
$tbl = mysqli_query($conn, $result);


$result = "SELECT count(`ip`) as total FROM `hitted_urls` WHERE `ip`='" .
$ip . "'AND `timestamp` > '$check'";
$res = mysqli_query($conn, $result);
$tbl = mysqli_fetch_assoc($res);

$num_rows = $tbl['total'];
$show_warning_footer = 0;

if ($num_rows > 100 && $num_rows < 400)
{
    $show_warning_footer_num = $num_rows;
    $show_warning_footer = 1;
}
elseif ($num_rows > 400)
{
    $show_warning_footer = 0;
    $command = 'csf -d ' . $ip;
    shell_exec($command);

    $message = "The IP " . $ip . " is now banned in CSF. The command I run
was: " . $command;

    $url = 'https://api.dig.gr/alert_firewall.php';
    $data = array('subject' => "IP is banned for multiple requests.",
'message_body' => $message);

    $options = array(
        'http' => array(
            'header'  => "Content-type: application/x-www-form-
urlencoded\r\n",
            'method'  => 'POST',
            'content' => http_build_query($data)
        )
    );
    $context  = stream_context_create($options);
    $result = file_get_contents($url, false, $context);

}
```

Καθώς ο server που φιλοξενεί την web εφαρμογή δεν έχει εγκατεστημένο mail server για την αποστολή μηνυμάτων, η επικοινωνία και οι ενημερώσεις γίνονται μέσω του API και τις αντίστοιχες ρουτίνες που υλοποιήθηκαν.

Η εφαρμογή κάνει εκτεταμένη χρήση της συνάρτησης shell_exec με την οποία μπορούμε να εκτελέσουμε bash commands (ουσιαστικά εντολές του Λειτουργικού Συστήματος) και να λάβουμε τα αποτελέσματα σε μια μεταβλητή. Επιπλέον, έχουν εγκατασταθεί τα απαραίτητα πακέτα της εντολής whois και dig, μέσω των οποίων λαμβάνουμε τις πληροφορίες για τις υπηρεσίες dig (simple και multiple), whois και ip lookup.

Σε αρκετές περιπτώσεις, όπως για παράδειγμα στο login και στην ανάκτηση του κωδικού πρόσβασης του χρήστη, έχει προστεθεί το reCAPTCHA v2 της Google για την αποτροπή κακόβουλων bots, να ολοκληρώνουν συνεχόμενα requests προς την ιστοσελίδα και να αποτρέψει αυτοματοποιημένες επιθέσεις από botnets.

Το design της web εφαρμογής, έχει υλοποιηθεί με bootstrap 4.1.0 και jQuery 3.3.1. Είναι φιλική προς τον χρήστη και Mobile First (πλήρως responsive σε κινητές συσκευές).

Η βάση δεδομένων δημιουργήθηκε με τέτοιο τρόπο, ώστε να είναι ευέλικτη στην προσθήκη πινάκων για επιπλέον λειτουργίες και γίνεται αποθήκευση δεδομένων για μελλοντική χρήση αυτών, προς αξιοποίηση νέων λειτουργιών. Για την διαχείριση των βάσεων δεδομένων και των πινάκων αυτών, έχει εγκατασταθεί σχετικό εργαλείο διαχείρισης, το PhpMyAdmin στην τελευταία stable έκδοσή του.

3.3.2 API που χρησιμοποιεί το Android

Το API που χρησιμοποιεί και επικοινωνεί η android εφαρμογή, βρίσκεται σε ξεχωριστό server, παρόμοιων δυνατοτήτων με τον server της web εφαρμογής (2 CPU, 2GB RAM). Έχει Λειτουργικό Σύστημα CentOS 7.6 και ως πίνακα ελέγχου, υπάρχει εγκατεστημένο cPanel®. Μαζί με το control panel, έχει εγκατασταθεί Apache Web server και εγκατεστημένο το module http2 για γρηγορότερη και ασφαλέστερη επικοινωνία σε επίπεδο πρωτοκόλλου, πολλαπλές εκδόσεις php (το API κάνει χρήση της php 7.2.13) και Exim mail server. Στην περίπτωση του API, δεν υπάρχουν καθόλου frameworks (CSS, JavaScripts), συνεπώς ο χρόνος που απαιτείται για να ολοκληρωθούν οι διαδικασίες του εκάστοτε script, είναι σημαντικά μικρότερος από ότι η web εφαρμογή που πρέπει να φορτώσει πολλά διαφορετικά CSS και JS. Επιλέχθηκε το cPanel® καθώς προσφέρει ευκολότερη διαχείριση στην εγκατάσταση και παραμετροποίηση της php και των components της, όσο και στην δημιουργία emails (και συνεπώς mail server).
Το cPanel® προσφέρει built in πολλές υπηρεσίες που χρησιμοποιεί το API, χωρίς την προσθήκη με χειροκίνητους τρόπους και είναι πλήρως υποστηριζόμενοι από αυτό. Χαρακτηριστικό παράδειγμα, είναι η παραμετροποίηση του Apache Web server με το php-fpm ως handler της php στον Apache. Με μεγάλη ευκολία γίνονται αλλαγές και παραμετροποιήσεις μέσω του UI που προσφέρει. Επιπλέον αυτών, υπάρχει ο Exim Mail server, Brute-Force Protection, εύκολο interface για έκδοση πιστοποιητικών SSL και στη συνέχεια εγκατάσταση και παραμετροποίηση του web server ώστε να το χρησιμοποιεί και πολλά άλλα.
Η επικοινωνία ξεκινάει από την εφαρμογή Android προς κάποια συγκεκριμένα php scripts του API στέλνοντας τα απαραίτητα δεδομένα κάθε φορά, ώστε να ολοκληρωθεί η επεξεργασία και να επιστραφούν τα αποτελέσματα σε μορφή json. Αυτά τα δεδομένα παράγονται από τα php scripts, ενώ τα δεδομένα από την android εφαρμογή προς τον server που φιλοξενεί το API, ολοκληρώνεται με POST requests (τα πιο ευαίσθητα δεδομένα όπως username, password και μεγάλα inputs) ενώ οι περισσότερες λειτουργίες, πραγματοποιούνται με GET requests μέσω του url. Και στον server που φιλοξενείτε το API, υπάρχουν εγκατεστημένοι μηχανισμοί ασφαλείας για την αποτροπή κακόβουλης και μη εξουσιοδοτημένης χρήσης.
Είναι πιθανό να χρησιμοποιηθεί και μέσω browser, ωστόσο η μορφή που εμφανίζονται τα δεδομένα στους browsers, δεν είναι βελτιστοποιημένα και εύκολα αναγνώσιμα, καθώς δεν προορίζονται για απεικόνιση σε browsers.
Όλες οι επικοινωνίες της Android εφαρμογής με το API, πραγματοποιείτε με https πρωτόκολλο και τα δεδομένα που μεταφέρονται από και προς το API, γίνονται με

κρυπτογραφημένη σύνδεση για να εξαλειφθεί ο κίνδυνος υποκλοπής δεδομένων και αυτά να είναι αναγνώσιμα.
Το API βρίσκεται σε ξεχωριστό server και για να γίνει καλύτερα η κατανομή του φόρτου εργασίας ανάμεσα σε αυτό και την web εφαρμογή. Τα modules που χρειάζεται κάθε εφαρμογή είναι διαφορετικά και η βέλτιστη λύση είναι να διαχωριστούν οι υπηρεσίες.

Σε δοκιμές που ολοκληρώθηκαν σε έναν server, στον οποίο λειτουργούσε η web εφαρμογή και το API με ότι χρειάζεται για την ομαλή και σωστή λειτουργία του, η απόκριση καθολικά του συστήματος ήταν πιο αργή σε σχέση με τον διαμοιρασμό των υπηρεσιών σε ξεχωριστούς servers. Το πόρισμα σχετικά με την απόδοση του ενός server σε σχέση με τους 2 ξεχωριστούς, βγήκε μέσα από γραφήματα ενός εξωτερικού συστήματος monitoring που έδειξε αυξημένη χρήση CPU και μνήμης, όταν όλες οι υπηρεσίες ήταν ενεργές.
Στην περίπτωση του API, όπως και της web εφαρμογής, για την διαχείριση του κώδικα, χρησιμοποιήθηκε το φοιτητικό πακέτο της εταιρίας JetBrains, PHPStorm. Η σύνδεση με τον server έγινε με χρήση FTPS που ουσιαστικά είναι plain FTP πρωτόκολλο και χρήση SSL για κρυπτογραφία στα δεδομένα που αποστέλλονται και λαμβάνονται.

Όλες οι λειτουργίες που εκτελούνται στο API, καταγράφονται στην βάση δεδομένων και μπορεί να γίνει περιορισμός σε επίπεδο API, χωρίς να απαιτείται παραμετροποίηση σε επίπεδο Android εφαρμογής.

3.3.3 Android Application

Η εφαρμογή Android υλοποιήθηκε με το εργαλείο που προσφέρει η Google και προτείνει για ανάπτυξη εφαρμογών για Android συσκευές, μέσω του Android Studio. Η εφαρμογή ολοκλήρωνε συχνά updates και πάντα ήταν up to date ώστε να εφαρμόζονται όλα τα security patches και updates και να είναι διαθέσιμες όλες οι νεότερες επιλογές που κυκλοφορούν σε stable εκδόσεις.
Το Android Studio που χρησιμοποιήθηκε, αρχικά ξεκίνησε από την πλατφόρμα IntelliJ της JetBrains, η οποία χρησιμοποιείται για την γλώσσα Java. Καθώς είναι μια ολοκληρωμένη λύση και πολύ σταθερή στην συγγραφή κώδικα, η οποία υιοθετήθηκε από την Google, ως το εργαλείο ανάπτυξης Android εφαρμογών.
Για το οπτικό αποτέλεσμα και τον έλεγχο της λειτουργικότητας της εφαρμογής, χρησιμοποιήθηκε ο built in emulator του Android Studio.
Επιλέχτηκε το API level 26 που αντιστοιχεί στο Android 8.0 με ονομασία Oreo, καθώς ήταν το τελευταίο λογισμικό που κυκλοφόρησε η Google κατά την ημερομηνία έναρξης της παρούσας διπλωματικής διατριβής.
Στην εφαρμογή έχει δοθεί έμφαση στην λειτουργικότητά της, στην βέλτιστη ταχύτητα και ειδικά στην κατά το μέγιστο ασφάλεια, που μπορεί να έχει. Το συγκεκριμένο Android App, αποτελεί υλοποίηση της web εφαρμογής λαμβάνοντας τις ίδιες πληροφορίες και εμφανίζοντάς τες στον χρήστη. Επιπλέον από τις διάφορες επιλογές που έχει στη διάθεσή του ο χρήστης από κεντρικό μενού της εφαρμογής, υπάρχει και χάρτης που υλοποιήθηκε στην built in εφαρμογή, Google Maps, στην οποία λαμβάνονται οι τοποθεσίες του χρήστη, την στιγμή που υλοποίησε οποιαδήποτε ενέργεια μέσα από την εφαρμογή. Κατά την απεικόνιση εμφανίζονται ως marks στον χάρτη στην ακριβή τοποθεσία που έγινε η ενέργεια, ποια λειτουργία της εφαρμογής επέλεξε ο χρήστης και την ημερομηνία και ώρα που έγινε. Οι καταγραφές αποθηκεύονται σε απομακρυσμένη βάση δεδομένων MySQL και λαμβάνονται από την Android εφαρμογή, μέσω του API. Προκειμένου να μην μπορεί οποιοσδήποτε να λάβει τις πληροφορίες τοποθεσίας που αποθηκεύονται στην βάση δεδομένων, υπάρχει ως δικλείδα ασφαλείας η αποστολή μέσω POST request, ενός συγκεκριμένου κλειδιού, που εφόσον ταιριάζει με αυτό που

έχει προστεθεί στον κώδικα php του API, τότε και μόνο τότε γίνεται η αναζήτηση των τοποθεσιών του χρήστη και αποστέλλονται πίσω στην Android εφαρμογή.

```
String USER_AGENT = "Android_App_Dig_And_IP_Info";

String url = "https://api.dig.gr/fetch_coords.php";
URL urll = new URL(url);
HttpsURLConnection con = (HttpsURLConnection) urll.openConnection();

//add request header
con.setRequestMethod("POST");
con.setRequestProperty("User-Agent", USER_AGENT);
con.setRequestProperty("Accept-Language", "en-US,en;q=0.5");

String urlParameters = "val=2j7p77rQox7uXbSXhnLZYqCiWu8xpyUeOV6bBqRTeIMZCu0AYb";

// Send post request
con.setDoOutput(true);
DataOutputStream wr = new DataOutputStream(con.getOutputStream());
wr.writeBytes(urlParameters);
wr.flush();
wr.close();
```

Ως επιπλέον μέτρο ασφαλείας, η πρόσβαση στην βάση δεδομένων δεν είναι εφικτή από οποιονδήποτε άλλο, παρά από τον ίδιο server που τη φιλοξενεί και πιο συγκεκριμένα από έναν μοναδικό χρήστη που χρησιμοποιεί το API για την επικοινωνία. Η πρόσβαση είναι κλειστή, μέσω Software Firewall που υπάρχει εγκατεστημένο στον server.
Καθώς η χρήση της Android εφαρμογής, γίνεται από πολλά και διαφορετικά δίκτυα, δεν μπορεί να χρησιμοποιηθεί μια συγκεκριμένη IP διεύθυνση για να επικοινωνεί αποκλειστικά η IP με την βάση δεδομένων και επιπλέον επειδή βρίσκεται σε πολλές διαφορετικές συσκευές και διαφορετικούς χρήστες, η χρήση απομακρυσμένης βάσης δεδομένων, ήταν μονόδρομος.
Η εμφάνιση των δεδομένων που λαμβάνονται από το API, πραγματοποιείται με λήψη json strings.

```
BufferedReader in = new BufferedReader(new
InputStreamReader(con.getInputStream()));
String inputLine;
StringBuilder response = new StringBuilder();

while ((inputLine = in.readLine()) != null)
{
    response.append(inputLine);
}
in.close();

String txt = response.toString();
JSONParser parser = new JSONParser();

Object obj = parser.parse(txt);

JSONObject jsonObject = (JSONObject) obj;
```

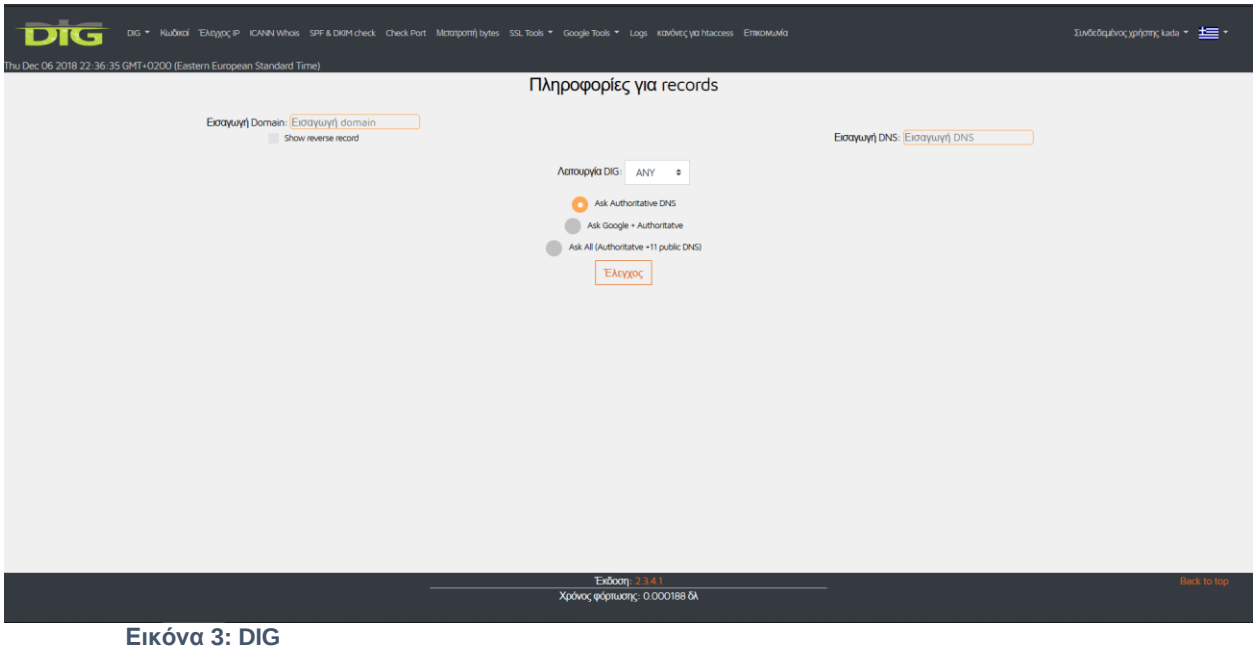
Όλα τα δεδομένα λαμβάνονται από τον buffer και έπειτα από επεξεργασία δημιουργείται ένα json object με όλα τα δεδομένα που έχουν ληφθεί από το API και στη συνέχεια θα εμφανιστούν στον χρήστη.

Σε όλες τις λειτουργίες της εφαρμογής, αφού ήδη έχει λάβει την έγκριση του χρήστη να χρησιμοποιεί το ενσωματωμένο GPS της συσκευής και αφού ξεκινήσει ο έλεγχος της ζητούμενης εργασίας, η εφαρμογή δημιουργεί ένα επιπλέον thread το οποίο λαμβάνει τις συντεταγμένες του χρήστη εκείνη την στιγμή και τις αποστέλλει στο API για να αποθηκευτούν στην βάση δεδομένων, ώστε να εμφανιστούν σε μελλοντικό σχετικό αίτημα (με τη χρήση του Google Maps).

Κεφάλαιο 4

Στο παρόν κεφάλαιο, γίνεται παρουσίαση των εφαρμογών που αναπτύχθηκαν και αναφέρονται λίγα λόγια για κάθε λειτουργία των διαφορετικών εργαλείων.

4.1 Παρουσίαση web εφαρμογής



Εικόνα 3: DIG

Κατά το άνοιγμα της web εφαρμογής, εμφανίζεται το μενού στο πάνω μέρος το οποίο περιλαμβάνει τις εξής επιλογές:

1. DIG
    a. Simple dig
    b. Multiple dig
2. Password Generator
3. IP Lookup
4. Whois (.com, .net και .edu domains)
5. SPF – DKIM & DMARC checker
6. Check Port
7. Bytes Transformation
8. SSL Tools
    a. CSR
    b. CRT
    c. Check SSL Cert
9. Google Tools
    a. Page Speed
    b. Mobile Friendly
10. Logs parser
11. .htaccess generator
12. Contact form

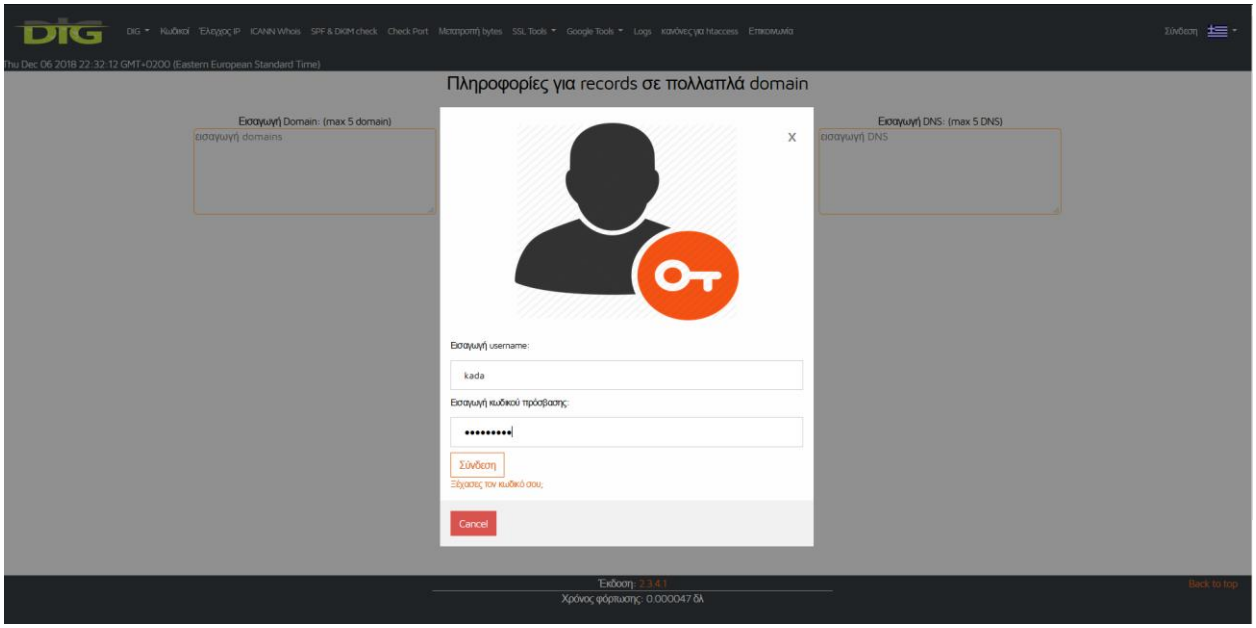
Το βασικό μενού της εφαρμογής βρίσκεται στην αριστερή πλευρά, δίπλα από το λογότυπο. Από την δεξιά πλευρά, εμφανίζεται η επιλογή της σύνδεσης (login) σε κάποιον περιηγητή που διαθέτει προσωπικό λογαριασμό. Εάν επιλέξει το “login”, θα εμφανιστεί ένα αναδυόμενο παράθυρο στην οθόνη ζητώντας τα στοιχεία εισόδου του χρήστη. Σε περίπτωση που δεν θυμάται τον κωδικό του, μπορεί να επιλέξει το σχετικό πεδίο “Forgot Your Password – Ξέχασες τον κωδικό σου”, ώστε συμπληρώνοντας το username του, να σταλεί ένα σχετικό μήνυμα ενεργοποίησης νέου κωδικού πρόσβασης, στο δηλωμένο email του χρήστη.
Σε περίπτωση που διαθέτει στοιχεία εισόδου και τα εισάγει σωστά, τότε στην θέση του “login” εμφανίζεται “Logged in as *username*” και υπάρχουν οι επιλογές Account Management (αλλαγή κωδικού πρόσβασης και λογαριασμού email) και Logout.
Τέλος, στην δεξιά πλευρά του μενού υπάρχει μια σημαία γλώσσας η οποία είναι ενεργή στην ιστοσελίδα. Επιλέγοντάς την, μπορεί να τροποποιηθεί είτε σε Αγγλικά, είτε σε Ελληνικά.
Στην κάτω πλευρά του παραθύρου, υπάρχει το footer της ιστοσελίδας το οποίο εμφανίζει την έκδοση της ιστοσελίδας. Επιλέγοντας την έκδοση, τότε σε νέο παράθυρο εμφανίζεται το σχετικό changelog στο οποίο περιγράφονται όλες οι αλλαγές και προσθήκες που έχουν πραγματοποιηθεί ανάλογα με την έκδοση. Ακριβώς από κάτω υπάρχει ο χρόνος φόρτωσης ολόκληρης της ιστοσελίδας από τον web server. Τέλος, στα δεξιά του footer, εμφανίζεται σχετική επιλογή “Back to top” για χάριν ευκολίας και συντομίας του χρήστη.

4.2 Λειτουργία web εφαρμογής

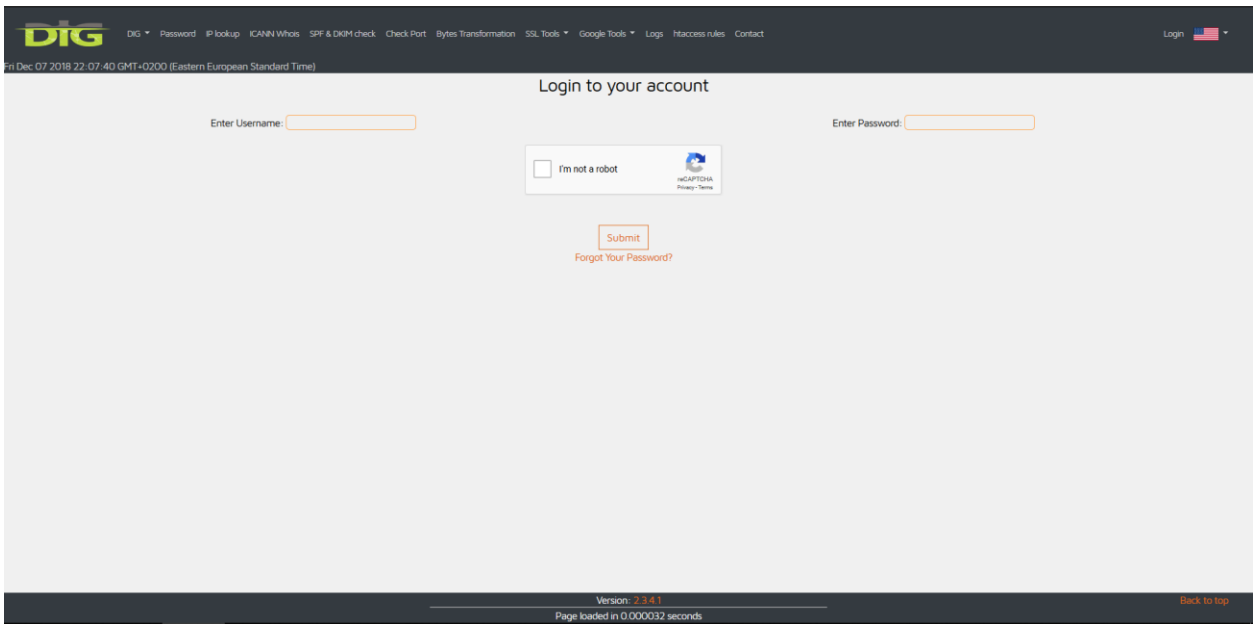
Η υλοποίηση της παρούσας μεταπτυχιακής διατριβής, περιλαμβάνει μια web εφαρμογή, στην οποία μπορούμε να περιηγηθούμε ως επισκέπτες, αλλά και να συνδεθούμε για περισσότερες λειτουργίες και επιπλέον μια Android εφαρμογή. Και στις 2 εφαρμογές, υπάρχουν οι ίδιες λειτουργίες, και εμφανίζουν ακριβώς τα ίδια αποτελέσματα. Χαρακτηριστική διαφορά είναι στο ότι η εφαρμογή Android απαιτεί την σύνδεση του χρήστη, ώστε να αποτραπεί κακόβουλη χρήση, ενώ η χρήση της web εφαρμογής δεν θέτει περιορισμούς εξαρχής, αλλά παρακολουθεί τα μοτίβα αναζητήσεων και θέτει όποιους περιορισμούς πρέπει, στην πορεία. Σε περίπτωση που ο χρήστης διαθέτει λογαριασμό, μπορεί να συνδεθεί και να αρθούν οι περιορισμοί. Σε κάθε περίπτωση, όλες οι αναζητήσεις και ενέργειες των χρηστών, αποθηκεύονται και γίνεται τακτικά έλεγχος για μη εξουσιοδοτημένη χρήση ή / και προσπάθεια κακόβολης χρήσης της εφαρμογής.

4.2.1 Login χρήστη

Ο χρήστης έχει την δυνατότητα να συνδεθεί μέσω αναδυόμενου παραθύρου (pop up), που υπάρχει στην δεξιά πλευρά του μενού. Εφόσον τα στοιχεία εισόδου είναι σωστά, το login πραγματοποιείται με επιτυχία και γίνεται reload η σελίδα στην οποία βρισκόταν. Εφόσον τα στοιχεία είναι λανθασμένα, είτε δεν υπάρχει ο χρήστης, γίνεται ανακατεύθυνση στην σελίδα του login που υπάρχει και captcha για προστασία απέναντι σε brute force επιθέσεις.



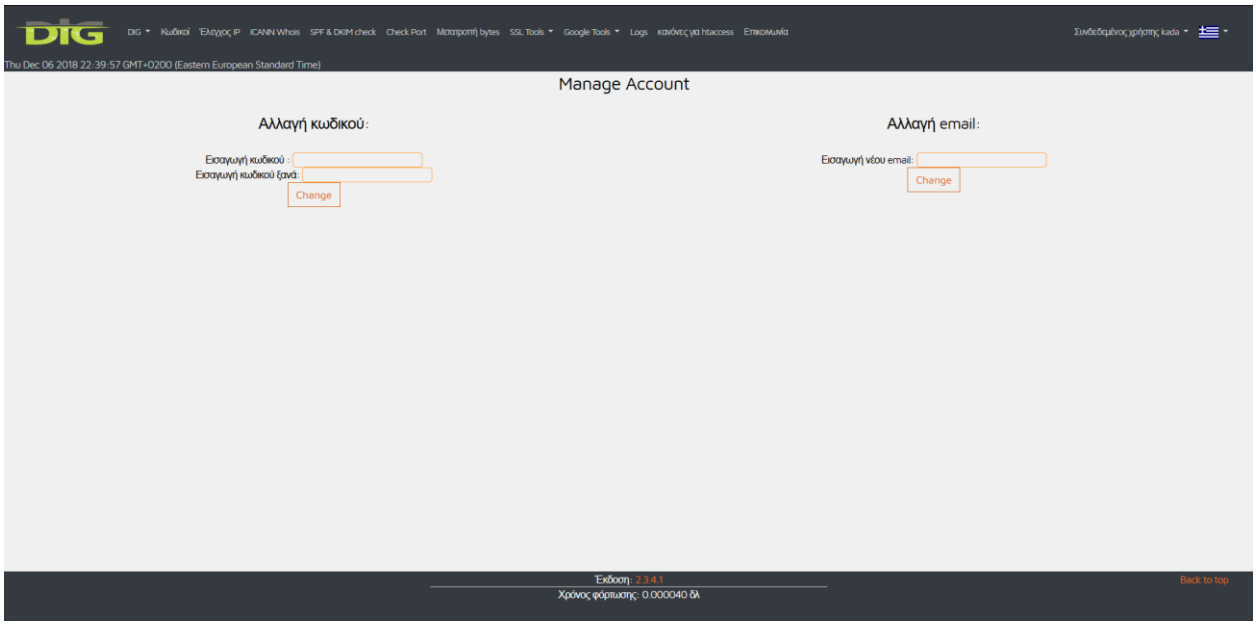
Εικόνα 4: Login



Εικόνα 5: Login with captcha

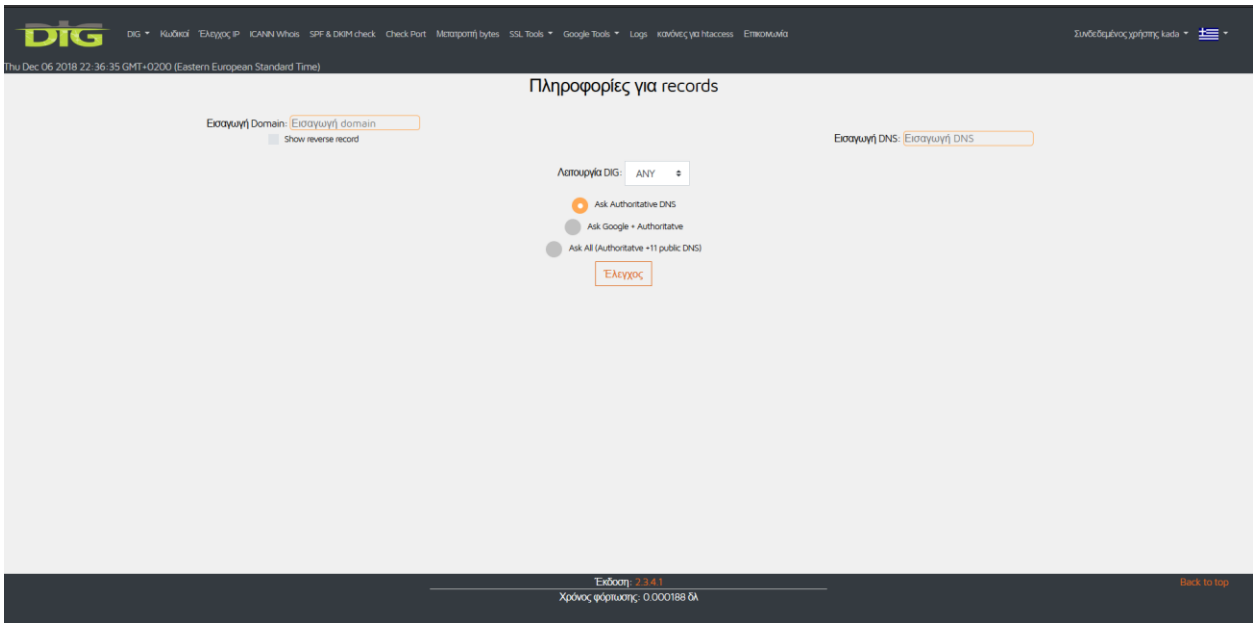
4.2.2 Περιβάλλον αλλαγής κωδικού και email

Αφού ο χρήστης έχει συνδεθεί επιτυχώς έχουν αρθεί όλοι οι περιορισμοί στην εφαρμογή, αλλά η καταγραφή δεδομένων και κινήσεων δεν σταματάει. Ο χρήστης δεν πρόκειται να δει προειδοποιητικό μήνυμα κατάχρησης της εφαρμογής, ωστόσο δεν θα πρέπει να γίνει μη ορθή χρήση. Μπορεί να επιλέξει το manage account ώστε να τροποποιήσει τον κωδικό πρόσβασής του ή το email το οποίο έχει δηλωθεί (το email χρησιμοποιείται για ανάκτηση κωδικού).



Εικόνα 6: account management

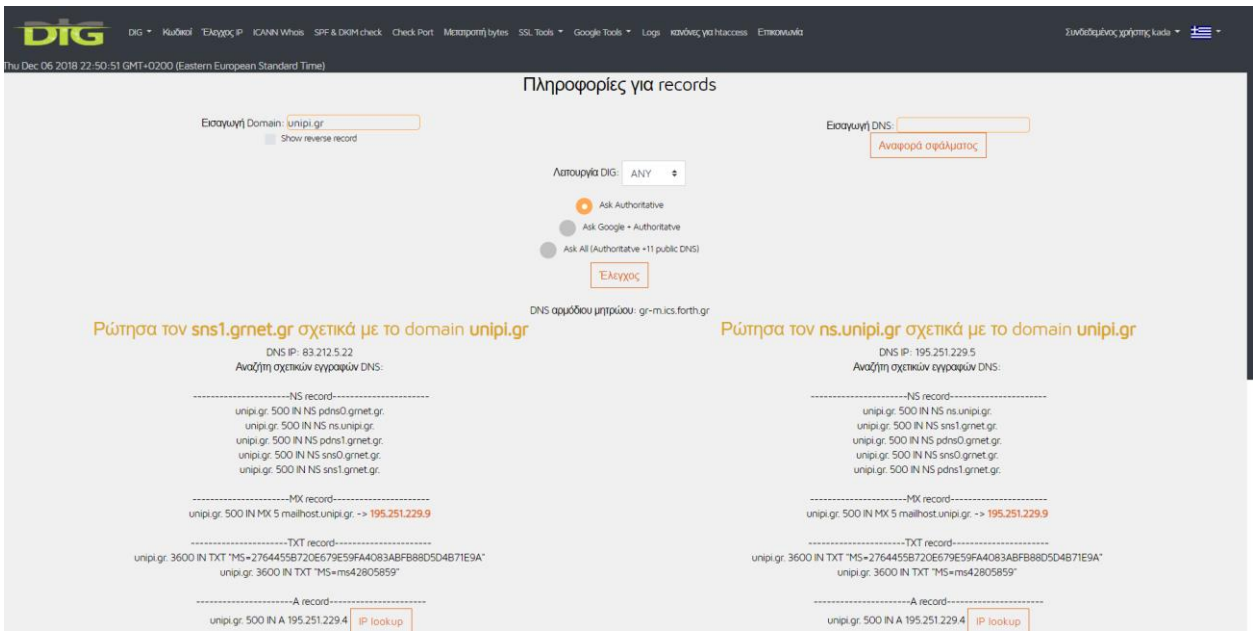
4.2.3 Αρχική σελίδα - DIG



Εικόνα 7: simple dig

Η πρώτη σελίδα της web εφαρμογής, είναι η πιο σύνθετη λειτουργία της ιστοσελίδας. Ολοκληρώνει την εύρεση των σχετικών records από τους DNS ενός domain που εισάγει ο χρήστης. Από τα διαθέσιμα πεδία, μπορεί να εισάγει 1 domain και έως 1 DNS (προαιρετικά). Ως επιλογές μπορεί να αφήσεις τις default ώστε να γίνουν αναζητήσεις μόνο στους δηλωμένους DNS του domain (authoritative DNS) ή να προσθέσει μόνο τη Google στα αποτελέσματα ή να επιλέξει τους authoritative DNS και επιπλέον ακόμη 11 public DNS. Η τελευταία λειτουργία απαιτεί 20-40 δευτερόλεπτα, καθώς οι αναζητήσεις που πρέπει να ολοκληρωθούν, είναι πολλές. Επιπλέον, μπορεί να επιλεγεί ως record αναζήτησης όχι το ANY που περιλαμβάνει A, MX, NS, MX, CNAME και txt record, αλλά οποιοδήποτε επιθυμεί, μεμονωμένα. Η εμφάνιση αποτελεσμάτων γίνεται σε δύο διαφορετικές στήλες όταν η ιστοσελίδα λειτουργεί μέσω υπολογιστή και σε μια στήλη όταν ανοίξει από κινητή συσκευή.

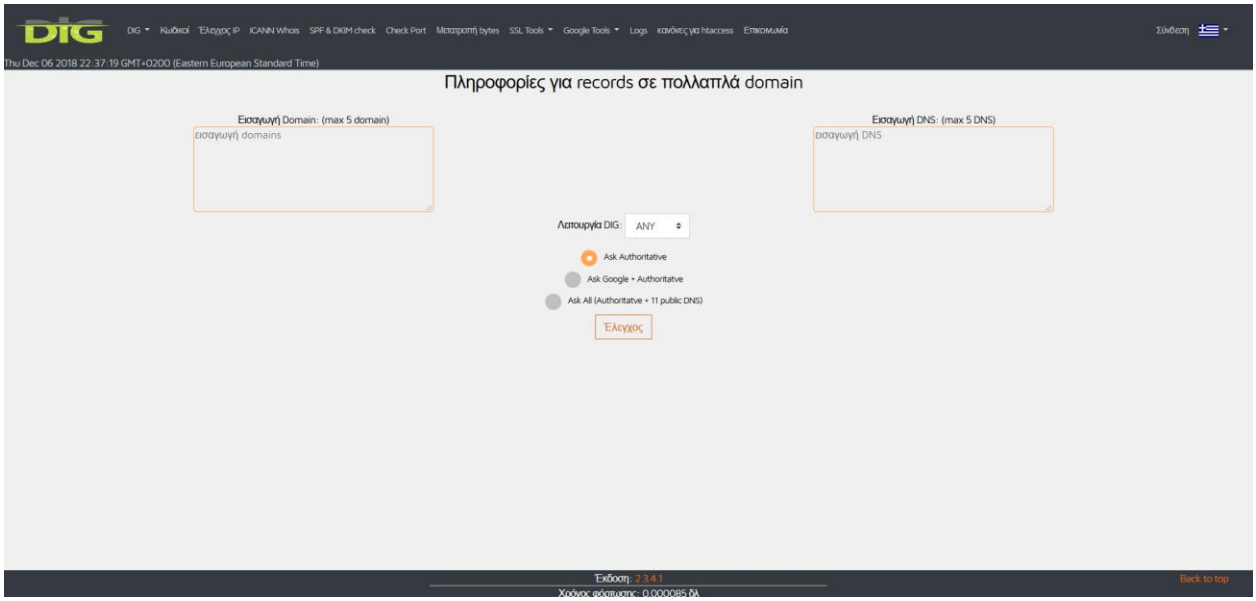
Το αποτέλεσμα της λειτουργίας του dig είναι το ακόλουθο (έχει επιλεγεί το ANY και μόνο authoritative DNS):



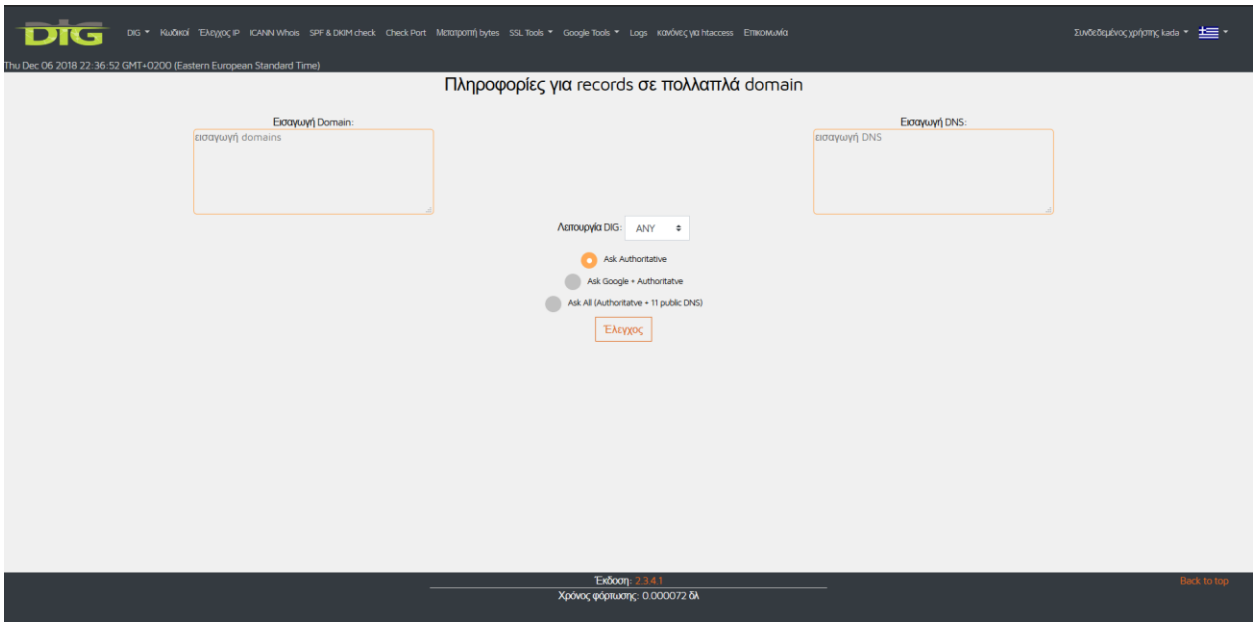
Εικόνα 8: simple dig complete

4.2.4 Πολλαπλό DIG

Παρόμοια λειτουργία με το απλό dig, με τη διαφορά ότι ο χρήστης μπορεί να εισάγει πολλαπλά domains και πολλαπλούς DNS για να γίνει μαζικά έλεγχος. Όλοι οι επισκέπτες έχουν περιορισμό σε 5 domains και 5 DNS, ενώ οι συνδεδεμένοι χρήστες, μπορούν απεριόριστο αριθμό αναζητήσεων.



Εικόνα 9: multiple dig



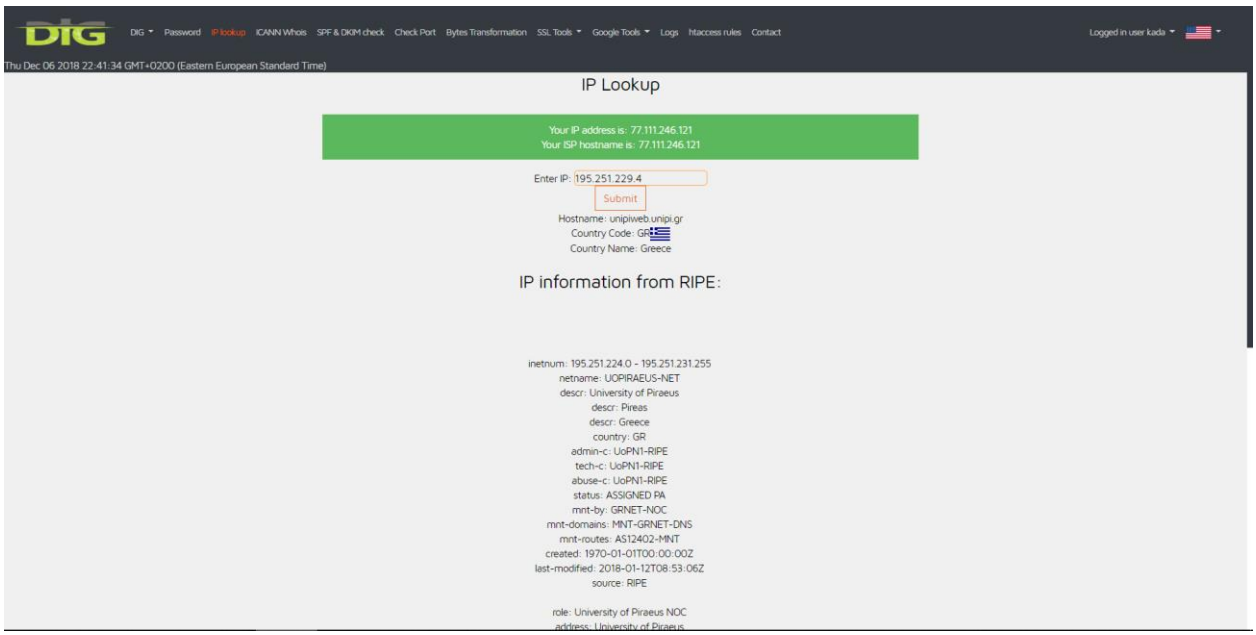
Εικόνα 10: multiple dig logged in

Δεν υπάρχει κάποιος διαχωρισμός μεταξύ των DNS και των domains (δηλαδή όλα τα domains θα ρωτήσουν τους DNS που έχει εισάγει ο χρήστης, τους DNS του μητρώου (authoritative) και – προαιρετικά – την Google).

4.2.5 IP Lookup

Ως εργαλείο έχει υλοποιηθεί ένα ip lookup, το οποίο ελέγχει την IP που εισάγει ο χρήστης και εμφανίζει τα αποτελέσματα που λαμβάνει. Σε αυτά συμπεριλαμβάνονται η χώρα στην οποία ανήκει, η εταιρία που την έχει μισθώσει, πότε μισθώθηκε και κάποιες επιπλέον πληροφορίες σχετικά με την εταιρία στην οποία ανήκει. Κάτω από το μενού, υπάρχει σε πράσινο πλαίσιο, η IP της σύνδεσης του χρήστη και το hostname της συγκεκριμένης IP διεύθυνσης.

Οι πληροφορίες που λαμβάνονται είναι στα Αγγλικά ως γλώσσα και δεν υπάρχει μετάφραση στα Ελληνικά, καθώς οι πληροφορίες προέρχονται από Αμερικάνικες πηγές και πιο συγκεκριμένα την RIPE.



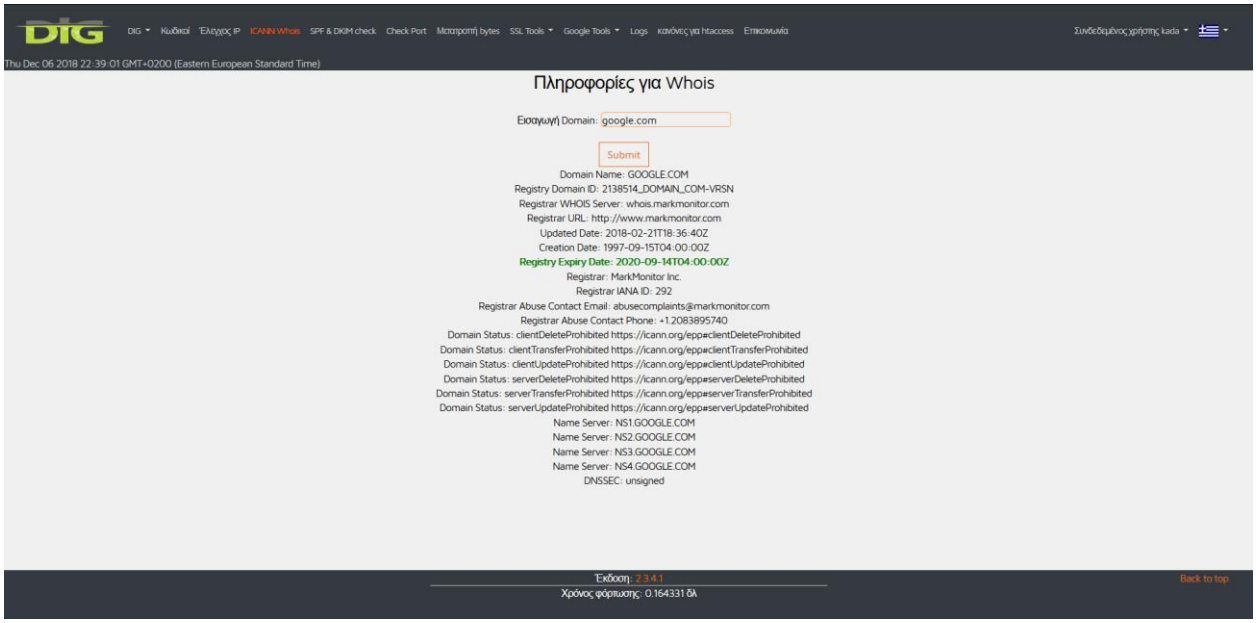
Εικόνα 11: ip lookup

4.2.6 Whois (.com, .net και .edu domains)

Μέσω της εντολής whois, λαμβάνονται πληροφορίες για τα υποστηριζόμενα domains, για τα οποία εμφανίζονται πληροφορίες σχετικά με ημερομηνία κατοχύρωσης, ημερομηνία λήξης, ποιος είναι ο καταχωρητής του, abuse email, ιστοσελίδα και στοιχεία επικοινωνίας με τον καταχωρητή και ποιο είναι το status του domain:

1. clientDeleteProhibited: το μητρώο απορρίπτει αίτημα διαγραφής του domain
2. clientTransferProhibited: το μητρώο απορρίπτει αίτημα μεταφοράς του domain
3. clientUpdateProhibited: το μητρώο απορρίπτει αίτημα αλλαγής του domain
4. serverDeleteProhibited: δεν μπορεί να γίνει deleted
5. serverTransferProhibited: δεν μπορεί να μεταφερθεί σε άλλο καταχωρητή
6. serverUpdateProhibited: δεν μπορεί να γίνει update (αλλαγή DNS, contacts κλπ)
7. clientHold: το domain έχει κατάσταση Suspended
8. clientOK: το domain έχει κατάσταση OK και καμία από τους παραπάνω περιορισμούς[19]

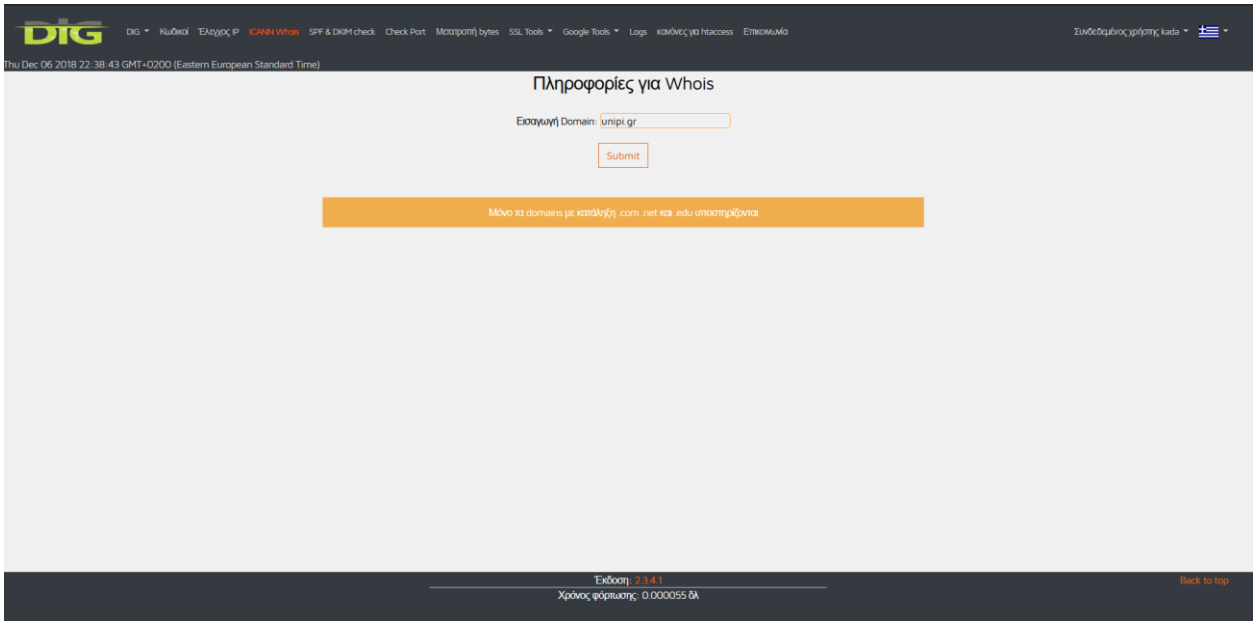
Η διαφορά μεταξύ του client και server, είναι στο ότι τα status που αναφέρουν client ορίζονται από τον καταχωρητή ενώ όπου αναφέρει server, ορίζονται από το αρμόδιο μητρώο.



Εικόνα 12: whois for com domain

Για τις υπόλοιπες καταλήξεις, δεν υποστηρίζεται whois μέσω της συγκεκριμένης εφαρμογής και εμφανίζεται σχετικό μήνυμα:

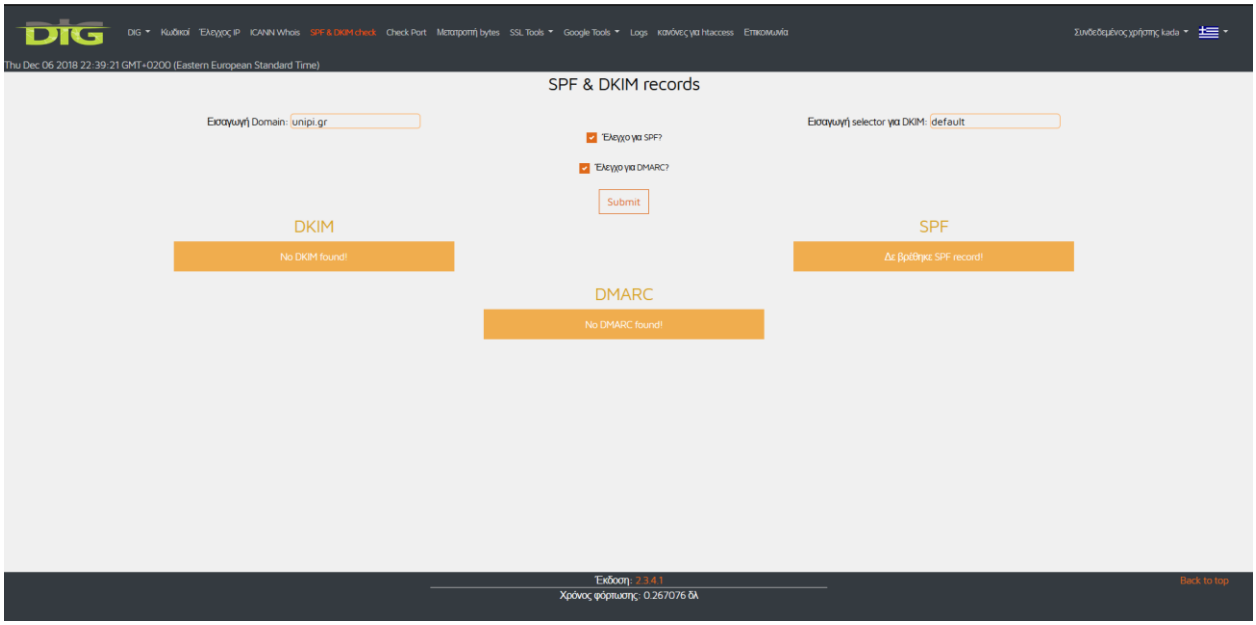
[19] EPP Status Codes. icann. Weblog.
Available from: https://www.icann.org/resources/pages/epp-status-codes-2014-06-16-en
[Accessed 8th Dec 20018]



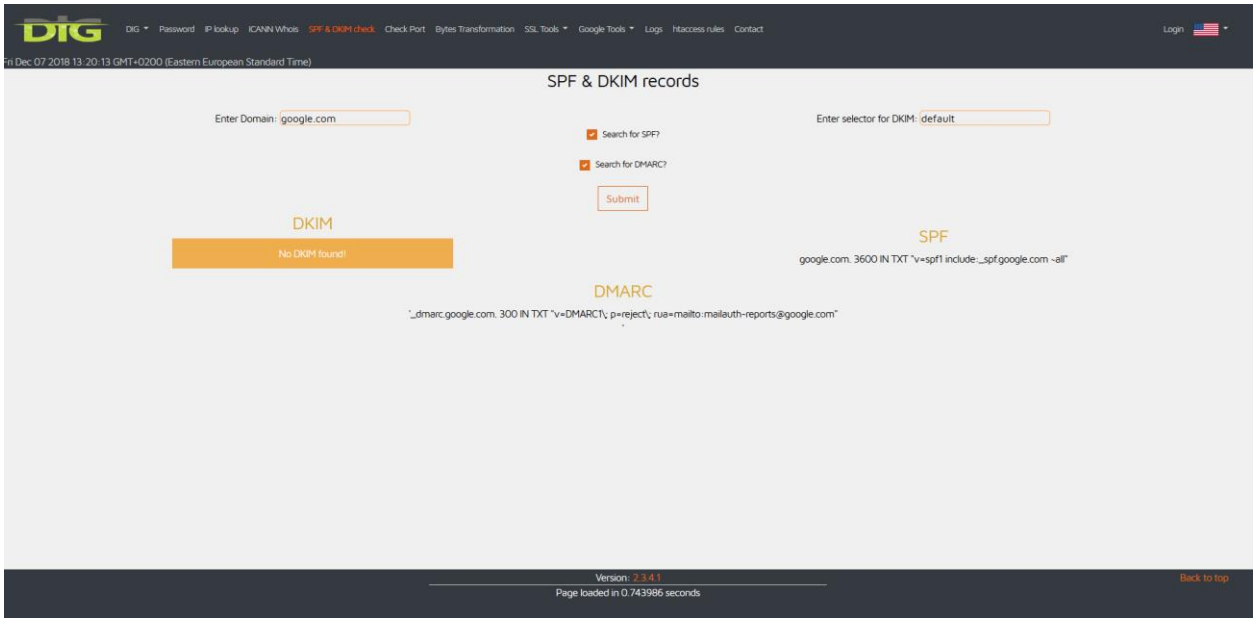
Εικόνα 13: whois for gr domain

4.2.7 SPF, DKIM και DMARC checker

Βάσει όσων έχουν ήδη αναφερθεί στην παράγραφο 3.2 Μεθοδολογία, για την λειτουργία των records που αφορούν τα emails του domain, η παρούσα εφαρμογή βρίσκει τα σχετικά records και τα εμφανίζει στον χρήστη. Με αυτόν τον τρόπο αφενός ο χρήστης παρατηρεί ότι όντως υπάρχουν και αφετέρου μπορεί να επιβεβαιώσει ότι είναι σωστά. Σε περίπτωση που λείπει κάποιο record, τότε στη θέση της εγγραφής, υπάρχει σχετικό μήνυμα.



Εικόνα 14: domain with no spf, dkim and dmarc

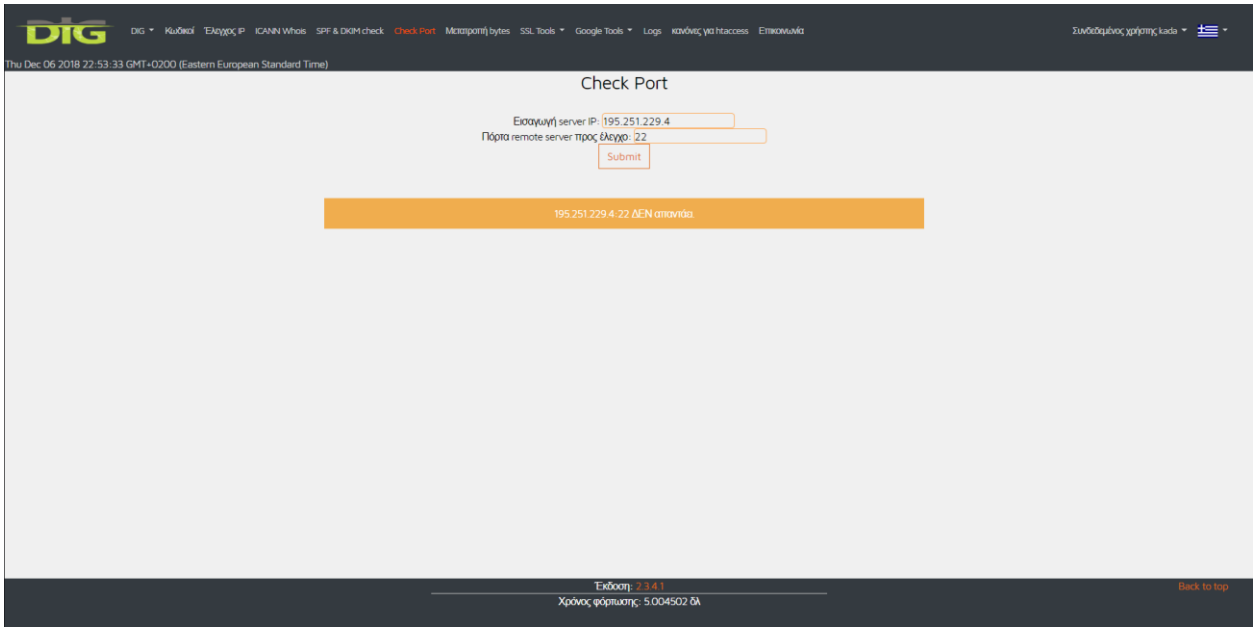


Εικόνα 15: domain with records

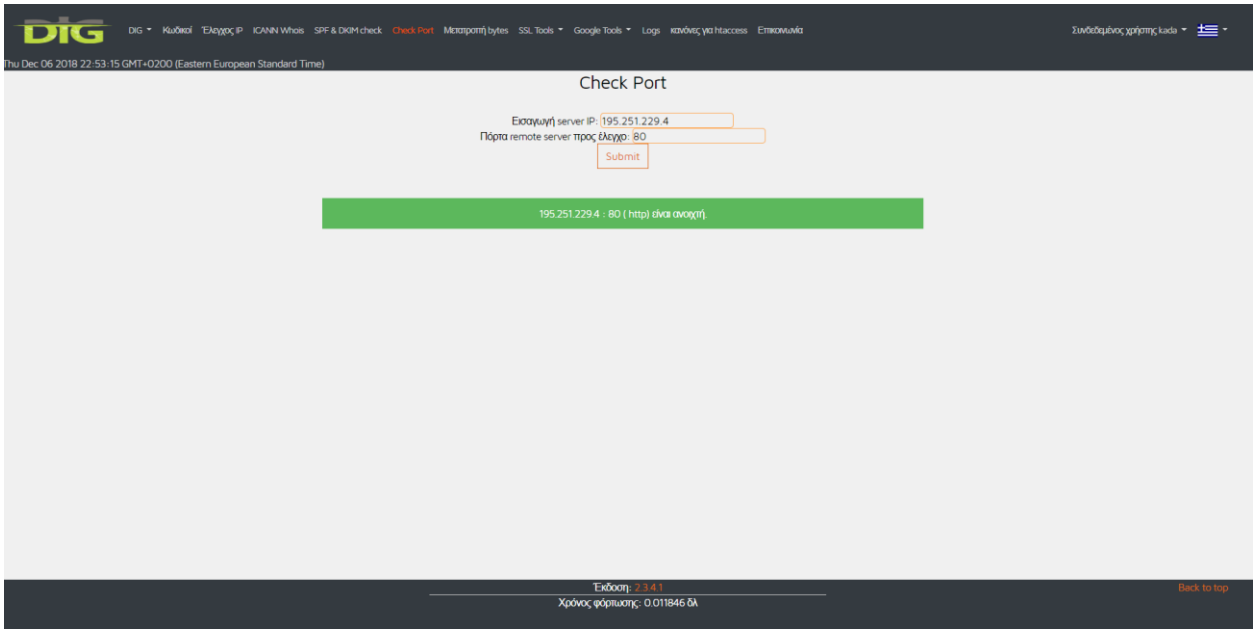
4.2.8 Check Port

Υπάρχουν πολλές περιπτώσεις που έχει χρειαστεί να ελέγξουμε εάν κάποια ενέργεια που έχει ολοκληρωθεί, έχει λάβει ισχύ. Σε περιπτώσεις server με ενεργά firewalls που αποκόπτουν πόρτες πρόσβασης, χρειαζόμαστε ένα εργαλείο ώστε να ελέγξουμε εάν μια συγκεκριμένη πόρτα του server είναι ανοιχτή για συνδέσεις (και συνεπώς εάν οι ενέργειες που ολοκληρώσαμε,

έλαβαν ισχύ). Άλλες περιπτώσεις, θέλουμε να βρούμε ενδεχόμενα κενά ασφαλείας στον server μας, ελέγχοντας τις πόρτες που έχει ανοιχτές, ώστε να απενεργοποιήσουμε την πρόσβαση σε αυτές ή έστω να περιορίσουμε.
Στην παρούσα διπλωματική διατριβή, έχει αναπτυχθεί ένα τέτοιο εργαλείο, χρησιμοποιώντας την bash εντολή telnet που ουσιαστικά ελέγχει εάν μπορεί να συνδεθεί σε μια συγκεκριμένη πόρτα μιας IP διεύθυνσης. Έγινε η χρήση της telnet και όχι υλοποίηση με δημιουργία sockets, για να αποτραπεί κακόβουλη χρήση, κάνοντας port scan.



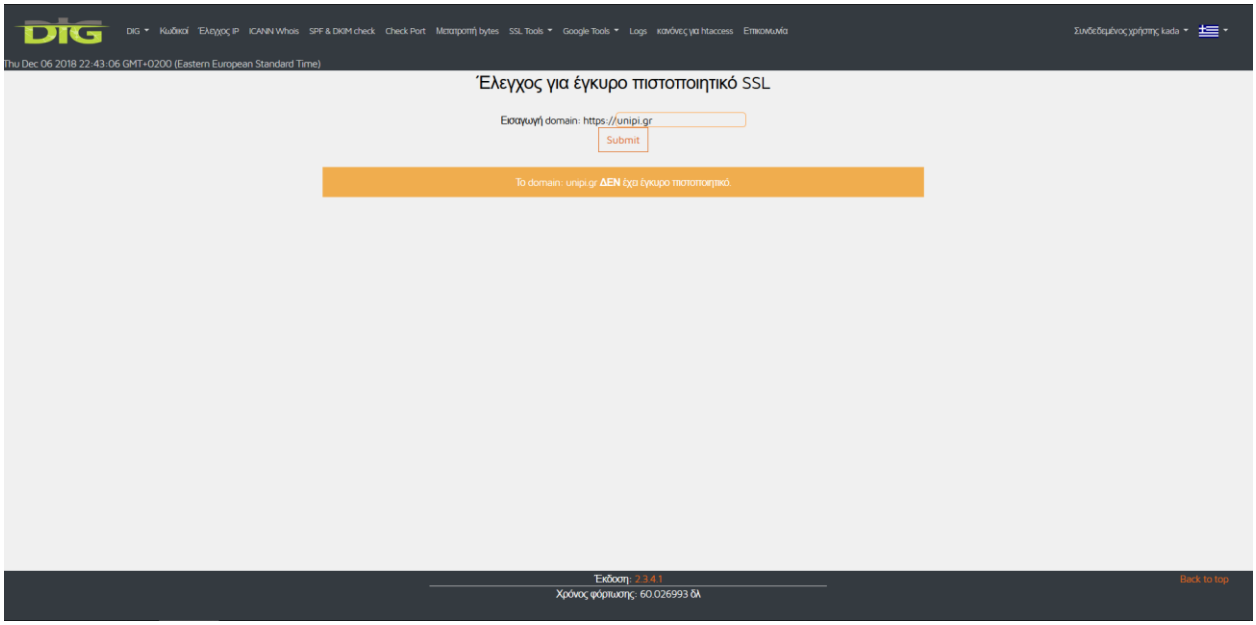
Εικόνα 16: port closed



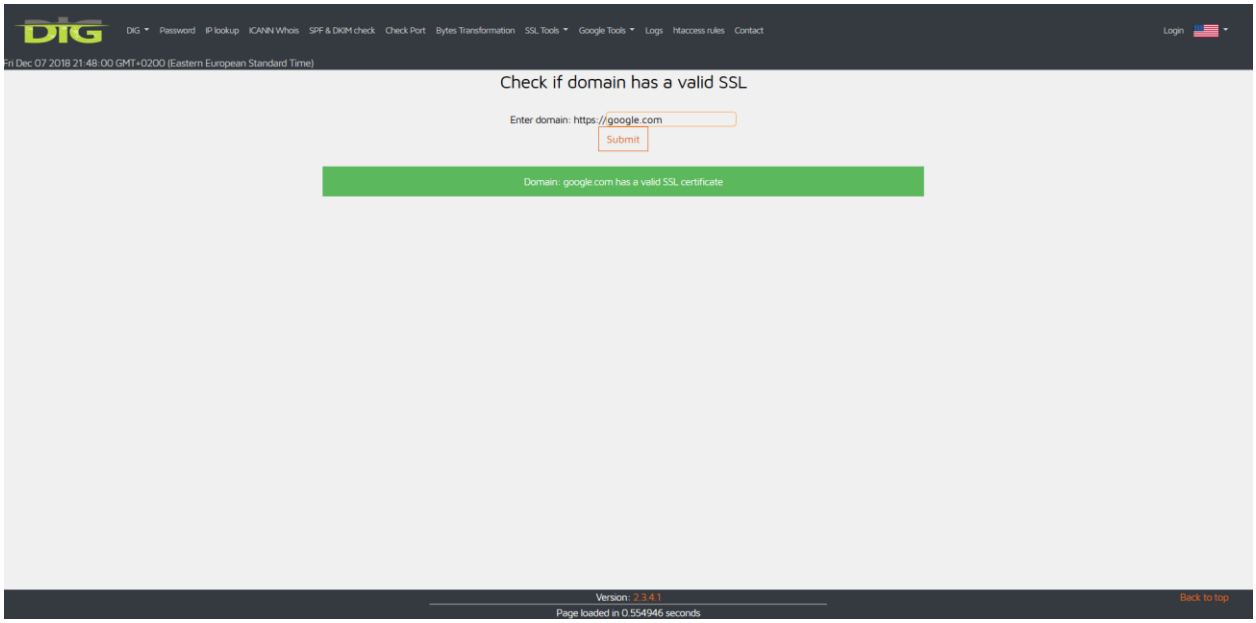
Εικόνα 17: port closed

4.2.9 SSL check & CRT + CSR Decoder

Μπορούμε να ελέγξουμε μέσω δημιουργίας connection μέσω socket, εάν ένα domain (ή και subdomain), έχουν ενεργό και σωστά εγκατεστημένο πιστοποιητικό SSL. Ο έλεγχος επιστρέφει εάν υπάρχει ή όχι SSL στην ιστοσελίδα, χωρίς να επιστρέψει πληροφορίες, εάν είναι ληγμένο, έχει λάθος παραμετροποίηση ή δεν υπάρχει.

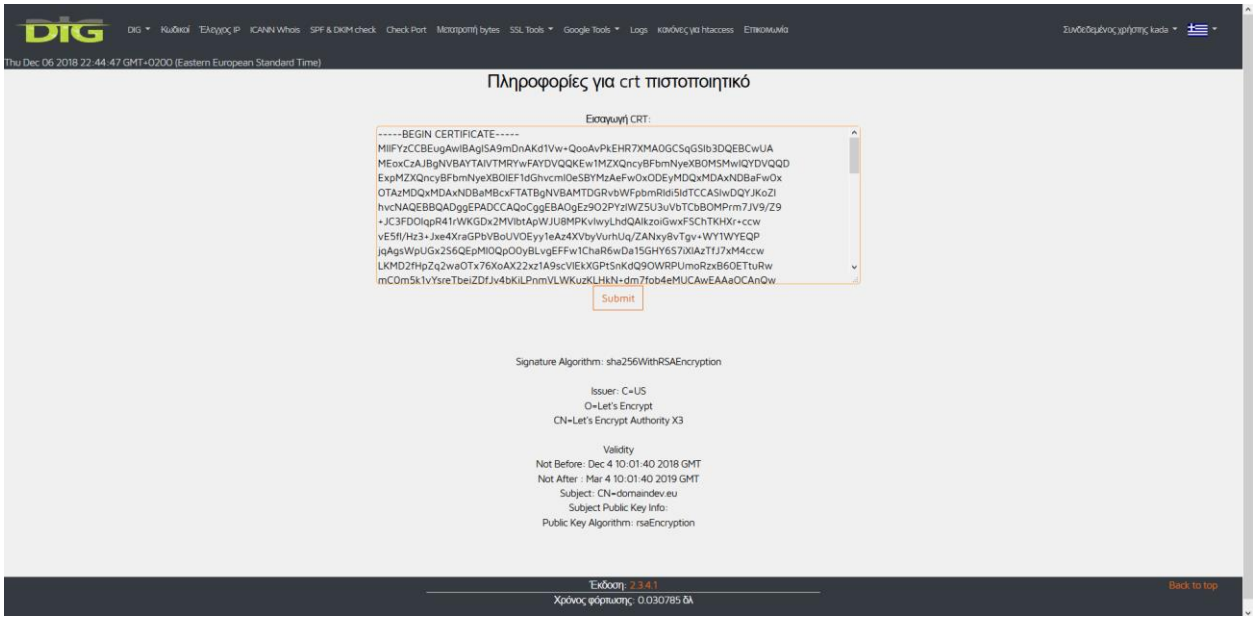


Εικόνα 18: ssl check fail

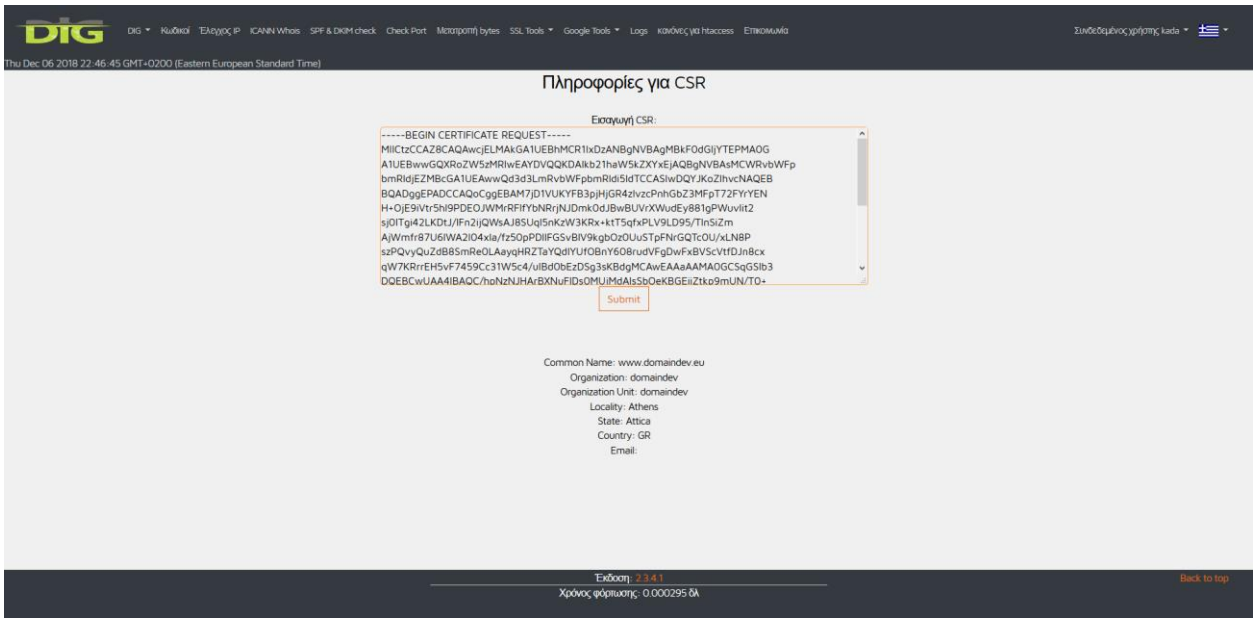


Εικόνα 19: ssl check success

Επιπλέον, μπορεί ο χρήστης να επιβεβαιώσει τις πληροφορίες που υπάρχουν σε ένα κωδικοποιημένο CSR ή CRT αρχείο που διαθέτει, πριν προβεί σε κάποια ενέργεια



Εικόνα 20: crt decode

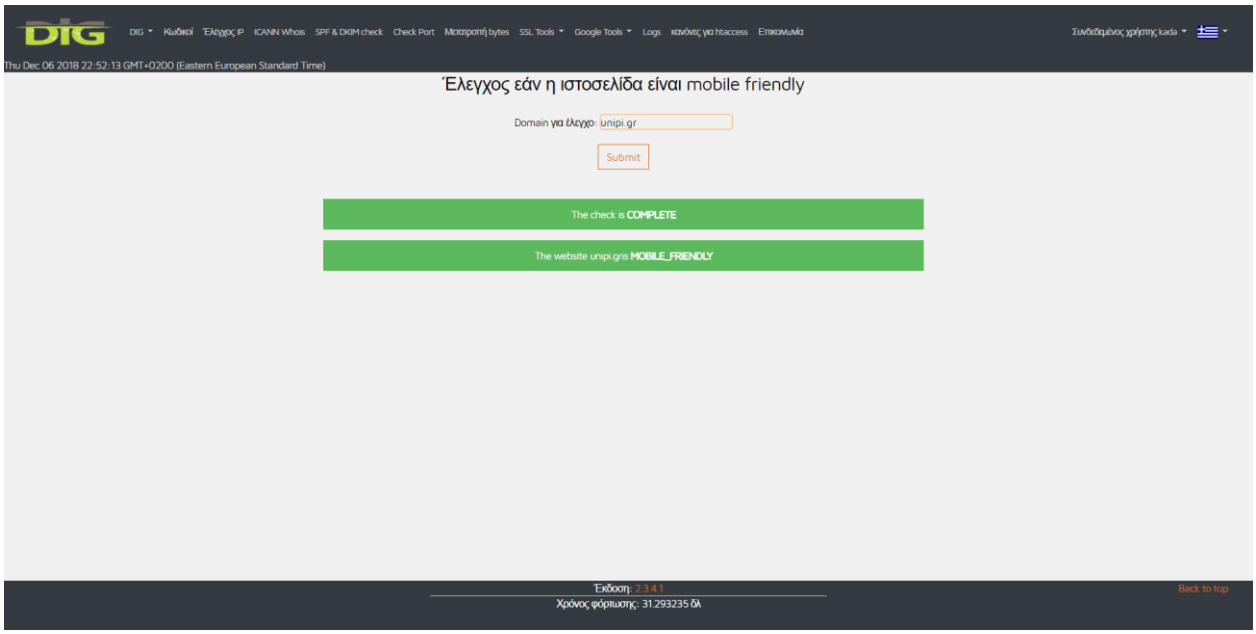


Εικόνα 21: csr decode

4.2.10 Google Tools – Mobile Friendly & Page Speed

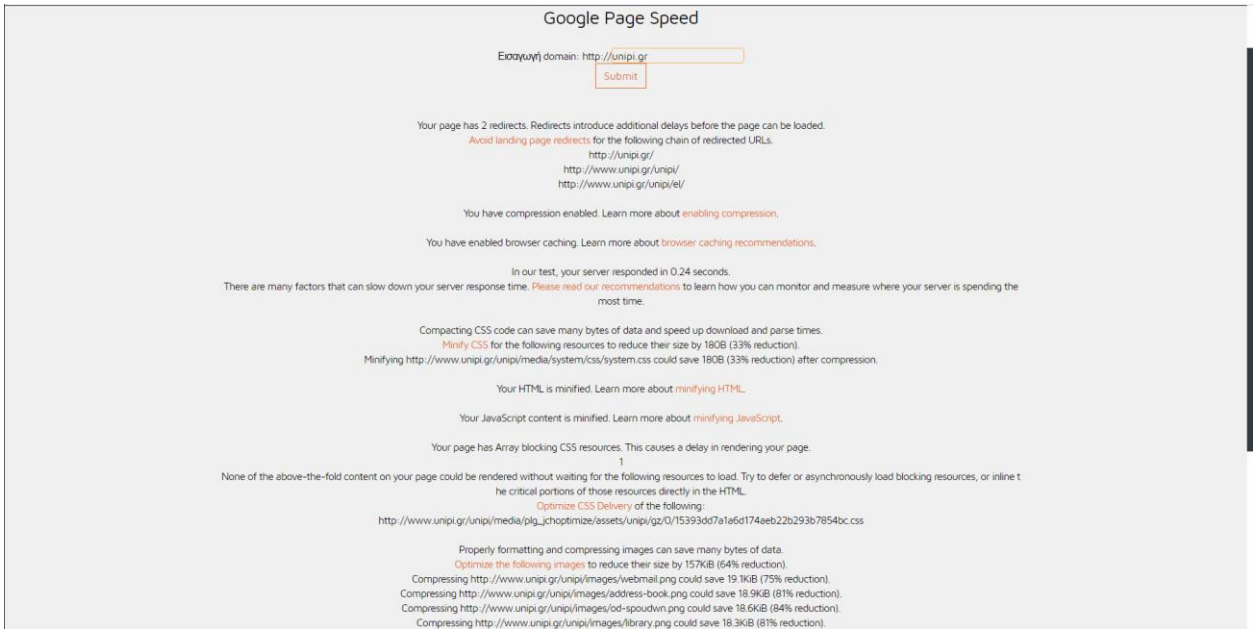
Από το dropdown menu Google Tools, υπάρχουν διαθέσιμες οι επιλογές για

a) έλεγχο εάν η ιστοσελίδα είναι mobile friendly (δηλαδή εάν προσαρμόζεται στις κινητές συσκευές και γενικά σε συσκευές με οθόνη μικρότερη από αυτή των υπολογιστών).



Εικόνα 22: mobile friendly

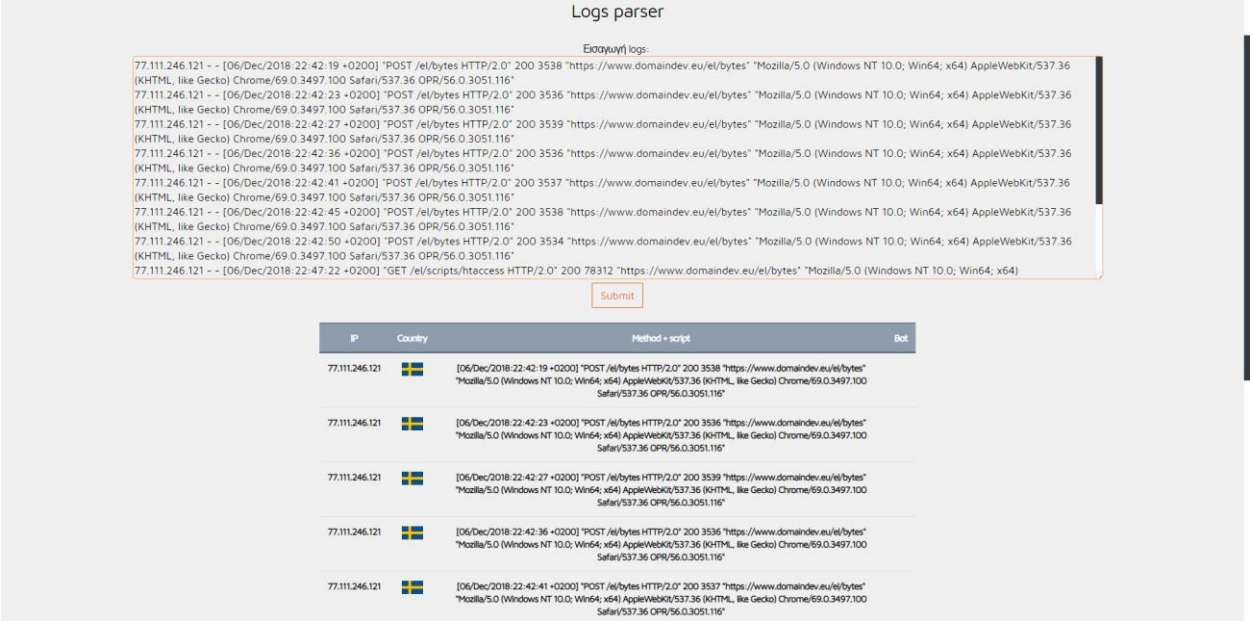
b) Γίνεται φόρτωση του url που ορίζει ο χρήστης και η Google εμφανίζει πληροφορίες και συμβουλές βελτίωσης της ταχύτητας και απόδοσης, με βάση το συγκεκριμένο url. Στα αποτελέσματα, συμπεριλαμβάνονται και σχετικοί σύνδεσμοι για περισσότερες πληροφορίες που μπορεί να αναζητήσει ο χρήστης.



Εικόνα 23: google page speed

4.2.11 Logs Parser

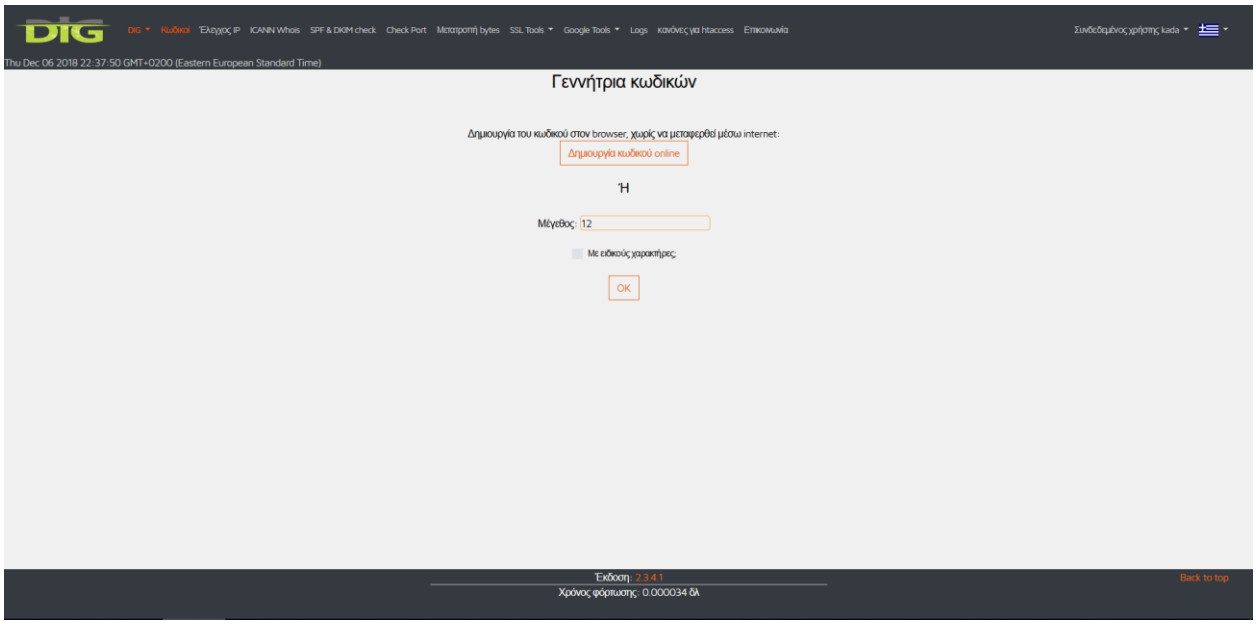
Διαθέσιμη επιλογή της εφαρμογής έγινε κοντά στο τέλος της διπλωματικής εργασίας, ένας logs parser. Ουσιαστικά, ο χρήστης εισάγει το μεγάλο κείμενο που βλέπει από τις καταγραφές που παράγει η ιστοσελίδα (τα αποκαλούμενα access logs) και το εργαλείο αναλαμβάνει να τα εμφανίσει με πιο όμορφο και κατανοητό τρόπο. Επίσης ξεχωρίζει την IP των requests, την χώρα προέλευσής της, το κυρίως σώμα του request που περιλαμβάνει το url, ημερομηνία και τύπο request και τέλος το bot ή τον agent ο οποίος ολοκλήρωσε το request.



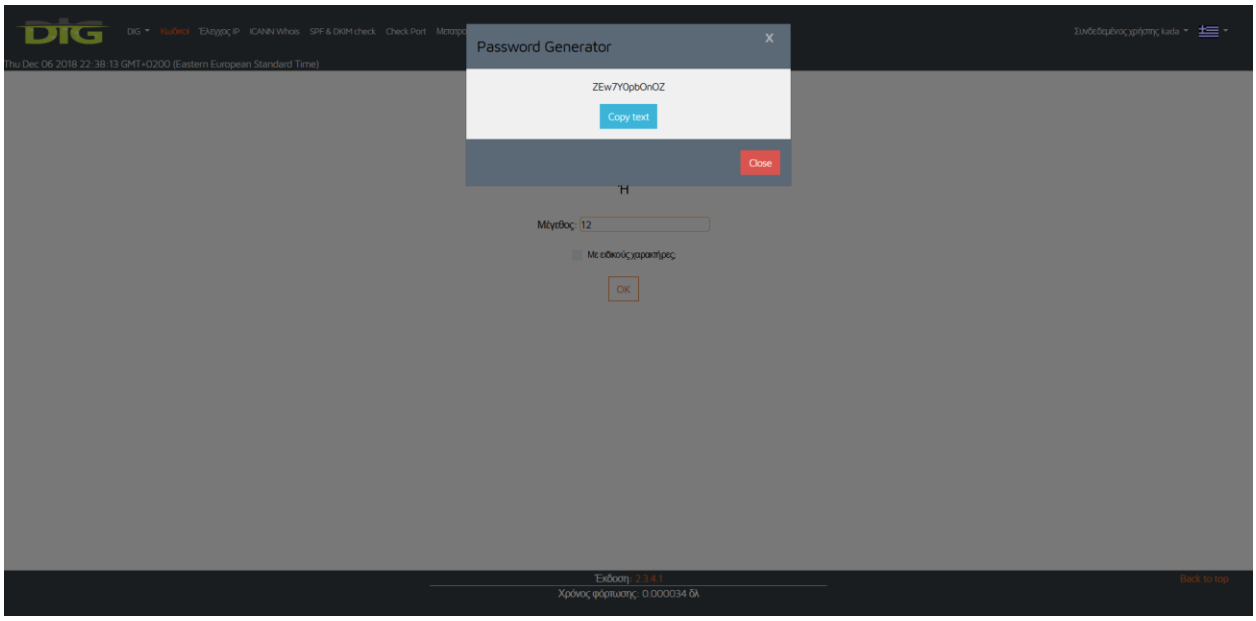
Εικόνα 24: logs decoder

4.2.12 Password Generator (client and server side)

Ένας password generator έχει μεταβλητό μήκος χαρακτήρων και δίνεται η επιλογή εάν θα παραχθούν ειδικά σύμβολα (θαυμαστικό, δίεση, δολάριο κλπ) ή όχι. Επειδή κατά την υλοποίηση της εφαρμογής, υπήρχε ως γνώμονας η ασφάλεια, έχει δημιουργηθεί ένας επιπλέον password generator, ο οποίος δεν παράγει τον κωδικό στον server και στην συνέχεια τον αποστέλλει στον browser, αλλά παράγεται κατευθείαν στον browser του επισκέπτη, ώστε να αυξηθεί η ασφάλεια στην μεταφορά ευαίσθητων δεδομένων.



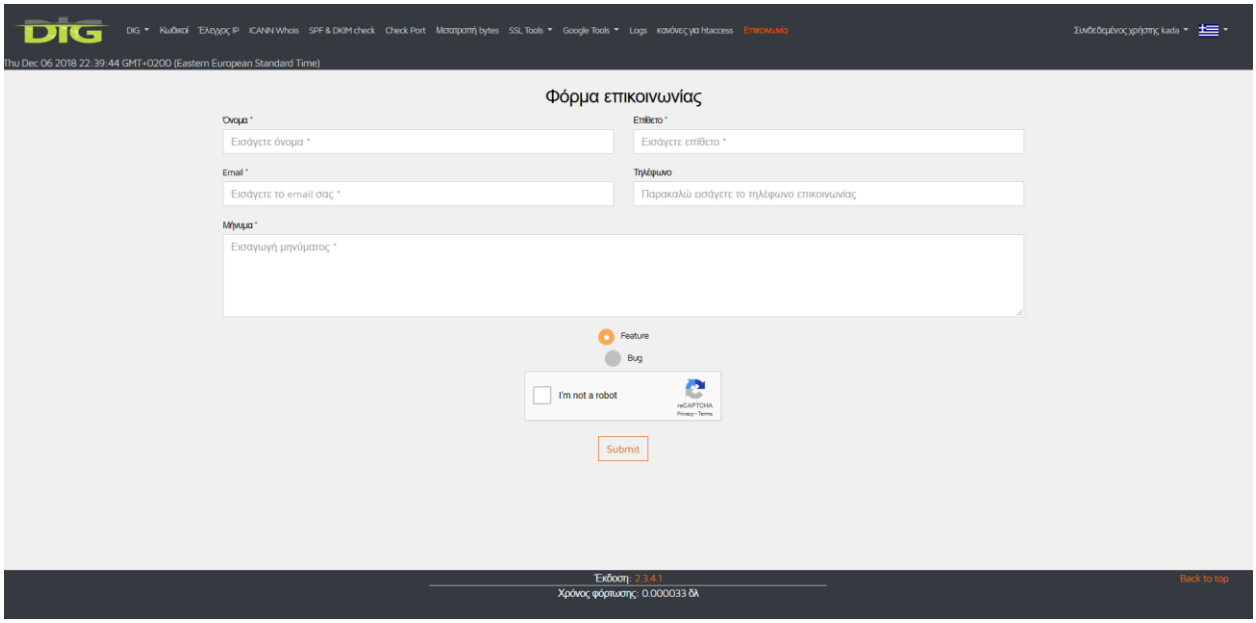
Εικόνα 25: password generator



Εικόνα 26: password generator javascript

4.2.13 Contact - Φόρμα επικοινωνίας

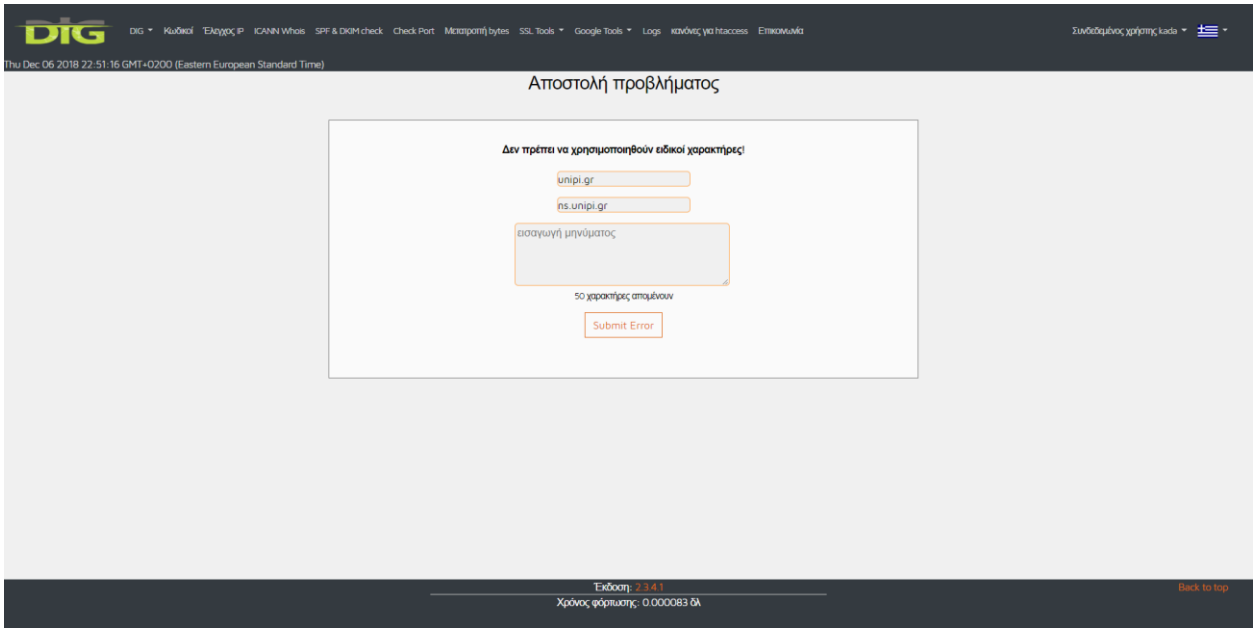
Έχει υλοποιηθεί μια απλή φόρμα επικοινωνίας, ώστε οποιοσδήποτε χρήστης να μπορεί να επικοινωνήσει και να αποστείλει είτε κάποιο report, είτε να ζητήσει κάποιο feature request. Στο τέλος της φόρμας, υπάρχει captcha και εφόσον επιλυθεί, θα είναι valid οι πληροφορίες που θα αποσταλούν. Η αποστολή του email από την contact form, γίνεται άμεσα με το submit της φόρμας.



Εικόνα 27: contact form

4.2.14 Error reporting – Αναφορά σφάλματος

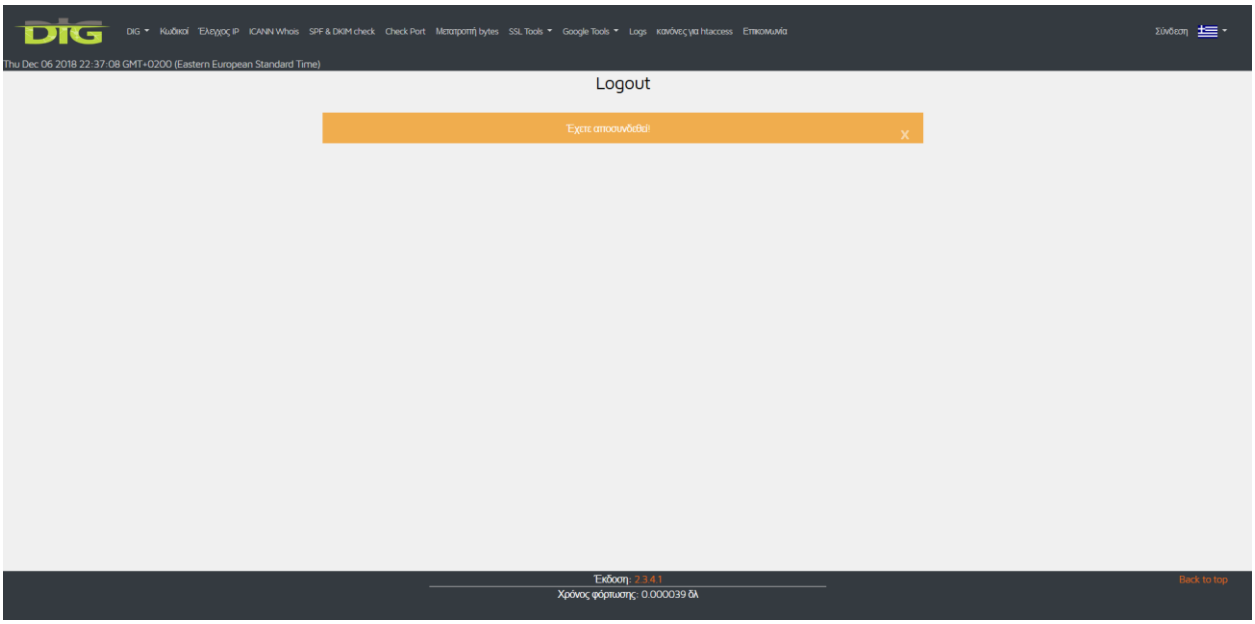
Αφού ο χρήστης ολοκληρώσει μια αναζήτηση records, κάτω από το πεδίο εισαγωγής DNS, εμφανίζεται ένα κουμπί που μπορεί να αναφέρει ένα σφάλμα ή κάποιο λάθος. Ανοίγει σε νέα καρτέλα στον browser το error reporting και έχει προ-συμπληρωμένα τα πεδία domain και NS. Ο χρήστης μπορεί να εισάγει ένα μικρό κείμενο με μέγιστο αριθμό 50 χαρακτήρων ώστε να αναφέρει το λάθος.
Όλα τα δεδομένα που συμπληρώνει ο χρήστης, αποθηκεύονται στην βάση δεδομένων και μαζικά 1 φορά την ημέρα, συγκεντρώνονται τα reports και αποστέλλονται με email.



Εικόνα 28: error reporting

4.2.15 Logout

Αφού ο χρήστης επιθυμεί να αποσυνδεθεί, μπορεί να επιλέξει το username του -> Logout. Το ενεργό session τερματίζεται και εμφανίζεται σχετικό μήνυμα.

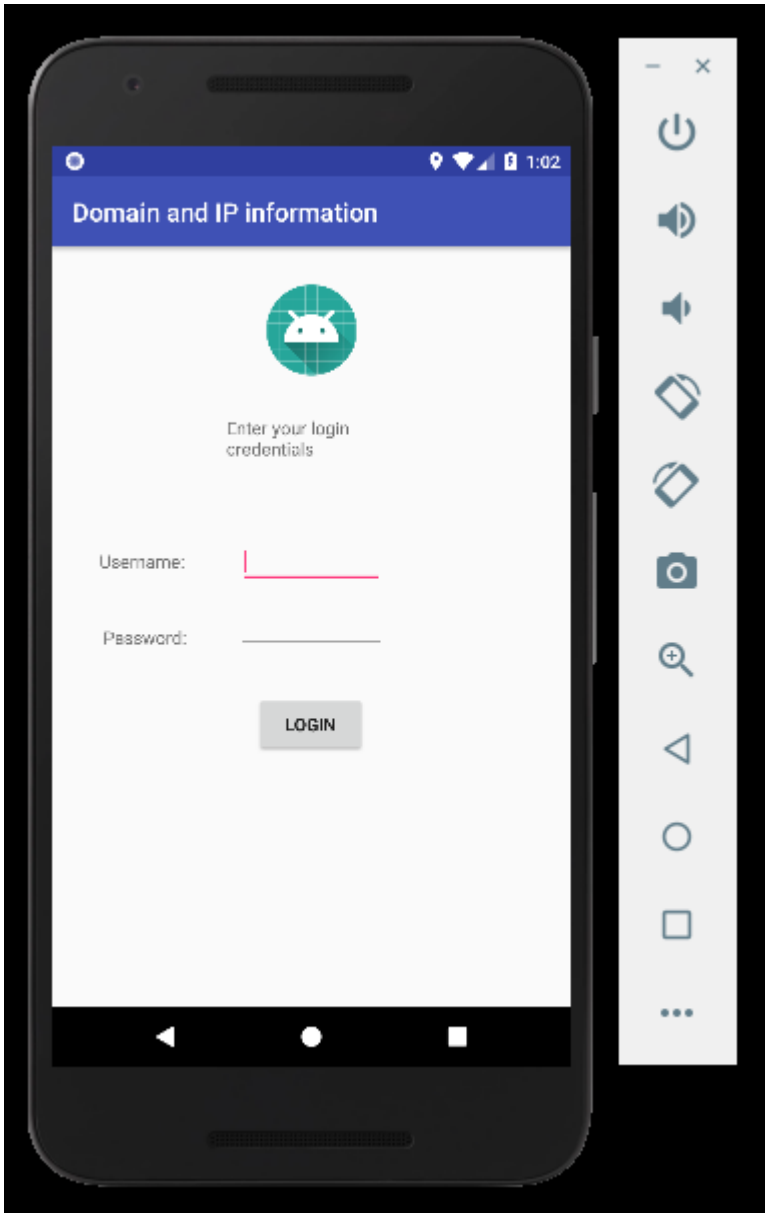


Εικόνα 29: logout

4.3 Λειτουργία Android εφαρμογής

4.3.1 Login χρήστη

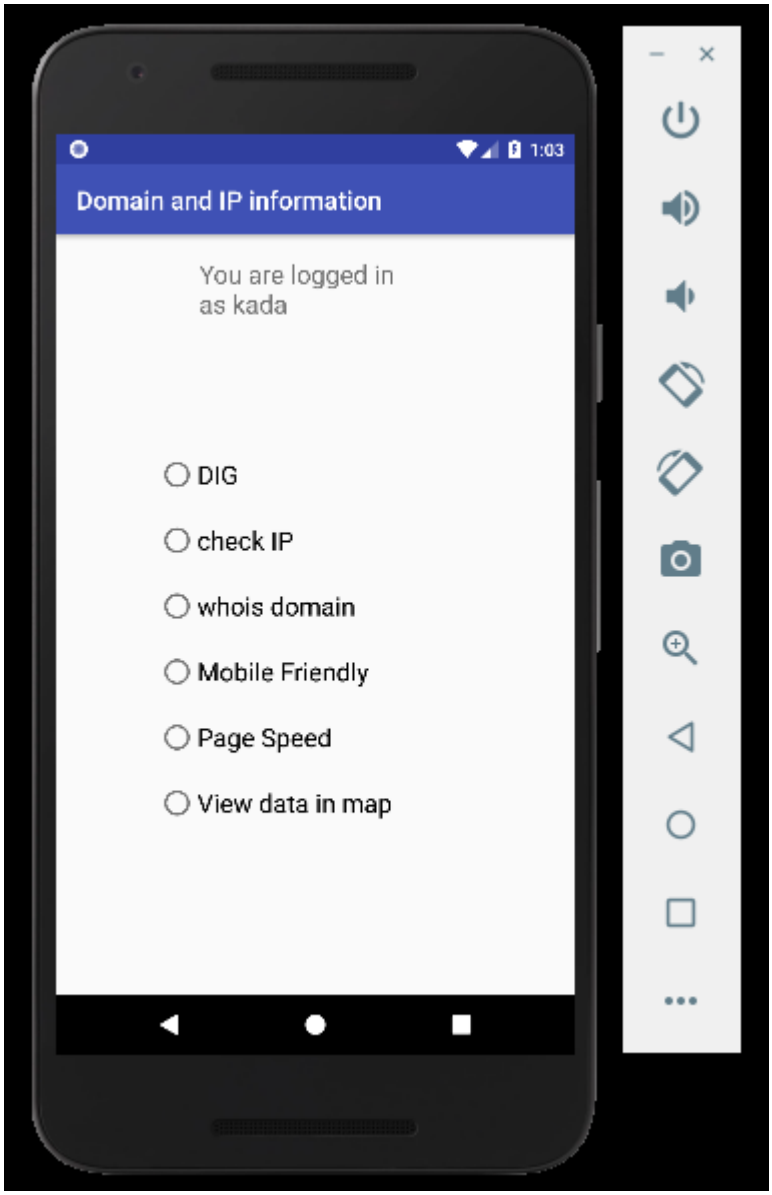
Μόλις ανοίξει η εφαρμογή Android, ζητάει υποχρεωτικά τα στοιχεία εισόδου του χρήστη. Το login πραγματοποιείται μέσω του API στο οποίο υπάρχει η βάση δεδομένων και βρίσκονται όλα τα στοιχεία εισόδου των χρηστών. Η σύνδεση της εφαρμογής με το API, γίνεται με κρυπτογραφημένη σύνδεση και η αποστολή στοιχείων εισόδου (username και password) με τη χρήση post request



Εικόνα 30: android login

4.3.2 Εμφάνιση Menu

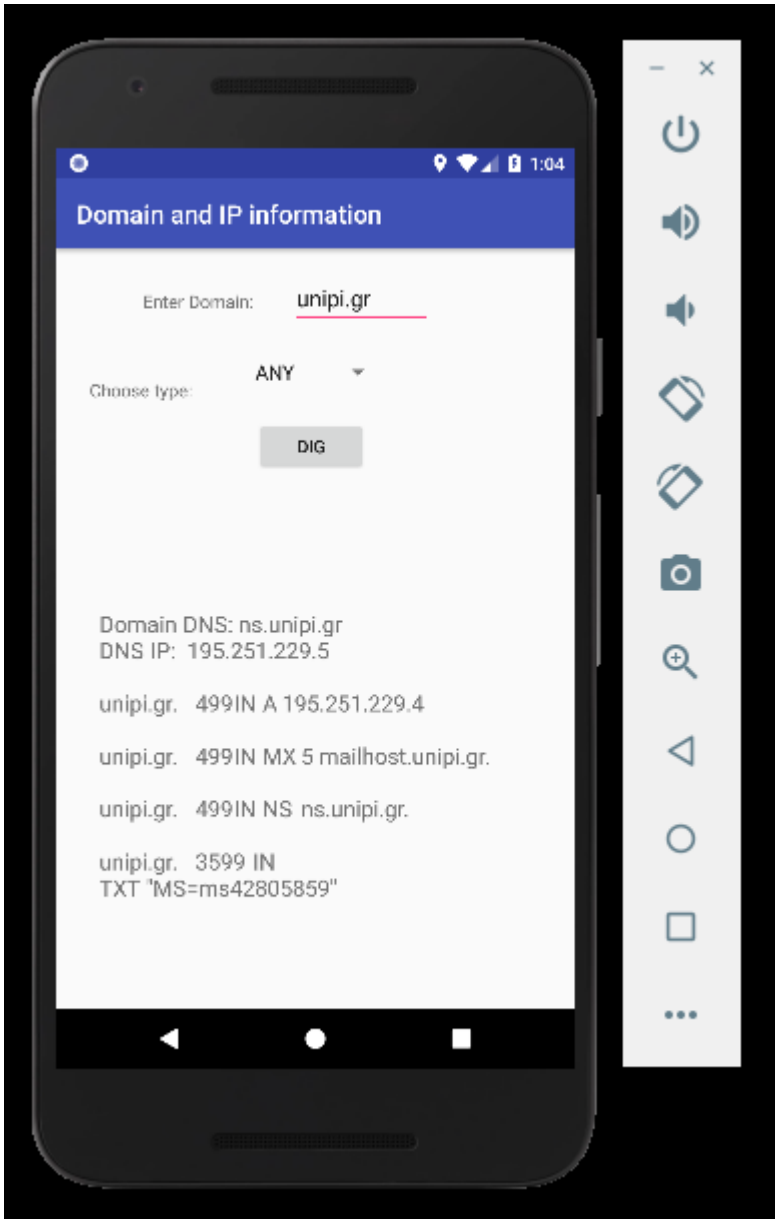
Αφού συνδεθεί ο χρήστης επιτυχώς, εμφανίζεται το μενού μπροστά του από το οποίο μπορεί να περιηγηθεί στις διαθέσιμες επιλογές και λειτουργίες της εφαρμογής.



Εικόνα 31: android menu

4.3.3 DIG

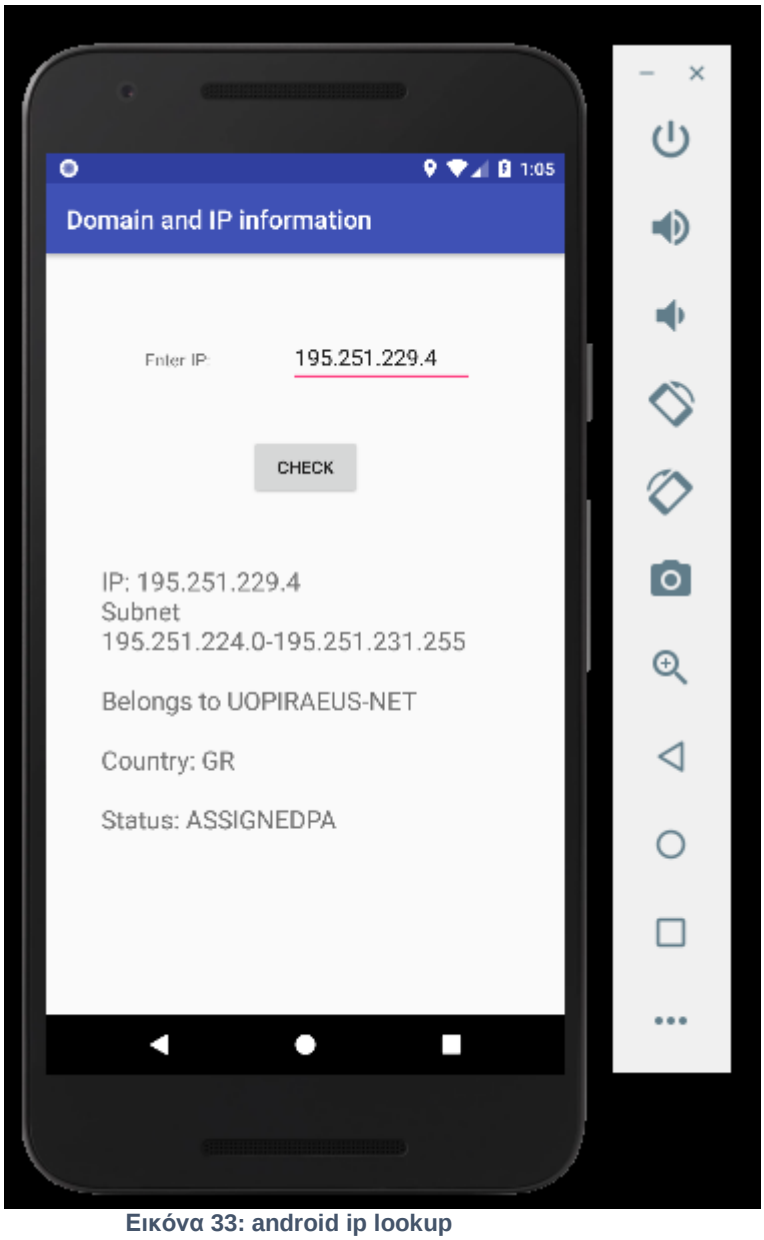
Όπως και στην web εφαρμογή, έτσι και στο Android app, εμφανίζεται στον χρήστη η σχετική επιλογή γραφής του επιθυμητού domain προς έλεγχο και μπορεί να επιλέξει τον τύπο του dig που θέλει να υλοποιηθεί από το API. Η απάντηση εμφανίζεται μέσα σε ελάχιστα δευτερόλεπτα, ακριβώς από κάτω.



Εικόνα 32: android dig

4.3.4 IP Lookup

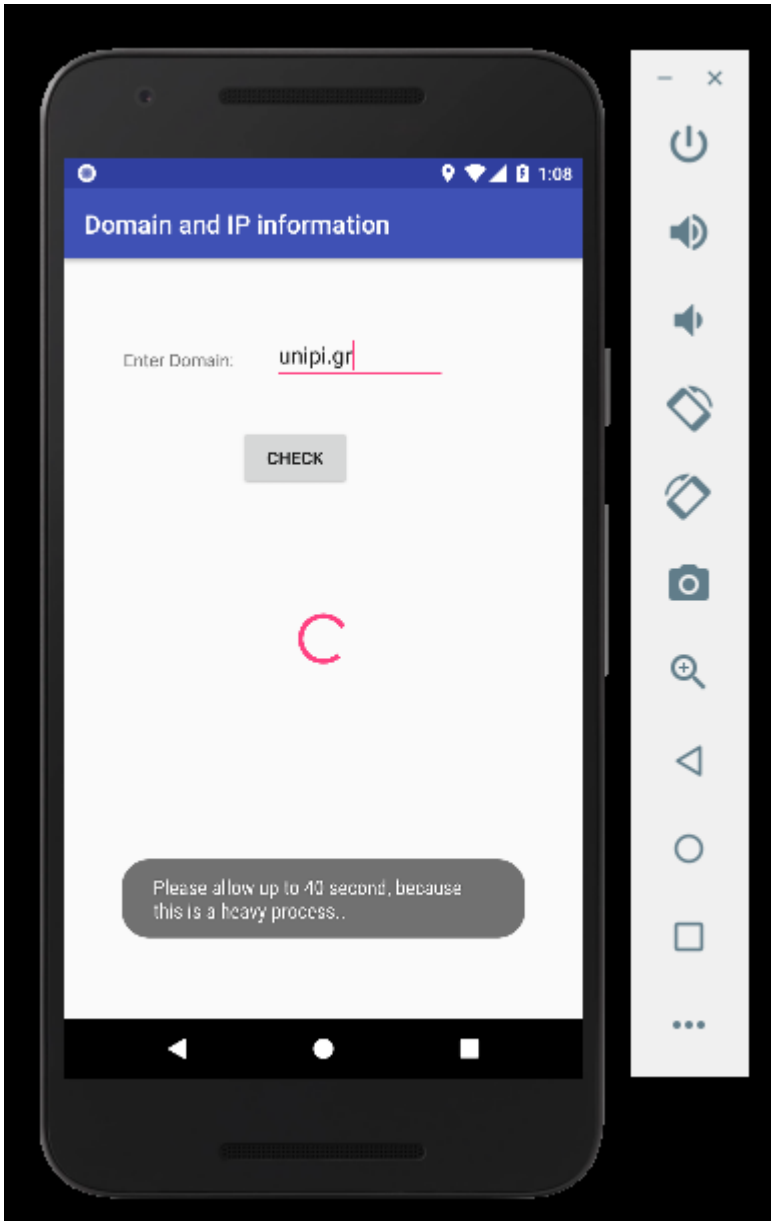
Στο IP lookup, ο χρήστης μπορεί να εισάγει την IP που επιθυμεί να μάθει πληροφορίες και αυτές εμφανίζονται αφού πρώτα ολοκληρωθεί η επικοινωνία με το API και ληφθούν όλες οι απαραίτητες πληροφορίες από αυτό.



Εικόνα 33: android ip lookup

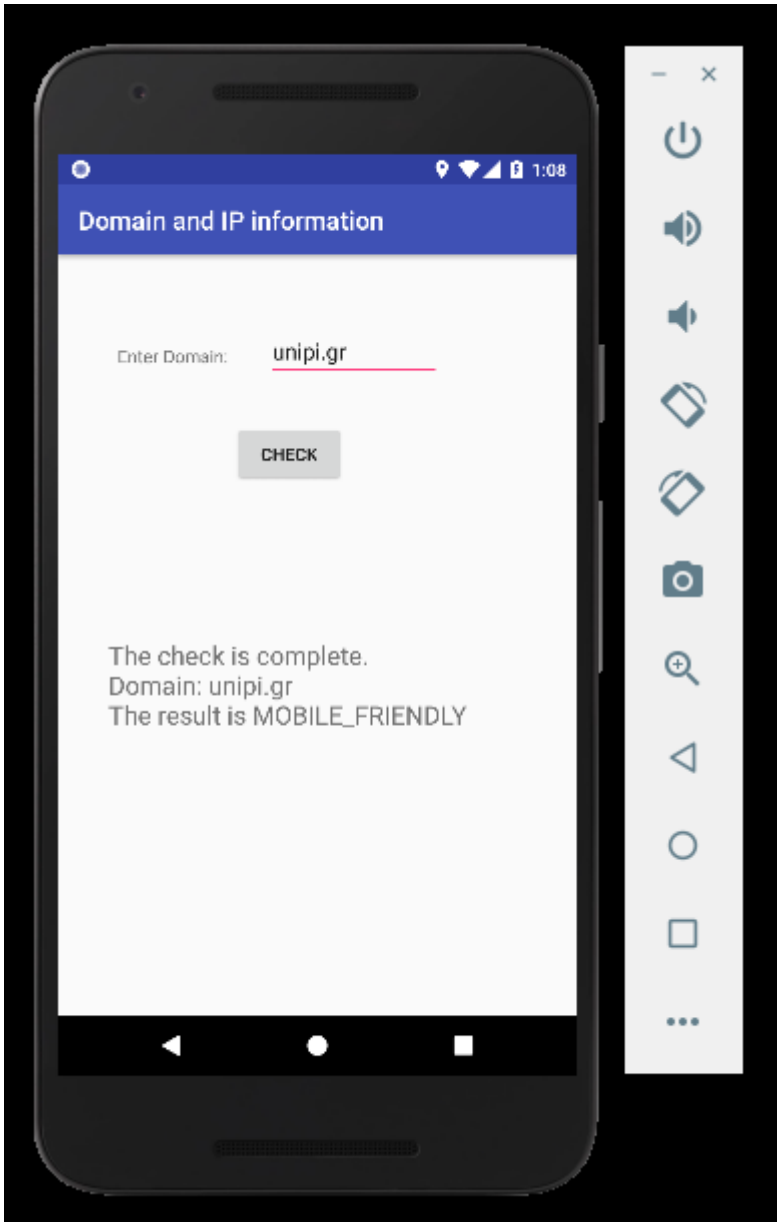
4.3.5 Google Mobile Friendly

Από το API της Google, μπορούμε να λάβουμε πληροφορίες σχετικά με το εάν η ιστοσελίδα που θέλουμε να ελέγξουμε, είναι responsive, είναι δηλαδή mobile friendly. Καθώς ο συγκεκριμένος έλεγχος είναι αρκετά απαιτητικός, η εφαρμογή εμφανίζει σχετικό μήνυμα προς τον χρήστη, ενημερώνοντας τον ότι η διαδικασία μπορεί να διαρκέσει ακόμη και 40 δευτερόλεπτα.



Εικόνα 34: android loading mobile friendly

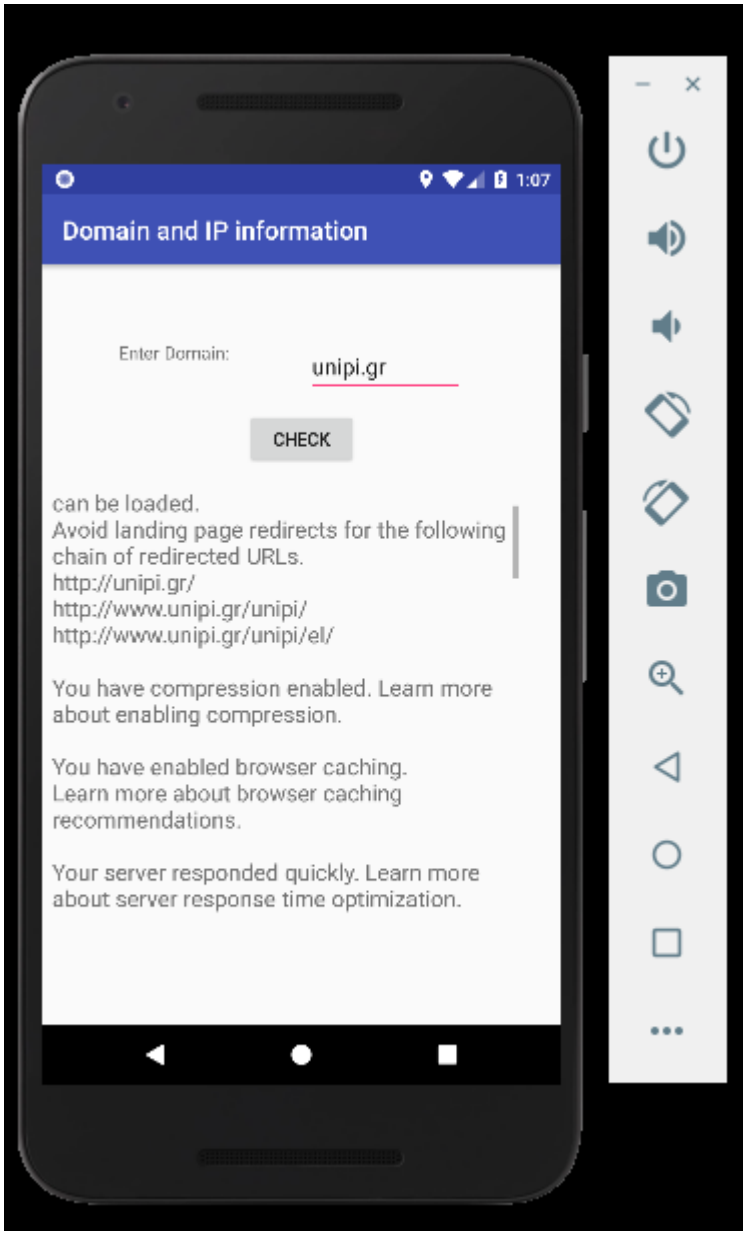
Μόλις ολοκληρωθεί ο έλεγχος και ληφθούν οι πληροφορίες, γίνονται άμεσα διαθέσιμες στον χρήστη.



Εικόνα 35: android results mobile friendly

4.3.6 Google Page Speed

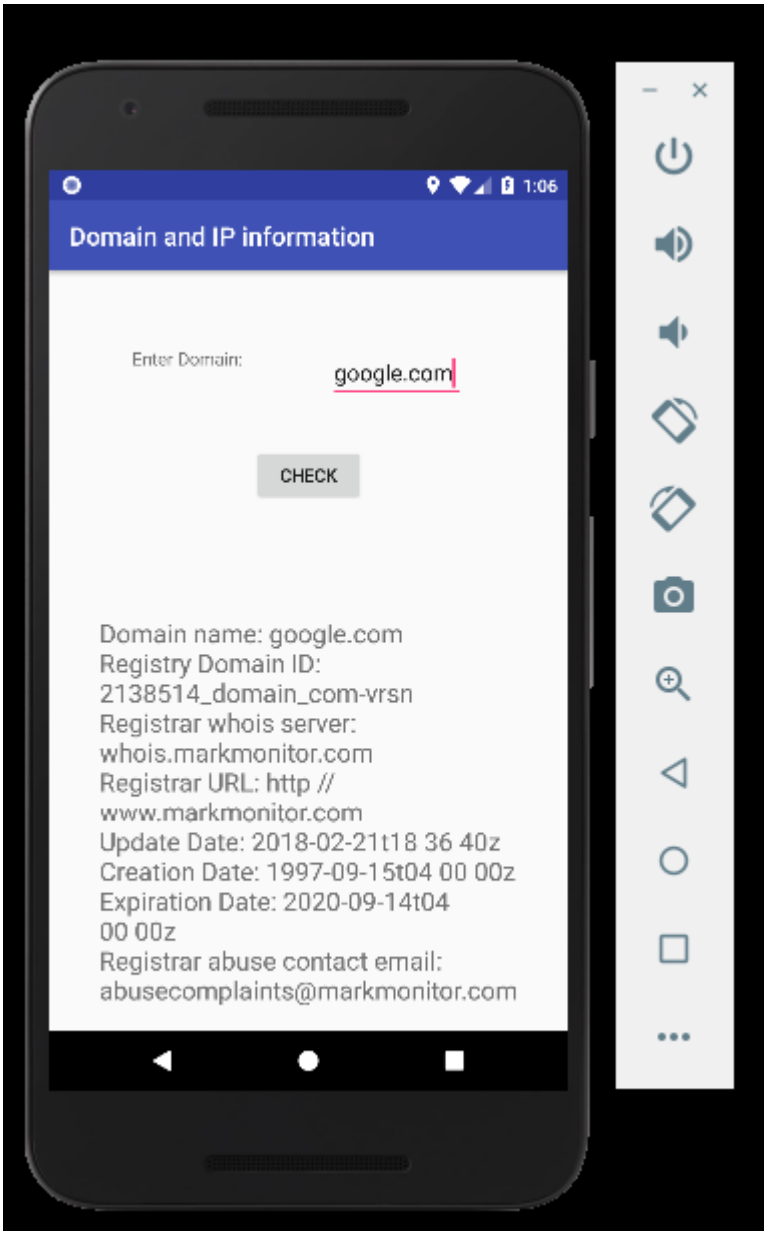
Επιπλέον ένα API της Google που εμφανίζεται και στην web εφαρμογή, εισάγοντας το domain και έπειτα από αναμονή μερικών δευτερολέπτων, εμφανίζεται το κείμενο με τα recommendations και οι σχετικές πληροφορίες. Τα urls έχουν αποκοπεί και εμφανίζεται μόνο το κείμενο που αποστέλλει η Google για λόγους ευκολίας στην ανάγνωση του κειμένου και για αποφυγή μη επιθυμητών clicks σε αυτά.



Εικόνα 36: android page speed

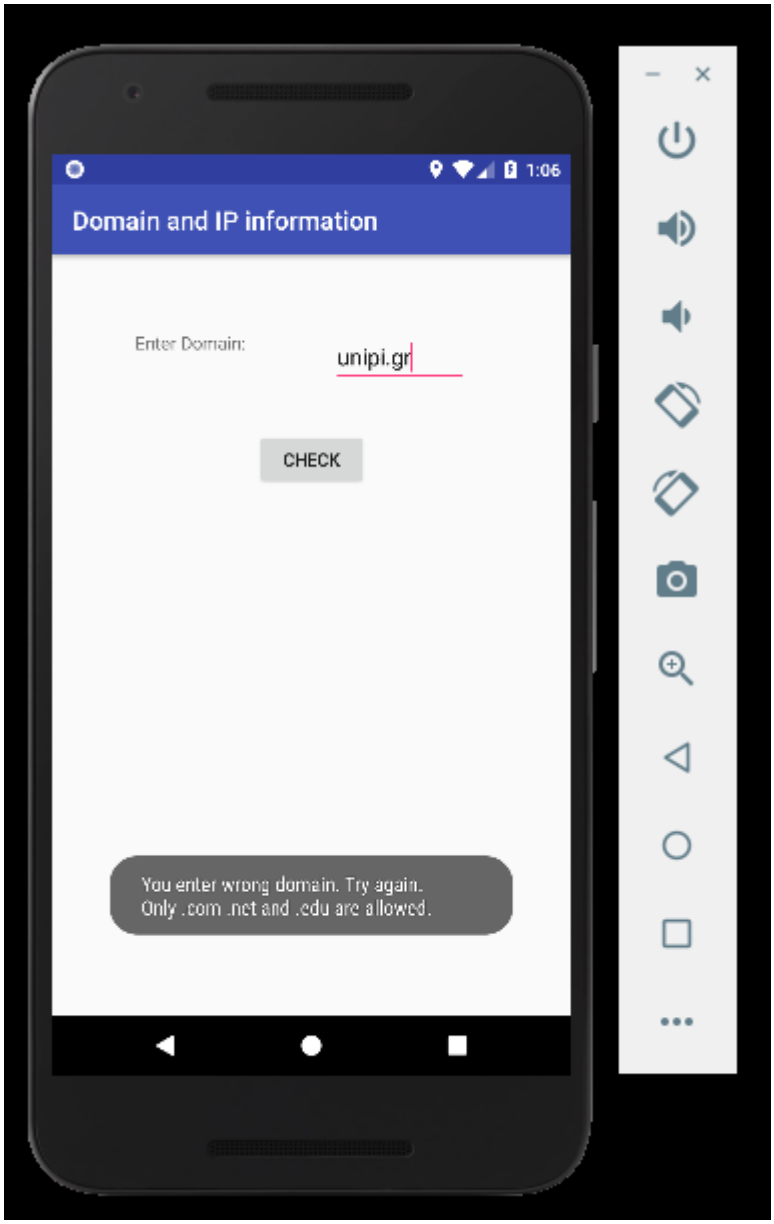
4.3.7 Whois (com και gr)

Για domains που έχουν κατάληξη .com, .net και .edu, υπάρχει διαθέσιμο whois το οποίο επιστρέφει τις πληροφορίες, απευθείας από το μητρώο και τις εμφανίζει στον χρήστη.



Εικόνα 37: android whois com domain

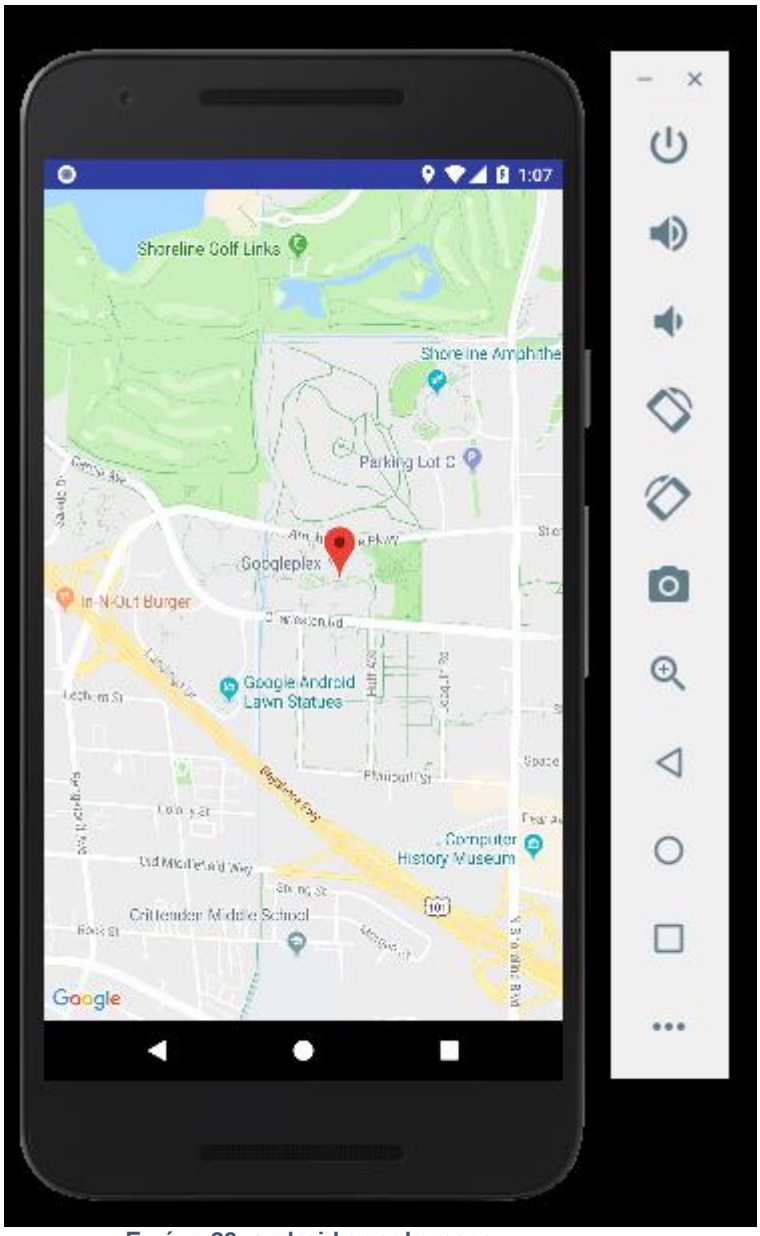
Και στην Android εφαρμογή, δεν υποστηρίζονται διαφορετικής κατάληξης domain, όπως για παράδειγμα τα .gr. Σε τέτοια περίπτωση, εμφανίζεται σχετικό μήνυμα στον χρήστη.



Εικόνα 38: android whois gr domain

4.3.8 Google Maps

Καθώς κάθε ενέργεια που ολοκληρώνει ο χρήστης, καταγράφεται στην απομακρυσμένη βάση δεδομένων, συμπεριλαμβανομένου και της ακριβής τοποθεσίας του, υπάρχει διαθέσιμη επιλογή εμφάνισης των τοποθεσιών του συγκεκριμένου χρήστη. Εάν επιλέξει οποιαδήποτε τοποθεσία του από τον χάρτη, του εμφανίζεται το action που έκανε (παραδείγματος χάριν εάν ήταν login, ip lookup, whois κλπ) και την ημερομηνία και ώρα.
Η παρακάτω εικόνα δείχνει την τοποθεσία στην Αμερική, καθώς γίνεται χρήση (emulator) και όχι πραγματικού GPS, ώστε να λάβει έγκυρες πληροφορίες τοποθεσίας.



Εικόνα 39: android google maps

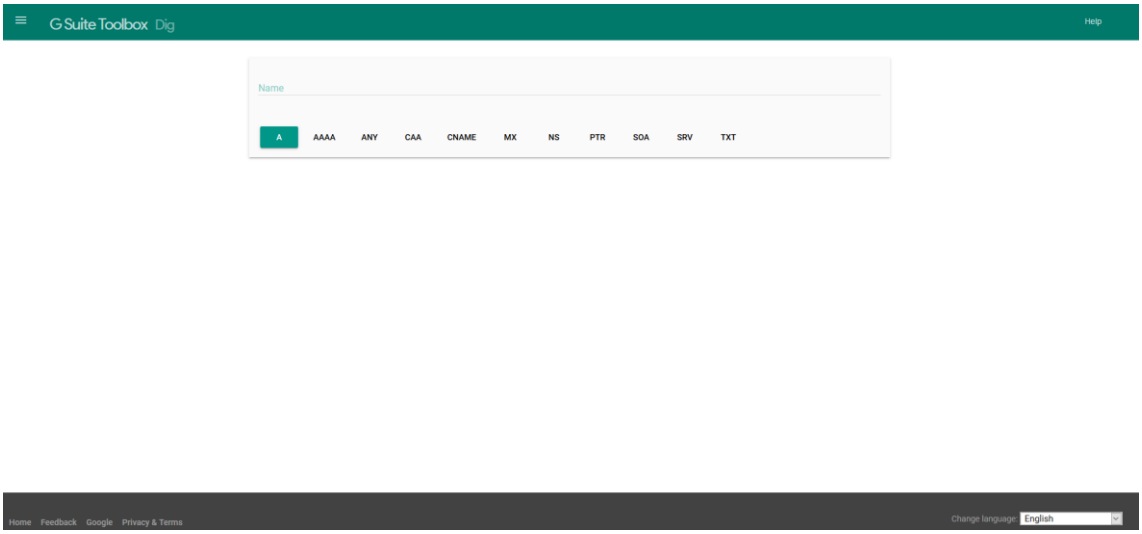
4.4 Σύγκριση εφαρμογής

Στην παρούσα ενότητα γίνεται σύγκριση της εφαρμογής που παρουσιάστηκε στις προηγούμενες ενότητες με παρόμοιες εφαρμογές με την ίδια λειτουργία. Χωρίζεται σε δύο ενότητες, ώστε να καλύψει την web εφαρμογή και το Android application.

4.4.1 web εφαρμογή

4.4.1.1 DIG

Για την λειτουργία του dig, έχουν επιλεγεί 2 από τις πιο δημοφιλείς πλατφόρμες εύρεσης πληροφοριών για domains.



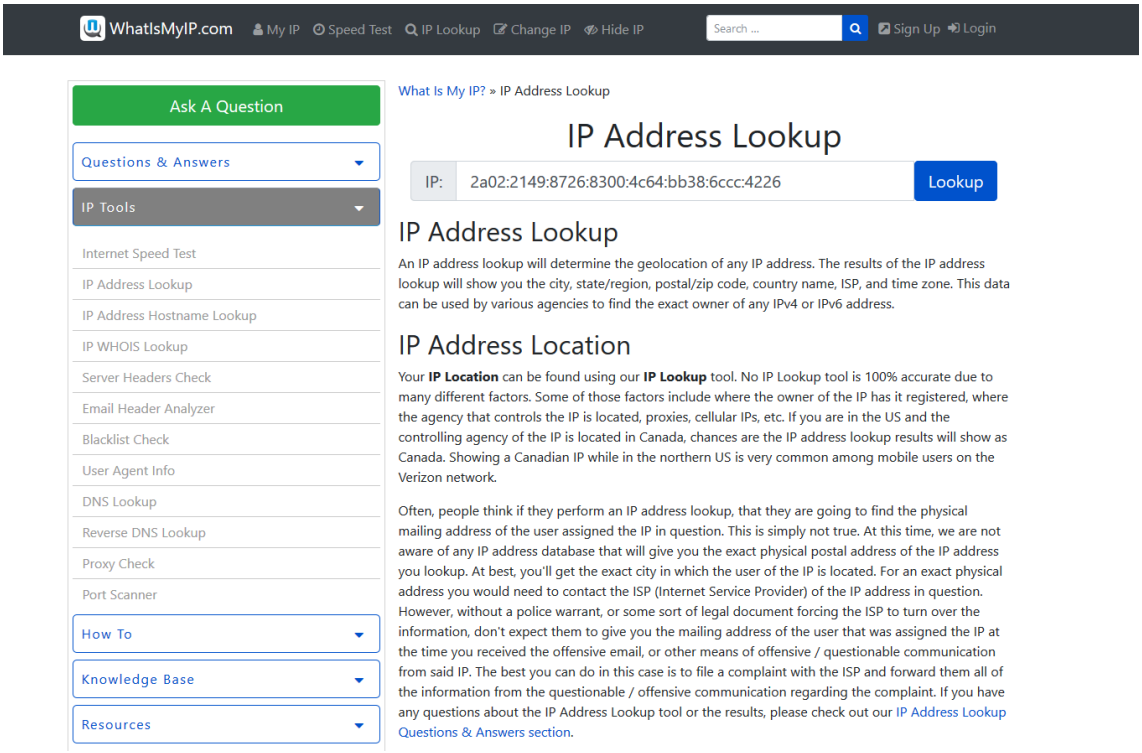
Εικόνα 40: dig google

Η παραπάνω πλατφόρμα, διαθέτει περισσότερες επιλογές για εύρεση συγκεκριμένης πληροφορίας για ένα domain. Το γραφικό περιβάλλον είναι όμορφο και εύχρηστο για τις λειτουργίες που προσφέρει. Η ταχύτητα φόρτωσης των απαραίτητων δεδομένων, είναι πολύ καλή, καθώς λειτουργεί μέσω της Google (από server farms). Ωστόσο, δεν παρέχει λειτουργίες εύρεσης πληροφοριών από DNS της επιλογής του χρήστη και δεν υποστηρίζει πολλαπλά domains και DNS. Η εμφάνιση των δεδομένων είναι raw output, δηλαδή εμφανίζει τα αποτελέσματα όπως ακριβώς παραλαμβάνονται, χωρίς επεξεργασία ή διαφοροποίηση στην εμφάνισή τους.
Φυσικά είναι μια ολοκληρωμένη λύση και ακριβής στα αποτελέσματα που παράγει και εμφανίζει στον χρήστη.

Εικόνα 41: digwebinterface

Μια επίσης δημοφιλής πλατφόρμα εύρεσης πληροφοριών, είναι το digwebinterface. Το συγκεκριμένο εργαλείο, υποστηρίζει εύρεση πληροφοριών για πολλαπλά domains και DNS και η πληροφορία που εμφανίζει γίνεται μέσω JavaScript. Πρακτικά αυτό σημαίνει ότι ο χρήστης δεν περιμένει έως ότου ολοκληρωθούν όλοι οι έλεγχοι και εμφανιστούν αποτελέσματα, κάτι το οποίο είναι σωστό όταν γίνεται έλεγχος πολλαπλών domain και DNS, κάτι το οποίο απαιτεί αρκετό χρόνο.
Η εμφάνιση δεν έχει τροποποιηθεί καθόλου (δεν έχει χρησιμοποιηθεί κάποιο CSS Framework) και είναι πολύ απλή. Όποιες ενέργειες προσθέτονται ή τροποποιούνται εμφανίζονται με κείμενο στην ίδια σελίδα. Αντίθετα στην εφαρμογή της παρούσας διπλωματικής διατριβής, έχει δοθεί μεγάλη έμφαση στην εμφάνιση τόσο των αποτελεσμάτων προς τον χρήστη και γενικότερα την διεπαφή μεταξύ εφαρμογής και χρήστη, όσο και στην εμφάνιση των προβλημάτων ή καθυστερήσεων ή αδυναμία διεκπεραίωσης κάποιας λειτουργίας. Λειτουργικά είναι σωστή και τα αποτελέσματα που εμφανίζει είναι έγκυρα.

4.4.1.2 IP Lookup



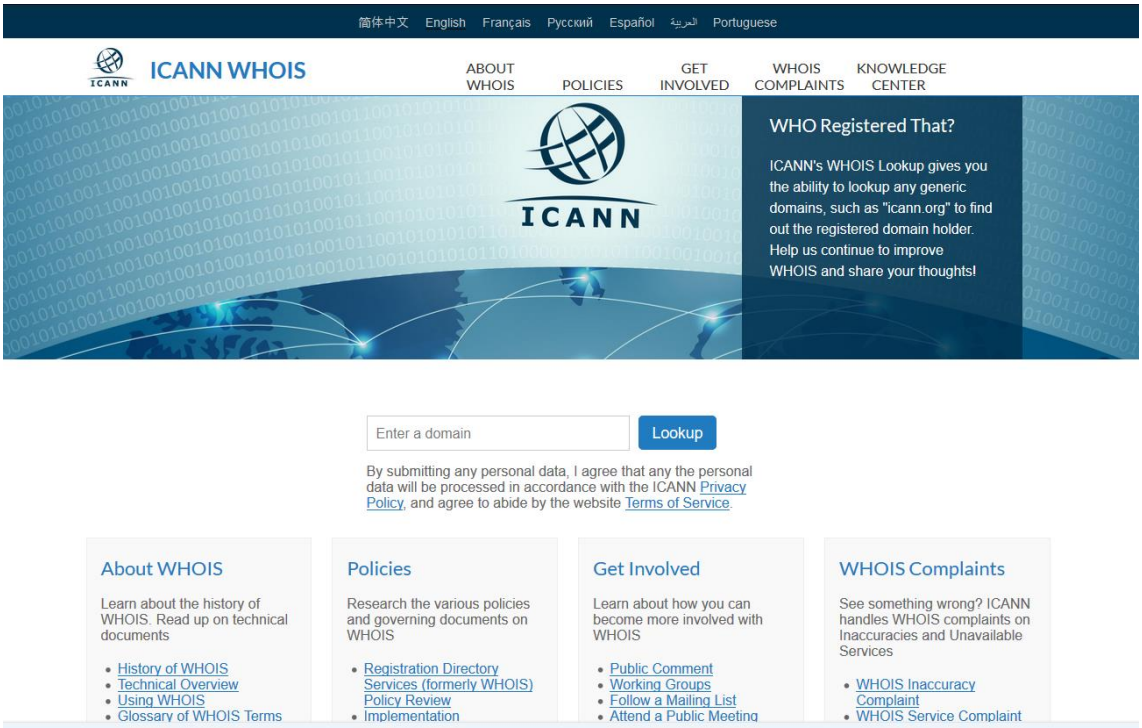
Εικόνα 42: ip address lookup

Το εργαλείο IP Address Lookup, εμφανίζει πληροφορίες σχετικά με την IP μέσω διαφορετικού API από ότι οι εφαρμογές που παρουσιάστηκαν παραπάνω. Εμφανίζει ως αποτελέσματα, την IP, την εταιρία στην οποία έχει αποδοθεί, την πόλη, την περιοχή και την χώρα στην οποία έχει ανήκει η συγκεκριμένη IP, χωρίς να εμφανίζει επιπλέον πληροφορίες.

Εικόνα 43: ip lookup

Μια πιο ολοκληρωμένη λύση, καθώς τα αποτελέσματα που παρέχονται, προέρχονται από την ίδια πηγή που χρησιμοποιείται και στις εφαρμογές της παρούσας μεταπτυχιακής διατριβής. Πιο συγκεκριμένα, επιπλέον από τις πληροφορίες που λαμβάνονται από την RIPE, υπάρχουν πληροφορίες σχετικά με τον γεωεντοπισμό της IP. Ενδεχομένως να είναι λάθος η περιοχή που εμφανίζει, αλλά η πόλη είναι σωστή και η πληροφορία εμφανίζεται στον χάρτη.

4.4.1.3 Whois



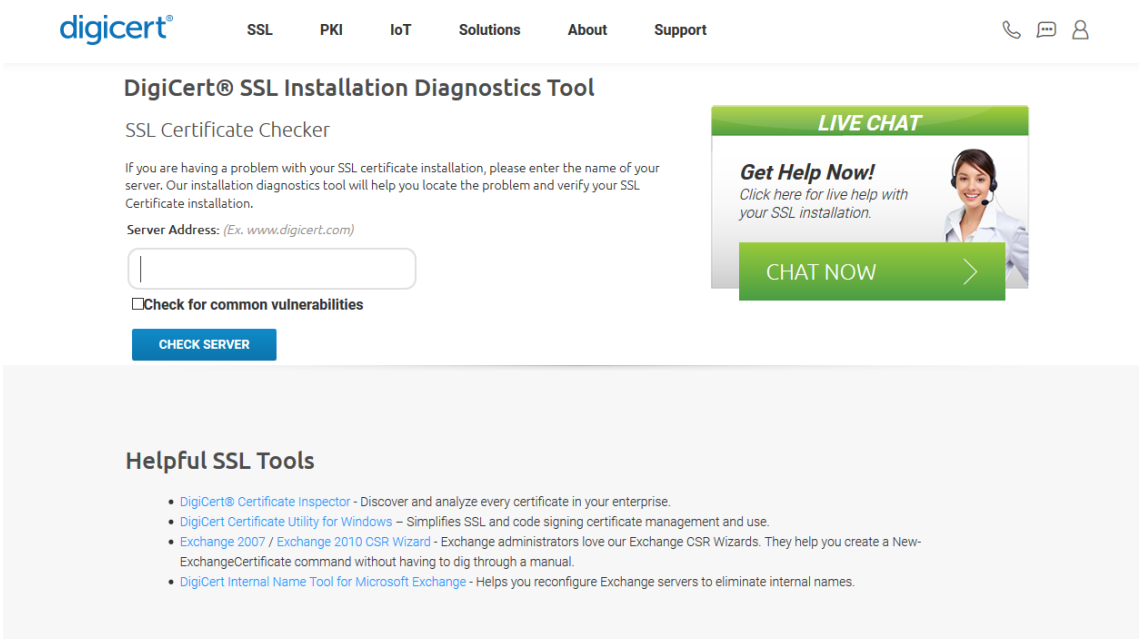
Εικόνα 44: icann whois

Το whois που εμφανίζει η ιστοσελίδα της ICANN, είναι το πιο έγκυρο που μπορεί να υπάρξει, καθώς τα αποτελέσματα προέρχονται κατευθείαν από το μητρώο. Η εμφάνιση και λειτουργία της εφαρμογής, είναι καλή και, φυσικά, τα αποτελέσματα έγκυρα.

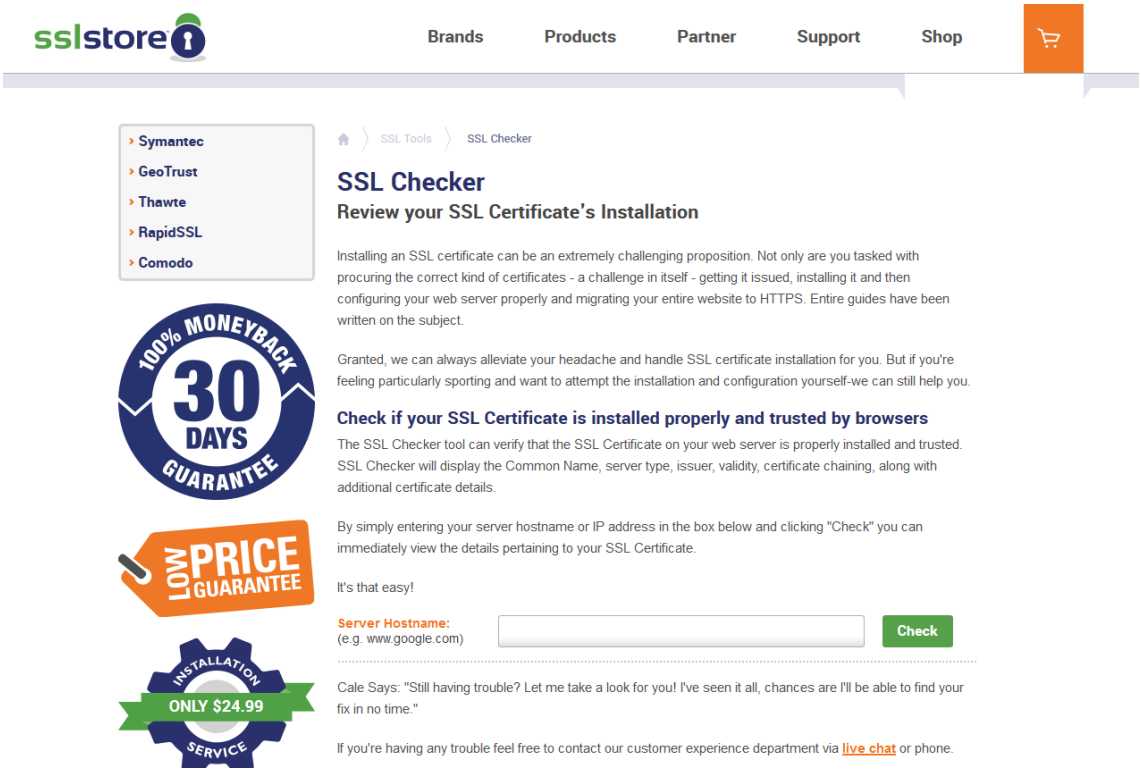
Εικόνα 45: whois

Η ιστοσελίδα που εμφανίζεται παραπάνω, είναι από τις πιο δημοφιλής ιστοσελίδες για χρήση whois. Η πηγή που λαμβάνει τις πληροφορίες, είναι η ίδια που χρησιμοποιήθηκε και στις εφαρμογές που παρουσιάστηκαν παραπάνω.

4.4.1.4 SSL Check



Εικόνα 46: digicert ssl check

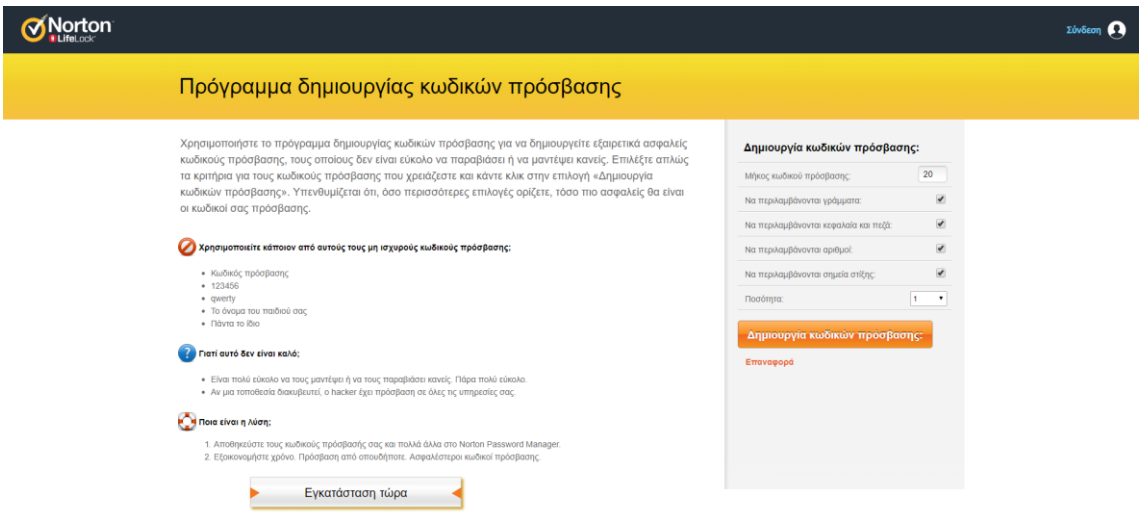


Εικόνα 47: thesslstore ssl checker

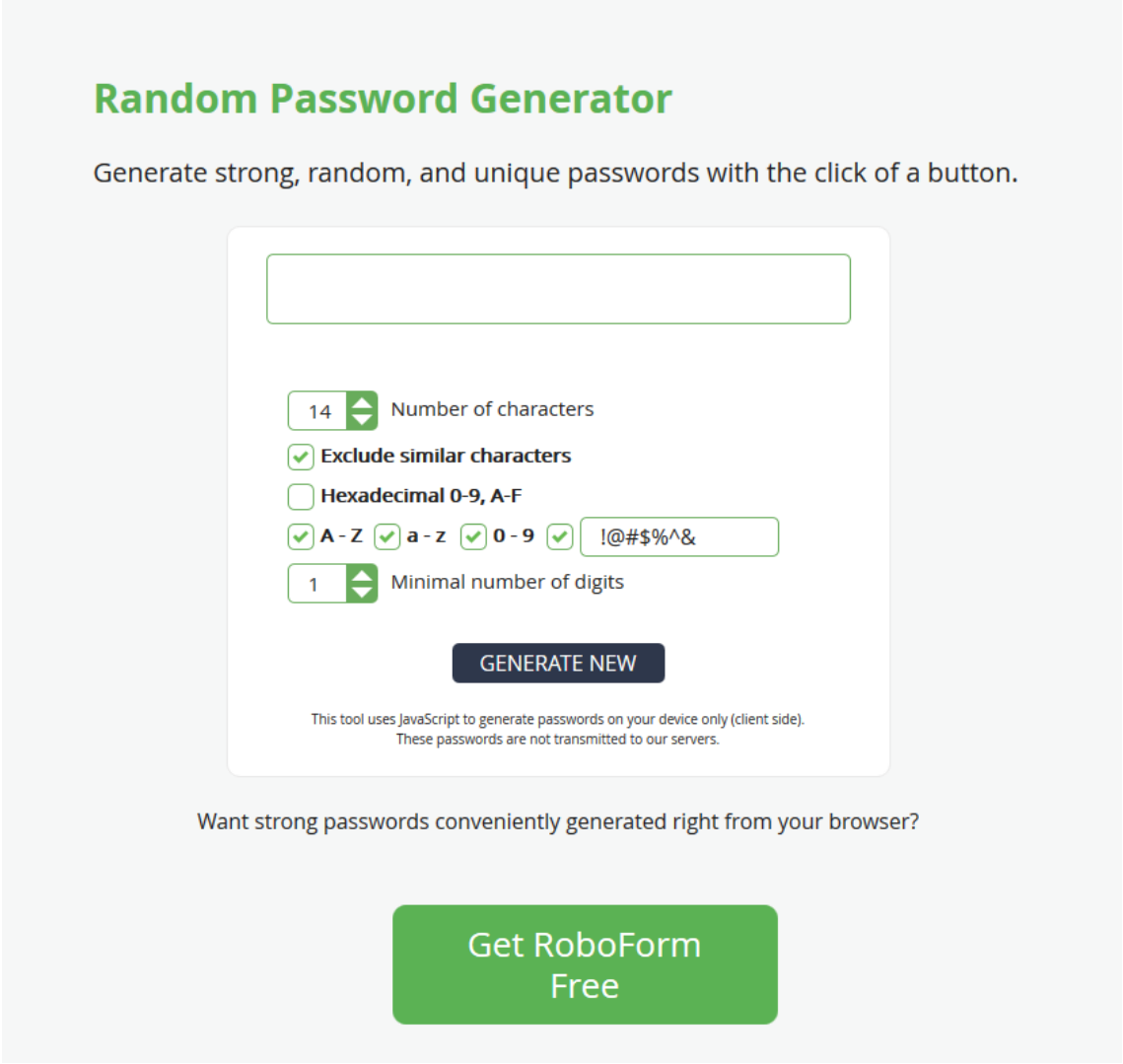
Οι 2 παραπάνω ιστοσελίδες, είναι πάροχοι πιστοποιητικών SSL. Όπως φαίνεται από τις εικόνες, διαθέτουν ένα εργαλείο εύρεσης ενεργού πιστοποιητικού SSL σε κάποιο

domain. Όταν πληκτρολογήσει ο χρήστης το επιθυμητό domain, εμφανίζονται πληροφορίες σχετικά με το πιστοποιητικό (ημερομηνία λήξης, web server κλπ) και εάν η εγκατάσταση έχει ολοκληρωθεί με επιτυχία.

4.4.1.5 Password Generator



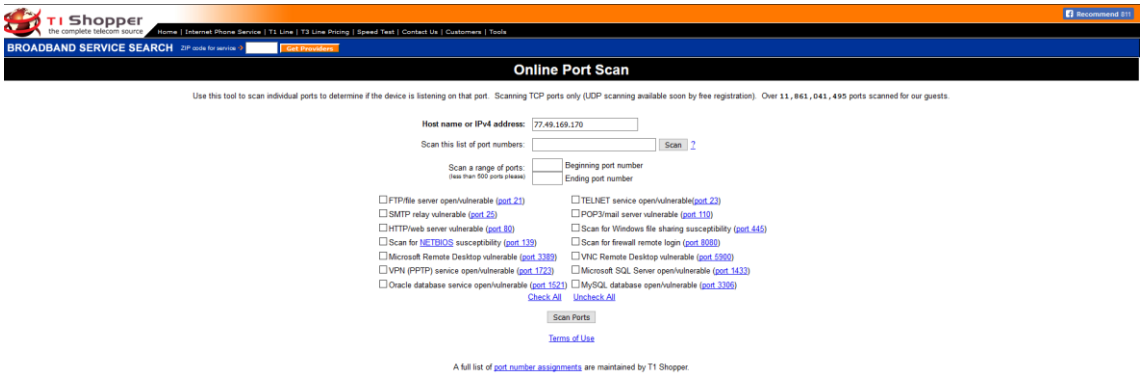
Εικόνα 48: Norton password generator



Εικόνα 49: roboform password generartor

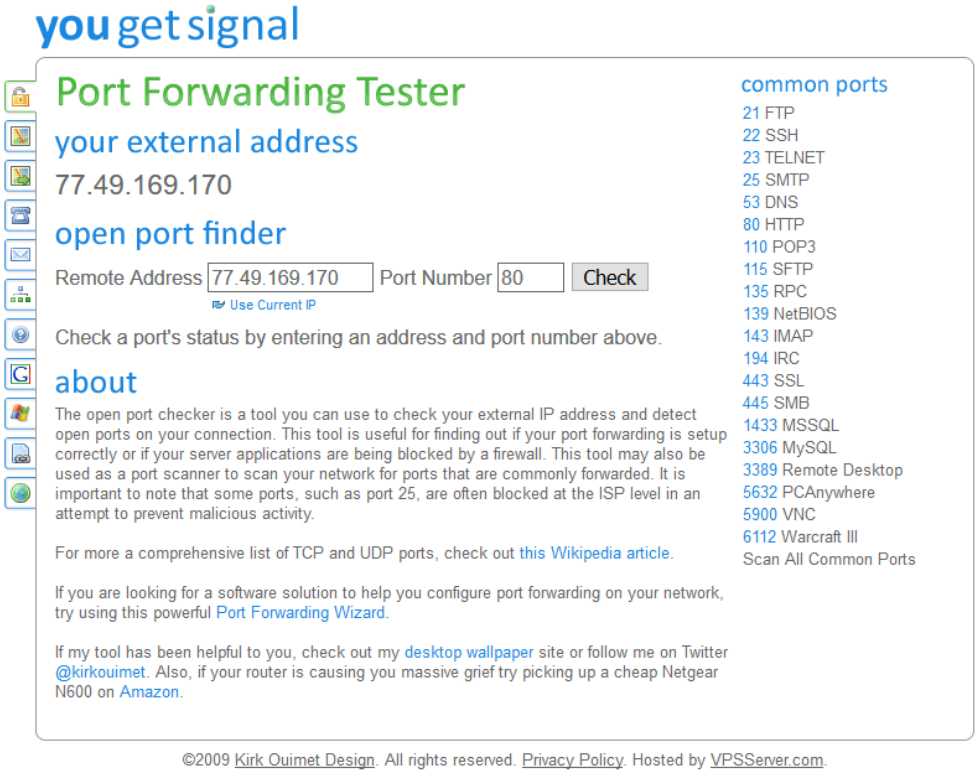
Τα 2 παραπάνω εργαλεία δημιουργίας κωδικών πρόσβασης, έχουν εξειδίκευση στον τομέα της ασφάλειας και της κρυπτογραφίας. Οι κωδικοί πρόσβασης που δημιουργούνται με τα παραπάνω εργαλεία, πραγματοποιείται από τον browser του επισκέπτη, ενώ υπάρχουν επιλογές παραμετροποίησης του παραγόμενου κωδικού πρόσβασης.

4.4.1.6 Port Scan / Check Port



Εικόνα 50: t1shopper port scan

Η εφαρμογή t1shopper είναι αρκετά διαδεδομένη για λειτουργίες port scan. Υποστηρίζει πολλαπλές πόρτες, αλλά όχι πολλαπλές IPs. Υπάρχουν αρκετοί μηχανισμοί ασφαλείας, που αποτρέπουν κακόβουλο port scan, ενώ έχει αρκετές επιλογές παραμετροποίησης του ελέγχου που θα πραγματοποιηθεί.



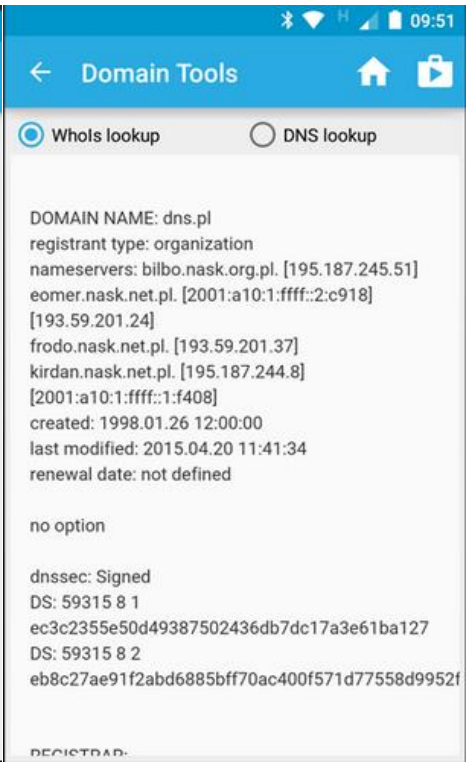
Εικόνα 51: you get signal port scan

Το εργαλείο you get signal, λειτουργεί με πιο απλό τρόπο, επιτρέποντας στον χρήστη να εισάγει μια IP και μία μόνο πόρτα ελέγχου. Ακριβώς από κάτω εμφανίζει το αποτέλεσμα, χωρίς να περιέχει κάποιο ιδιαίτερο γραφικό περιβάλλον, ωστόσο είναι εύχρηστο και έγκυρα τα αποτελέσματα που παρέχει στον χρήστη.

4.4.2 Android εφαρμογή

4.4.2.1 Whois, DNS lookup Domain Tools

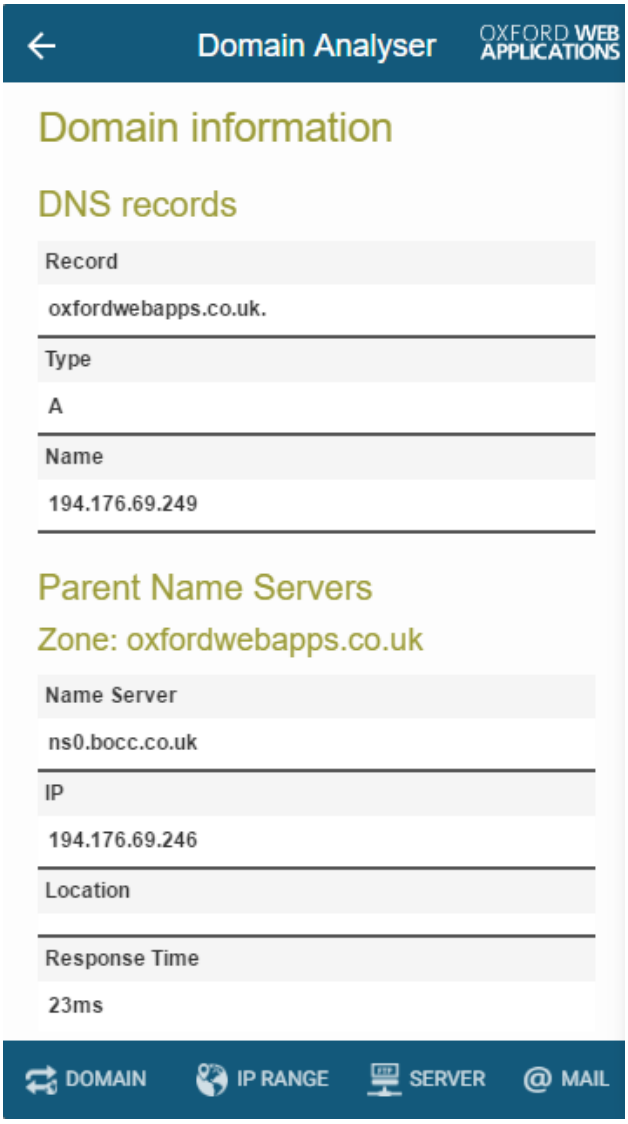
Εικόνα 52: dns lookup



Εικόνα 53: whois lookup

Η εφαρμογή, παρέχει εύρεση πληροφοριών σχετικά με records από τους DNS ενός domain και επιπλέον εμφανίζει πληροφορίες whois, εφόσον είναι διαθέσιμες (εφόσον υποστηρίζονται και μπορούν να εξαχθούν σχετικές πληροφορίες). Τελευταία ενημέρωση είναι στις 16 Μαΐου 2015 και η τρέχουσα έκδοση είναι η 1.1.3 που είναι συμβατή με ΛΣ Android 2.3 και νεότερα.

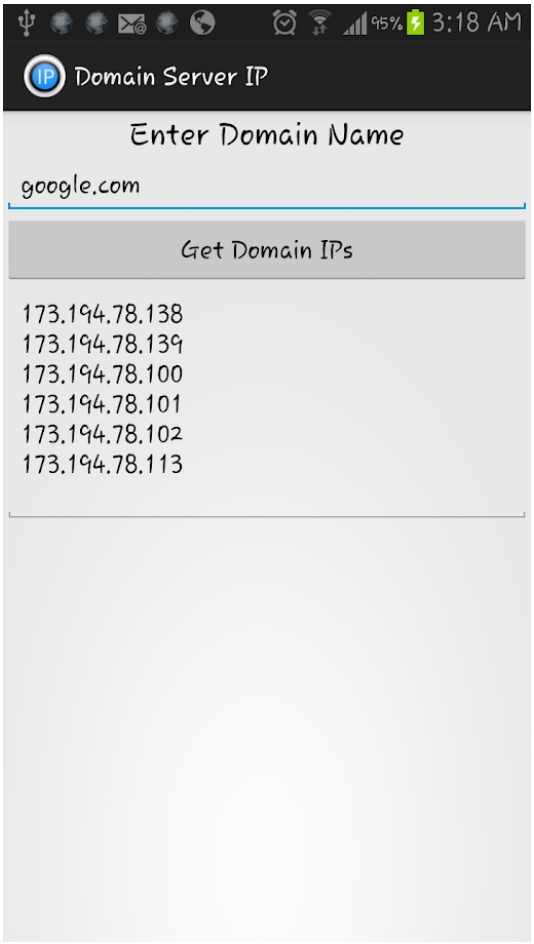
4.4.2.2 Domain Analyzer



Εικόνα 54: domain analyzer

Από το interface της εφαρμογής, παρατηρούμε ότι εμφανίζονται λεπτομερώς όλες οι πληροφορίες σχετικά με ένα domain από τους DNS του. Επιπλέον, μπορούν να εμφανιστούν πληροφορίες σχετικά με το ip range στο οποίο ανήκει η IP του domain, τον web server του και πληροφορίες για τα emails του. Τελευταία ενημέρωση έγινε στις 2 Ιουνίου 2017 και η τρέχουσα έκδοση είναι η 3.1.0 που είναι συμβατή για ΛΣ Android 4.0 και νεότερα.

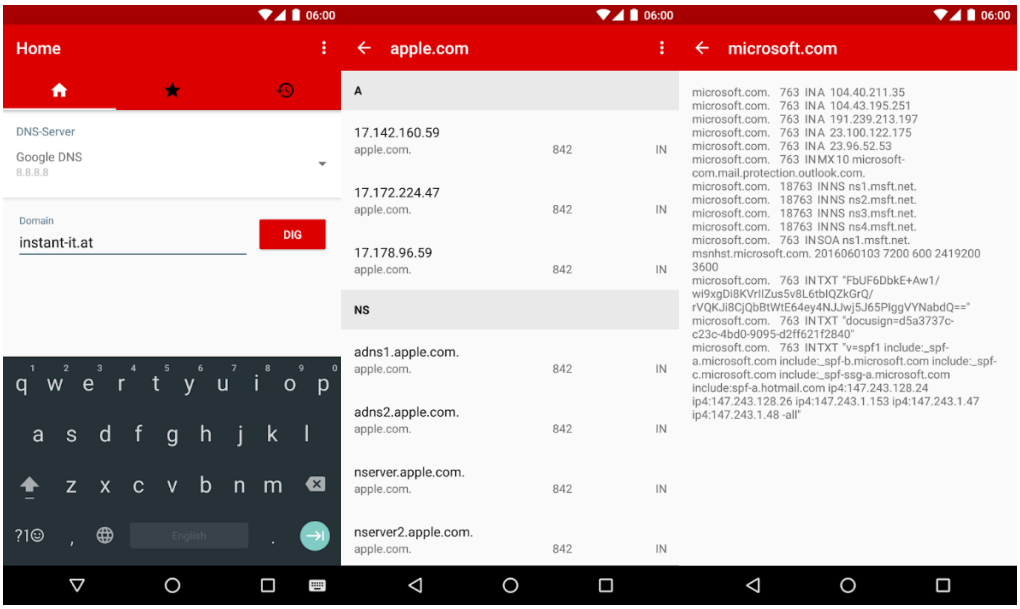
4.4.2.3 Domain Server IP



Εικόνα 55: domain server ip

Το interface της εφαρμογής είναι πολύ απλό και περιέχει μια μοναδική λειτουργία. Ο χρήστης εισάγει το domain για το οποίο επιθυμεί να μάθει πληροφορίες σχετικά με την ή τις IPs από τις οποίες λειτουργεί και αυτές εμφανίζονται ακριβώς από κάτω. Περαιτέρω λειτουργίες δεν υποστηρίζονται. Τελευταία ενημέρωση ολοκληρώθηκε στις 11 Σεπτεμβρίου 2013 και η τρέχουσα έκδοση είναι η 1.4 η οποία είναι συμβατή με ΛΣ Android 2.2 και νεότερα.

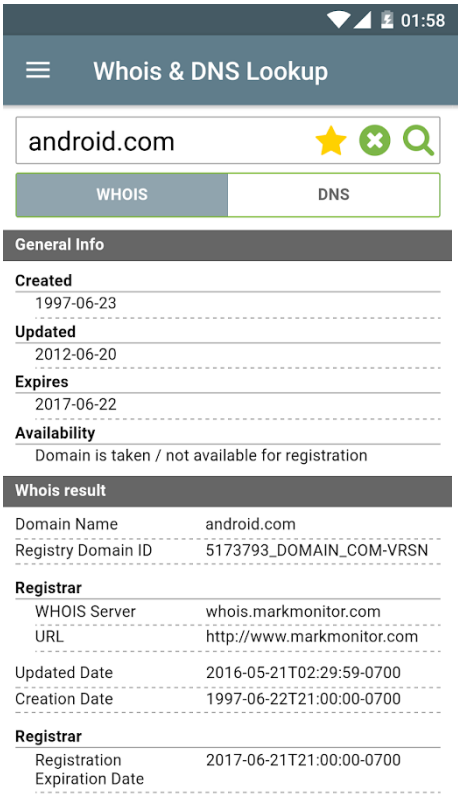
4.4.2.4 MyDIG



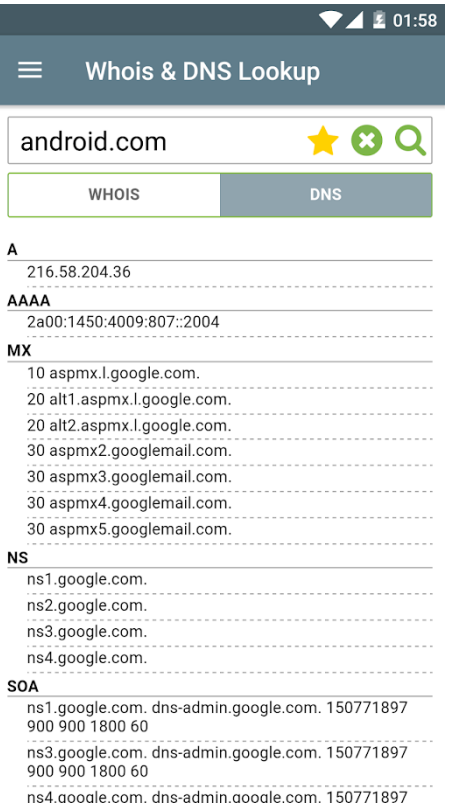
Εικόνα 56: MyDIG start **Εικόνα 57: MyDIG results** **Εικόνα 58: MyDIG text results**

Η εφαρμογή “MyDIG”, ολοκληρώνει έλεγχο για ένα domain για πολλαπλά records, εμφανίζοντάς τα στον χρήστη ταξινομημένα σε κατηγορίες. Μπορεί εάν επιθυμεί, να δει όλες τις πληροφορίες ως απλό κείμενο. Επιπλέον, μπορεί να αποθηκεύσει μια αναζήτηση που ολοκλήρωσε στα “Favorites” ώστε να έχει γρηγορότερη πρόσβαση σε εκ νέου έλεγχο και τέλος μπορεί να δει από το ιστορικό, τις αναζητήσεις που έχει ολοκληρώσει. Η εφαρμογή ολοκλήρωσε τελευταία φορά ενημέρωση την 1η Ιουνίου 2016 και η τρέχουσα έκδοση είναι η 1.0 η οποία είναι συμβατή με ΛΣ Android 4.0.3 και νεότερα.

4.4.2.5 Whois & DNS Lookup - Domain/IP



Εικόνα 59: whois & dns lookup - whois



Εικόνα 60: whois & dns lookup - dns

Τέλος η εφαρμογή που φαίνεται παραπάνω, έχει 2 λειτουργίες. Ο χρήστης εισάγει το domain για το οποίο επιθυμεί να μάθει πληροφορίες και η εφαρμογή εμφανίζει τα στοιχεία από το whois εφόσον αυτά είναι διαθέσιμα. Στο 2ο tab, μπορεί να δει σε μια ταξινομημένη λίστα, τα αποτελέσματα από το dig. Τελευταία ενημέρωση είναι στις 8 Αυγούστου 2018 και η τρέχουσα έκδοση είναι η 1.1.6 που είναι συμβατή με ΛΣ Android 4.4 και νεότερα.

Κεφάλαιο 5

Στο τελευταίο κεφάλαιο γίνεται σύγκριση των αποτελεσμάτων των web και Android εφαρμογών της παρούσας μεταπτυχιακής διατριβής σε σχέση με τις υπόλοιπες εφαρμογές που αναφέρθηκαν στο 2ο κεφάλαιο και παρουσιάστηκαν στο 4ο κεφάλαιο. Επιπλέον αναλύονται τα προβλήματα που παρουσιάστηκαν σε όλα τα στάδια της ανάπτυξης της διατριβής και τέλος μελλοντικές αναβαθμίσεις και προσθήκες τόσο στην web όσο και στην Android εφαρμογή.

5.1 Σύγκριση αποτελεσμάτων

Η web εφαρμογή της παρούσας μεταπτυχιακής διατριβής, έχει αναπτυχθεί πάνω στο CSS Framework Bootstrap. Όλα τα αποτελέσματα που παράγονται, εμφανίζονται σε αντίστοιχα πλαίσια και οι ενημερώσεις του χρήστη, είναι φιλικές προς αυτόν.

5.1.1 web εφαρμογή

- **DIG**

  Η λειτουργία του DIG στην web εφαρμογή, είναι πρακτικά το ίδιο με τις άλλες 2 που παρουσιάστηκαν στο προηγούμενο κεφάλαιο. Τα αποτελέσματα που παράγονται είναι πανομοιότυπα, καθώς ακολουθείται η ίδια ιεραρχική αναζήτηση. Διαφορές παρατηρούνται στον default τρόπο λειτουργείας σε σχέση με τις υπόλοιπες εφαρμογές:

  - **G Suite Toolbox DIG**

    Η Google αναζητά πληροφορίες από τον public DNS με IP 8.8.8.8 (που ανήκει στην Google) για πληροφορίες και όχι τους authoritative DNS που είναι η πιο ορθή διαδικασία και η πιο έγκυρη. Επιπλέον η εμφάνιση των αποτελεσμάτων δεν είναι φιλική προς τον χρήστη, καθώς επιπλέον από την πληροφορία που θέλει να μάθει, εμφανίζονται και άλλα δεδομένα που δεν τον αφορούν. Η παρουσίαση των αποτελεσμάτων, γίνεται σε ένα textarea το οποίο δεν ξεχωρίζει την πληροφορία που εμφανίζεται.
    Δεν υπάρχει επιλογή για δημιουργία ερωτήματος προς ξεχωριστό DNS ή πολλαπλά domains και δεν γίνεται αναζήτηση πληροφοριών από πολλαπλούς public DNS, για σύγκριση αποτελεσμάτων.

  - **DigWebInterface**

    Η λειτουργία του digwebinterface, έχει μεγάλες διαφορές ως προς την σχεδίαση της ιστοσελίδας και την παρουσίαση των αποτελεσμάτων. Υπάρχουν οι ίδιες επιλογές για διαφορετικού τύπου ελέγχους και εισαγωγή πολλαπλών domains και DNS, ωστόσο δεν υπάρχει η ίδια πληθώρα από public DNS. Η ταχύτητα φόρτωσης είναι πολύ καλή και λίγο πιο βέλτιστη όταν ο αριθμός των domains και των DNS, είναι μεγάλος.

- **IP Lookup**
  - **IP Lookup**

    Η λειτουργία του IP Lookup εμφανίζει τις πληροφορίες όπως και στην εφαρμογή της διπλωματικής διατριβής. Λαμβάνονται έγκυρες πληροφορίες και

εμφανίζονται στον χρήστη όλες οι απαραίτητες πληροφορίες, εκτός από λεπτομέρειες του subnet (ip range, ημερομηνία ανάληψης του subnet από τον πάροχο κλπ). Επιπλέον, λαμβάνονται πληροφορίες γεωεντοπισμού της IP και αυτά εμφανίζονται σε ένα χάρτη κάτω από τις πληροφορίες. Στα δεδομένα δεν παρατηρούνται ασυνέπειες και έπειτα από περαιτέρω έλεγχο, φαίνονται να είναι σωστά (εκτός από τα δεδομένα γεωεντοπισμού που δεν μπορούν να επιβεβαιωθούν από κάποια επίσημη πηγή).

- **IP Address Lookup**

  Η εμφάνιση των αποτελεσμάτων της συγκεκριμένης εφαρμογής, είναι 2 πίνακες που λαμβάνουν πληροφορίες μέσω API όπως αναφέρει και κάτω από τους πίνακες) και αναφέρει πληροφορίες σχετικά με τον γεωεντοπισμό της IP και σε ποιόν πάροχο ανήκει. Δεν εμφανίζονται πληροφορίες από την RIPE που είναι και ο αρμόδιος πάροχος για την IP, ώστε να εμφανίσει πληροφορίες σχετικά με το subnet, το IP range του, τον πάροχο, λεπτομέρειες του παρόχου και ποιο είναι το Reverse Record της IP. Η εμφάνιση των πληροφοριών γίνεται μέσω JavaScript κλήσης από τα 2 API και εισαγωγή των πληροφοριών στους πίνακες. Σε διάφορες δοκιμές που πραγματοποιήθηκαν, παρατηρήθηκε ασυνέπεια μεταξύ των αποτελεσμάτων που παρατίθενται στους πίνακες και αφορούν διαφορές στην πόλη, ταχυδρομικό κώδικα και timezone.

- **Password**
  - **Password Generator**

    Ο password generator της Norton, προσφέρει πολλές επιλογές για την παραμετροποίησή του κωδικού πρόσβασης. Λόγω της φύσης της δραστηριότητας της εταιρίας Norton (κυρίως ανάπτυξη Antivirus λογισμικών), υπάρχει αυξημένη ασφάλεια στις υπηρεσίες που προφέρει (συμπεριλαμβανομένου και του συγκεκριμένου μηχανισμού γεννήτριας κωδικών πρόσβασης). Το γραφικό περιβάλλον είναι εύχρηστο και η λειτουργία της εφαρμογής ομαλή. Συγκριτικά με την web εφαρμογή που παρουσιάστηκε παραπάνω, η λειτουργικότητα και ο τρόπος παραγωγής των κωδικών είναι ίδια, ωστόσο διαφέρει το γραφικό περιβάλλον που χρησιμοποιεί ο χρήστης, ενώ η γεννήτρια κωδικών της Norton προσφέρει περισσότερες επιλογές για την παραμετροποίηση του κωδικού (για παράδειγμα επιλογή προσθήκης αριθμών ή γραμμάτων για την δημιουργία)

  - **Random Password Generator**

    Η εφαρμογή που ανέπτυξε η RoboForm, έχει την ίδια λειτουργικότητα με την web εφαρμογή, ωστόσο υποστηρίζεται παραγωγή κωδικών με περισσότερες παραμετροποιήσεις και επιπλέον υπάρχει η ένδειξη σχετικά με το πόσο ισχυρός είναι ο παραγόμενος κωδικός. Η εμφάνιση βασίζεται στο ίδιο CSS Framework, Bootstrap και είναι αρκετά εύχρηστο.

- **Whois**
  - **Whois**

    Η υπηρεσία του whois.com, δέχεται το domain και απαντάει την πληροφορία όμορφα δομημένη και ευδιάκριτη. Οι πληροφορίες που εμφανίζονται είναι σωστές και η δομή της πληροφορίας που λαμβάνεται, είναι πανομοιότυπη με τα δεδομένα που λαμβάνει η Web εφαρμογή. Επιπλέον από την πληροφορία που δομείται για μεγαλύτερη ευκρίνεια, στο κάτω μέρος της σελίδας, φαίνεται και το raw output (είναι τα δεδομένα που έχουν ληφθεί και παρουσιάζονται με ομορφότερο τρόπο).

- ### ICANN WHOIS

  Η ιστοσελίδα για το whois από την ICANN, είναι σίγουρο ότι θα παράξει σωστά αποτελέσματα, καθώς πρόκειται για την πηγή των πληροφοριών για οποιοδήποτε whois. Η εμφάνιση της ιστοσελίδας είναι απλή, εμφανίζοντας την πληροφορία στοιβαγμένη σε πλαίσια και στο τέλος της σελίδας, το raw output το οποίο λαμβάνει όλοι οι whois clients (είτε το whois πραγματοποιείται μέσω API, είτε μέσω command). Το μόνο αρνητικό, είναι η επίλυση ReCaptcha μηχανισμού για λόγους ασφαλείας και αποτροπής αυτοματοποιημένων διαδικασιών, να πραγματοποιούν κατάχρηση της συγκεκριμένης εφαρμογής. Σε περιπτώσεις που πρέπει να ελεγχθούν πολλά διαφορετικά domains, η επίλυση των captcha είναι χρονοβόρα.

Port Scan

- ### you get signal

  Η εφαρμογή για port scan από την you get signal, είναι αρκετά απλή, αλλά λειτουργική. Αφού εισαχθούν η IP και η επιθυμητή πόρτα, ακριβώς από κάτω εμφανίζεται το αποτέλεσμα του ελέγχου. Η εμφάνιση της εφαρμογής, είναι απλή, χωρίς χρήση CSS Frameworks και η πληροφορία εμφανίζεται στον χρήστη ως κείμενο με ένα εικονίδιο (πράσινο για ανοιχτή θύρα και κόκκινο για κλειστή θύρα).

- ### Online Port Scan

  Η T1 Shopper, δημιούργησε ένα εργαλείο που μπορεί να υποστηρίξει port scan για μία IP, αλλά για πολλαπλές πόρτες (έως 500). Επιπλέον, έχει δημιουργημένες συντομεύσεις για έλεγχο συγκεκριμένων θυρών, γνωστών services των servers. Η λειτουργικότητά του είναι πολύ καλή και έχει μεγάλη ακρίβεια στα αποτελέσματα που παράγει. Εμφανισιακά, είναι απλά στημένη η ιστοσελίδα, χωρίς CSS Frameworks και τα αποτελέσματα εμφανίζονται στον χρήστη ως απλό κείμενο σε διαφορετική σελίδα.

SSL Check

- ### DigiCert® SSL Installation Diagnostics Tool
- ### SSL Checker

  Τα διαγνωστικά εργαλεία που αναφέρονται παραπάνω, εμφανίζουν τα αποτελέσματα του ελέγχου που ολοκληρώνουν με τον ίδιο ακριβώς τρόπο (αλλάζει μόνο η εμφάνιση, αλλά όχι η πληροφορία που φαίνεται). Μέσα σε όμορφα πλαίσια εισάγεται η πληροφορία και την εξηγούν με σωστό και ευκρινές τρόπο. Στο τέλος των ελέγχων, εμφανίζεται συγκεντρωτικά εάν, η διαδικασία της εγκατάστασης του πιστοποιητικού SSL, έχει ολοκληρωθεί με επιτυχία και εάν οι browsers λαμβάνουν όποιες πληροφορίες απαιτούν, ώστε να εμφανίσουν την ιστοσελίδα ως secure.

5.1.2 Android εφαρμογή

- **WhoIs, DNS lookup Domain Tools**

  Η λειτουργία της εφαρμογής είναι απλή και εμφανίζει σωστά αποτελέσματα. Με την εισαγωγή του domain, ο χρήστης έχει διαθέσιμη πληροφορία τόσο για το dig (πληροφορίες σχετικά με τα records, εμφανιζόμενα σε μια λίστα με ξεχωριστές ενότητες), και πληροφορίες σχετικά με το whois για το domain (εφόσον υποστηρίζεται). Δεν υπάρχουν περαιτέρω δυνατότητες (για παράδειγμα ip lookup) και δεν μπορεί ο χρήστης να επιλέξει πιο συγκεκριμένα τι επιθυμεί να δει.

- **Domain Analyzer**

  Η εφαρμογή είναι ολοκληρωμένη και εμφανίζει με όμορφο τρόπο τις πληροφορίες τόσο του whois (εάν υποστηρίζεται) όσο και του dig. Υπάρχουν σε διαφορετικές καρτέλες (tabs) με επιπλέον λειτουργίες, που στην Android εφαρμογή της παρούσας μεταπτυχιακής διατριβής, οι αντίστοιχες επιλογές παρέχονται μέσα από το κεντρικό μενού.

- **Domain Server IP**

  Η συγκεκριμένη εφαρμογή, έχει ως μοναδική λειτουργία, την εμφάνιση των IPs από τις οποίες λειτουργεί ένα domain που αναζητά ο χρήστης. Ουσιαστικά είναι ένα dig ενός domain το οποίο ελέγχει μόνο για το A record από τους DNS. Δεν περιέχει καμία άλλη λειτουργία και καμία επιπλέον επιλογή για τον χρήστη.

- **MyDIG**

  Η εφαρμογή MyDIG, ζητάει το domain από τον χρήστη και μπορεί να επιλέξει ποιον DNS θα ρωτήσει για να λάβει τα αποτελέσματα. Στην συνέχεια εμφανίζει ταξινομημένα τα αποτελέσματα ανάλογα με τον τύπο των records. Μπορεί κάποιος χρήστης να εισάγει ένα domain ως αγαπημένο και να δει όλες τις προηγούμενες αναζητήσεις του. Δεν υπάρχουν επιπλέον ενέργειες που μπορεί να κάνει κάποιος χρήστης, ούτε περισσότερες πληροφορίες που μπορεί να δει όπως στην Android εφαρμογή που παρουσιάζεται παραπάνω.

- **Whois & DNS Lookup - Domain/IP**

  Η τελευταία εφαρμογή της παρούσας σύγκρισης, έχει ως λειτουργίες το DIG και το whois. Με την εισαγωγή του domain, εμφανίζονται στον χρήστη, πρώτα οι πληροφορίες του whois (εφόσον είναι διαθέσιμες) και σε διαφορετικό tab οι πληροφορίες των records, ταξινομημένες ανά τύπο record. Δεν υπάρχουν επιπλέον ενέργειες όπως ip lookup ή επιλογή DIG για συγκεκριμένο τύπο records.

5.2 Προβλήματα που προέκυψαν κατά την υλοποίηση των συστημάτων και προβλήματα σε επίπεδο σχεδίασης και κώδικα

Παρουσιάζονται αναλυτικά τα πρόβλημα που προέκυψαν κατά την υλοποίηση της παρούσας μεταπτυχιακής διατριβής, τόσο σε επίπεδο κώδικα, όσο και σε επίπεδο αρχιτεκτονικής συστημάτων.

5.2.1 Προβλήματα κατά την αρχιτεκτονική των συστημάτων

Ο πρώτος προβληματισμός εμφανίστηκε κατά το στήσιμο των servers ως προς την επιλογή του hardware, τον αριθμό των servers και την επικοινωνία που θα έχουν μεταξύ τους. Επιλέχθηκαν σχετικά μικροί servers με hardware, 30GB δίσκο, 2GB RAM και 2 CPUs. Οι servers επιλέχθηκαν να είναι όλοι Virtual Machines και όχι ένας φυσικός server, για το μεγαλύτερο uptime που παρέχεται, την καλύτερη διαχείριση των πόρων (αύξηση – μείωση) και την ευκολία λήψης backup ολόκληρου του server πριν ολοκληρωθούν εγκαταστάσεις που μπορεί να προκαλέσουν πρόβλημα στο setup του μηχανήματος. Αφού οι servers είχαν στηθεί με επιτυχία και το υλικό τους ήταν αρκετό για την φυσιολογική και σωστή λειτουργία τους, τα προβλήματα συνεχίστηκαν ως προς την εγκατάσταση του web server και επιλογής της php.

Η τελική επιλογή του web server και της έκδοσης php που θα φιλοξενούσε την web εφαρμογή, έπρεπε να είναι εύκολα διαχειρίσιμα, γρήγορα σε ταχύτητα και απόδοση, σταθερές οι εκδόσεις τους και κατάλληλες για production servers και ασφαλή.
Έγιναν διάφορες δοκιμές έως ότου καταλήξω στην επιλογή του Nginx ως web server και ως handler το php-fpm ενώ ως php, επιλέχθηκε η τελευταία stable έκδοση που ήταν η έκδοση 7.2. Υπήρξαν προβλήματα ασυμβατότητας ανάμεσα στις διαφορετικές εκδόσεις του nginx και του php-fpm με αποτέλεσμα να μην λειτουργεί σωστά ή να μην λειτουργεί καθόλου. Αυτά τα προβλήματα επιλύθηκαν εφαρμόζοντας δοκιμαστικά αλλαγές στα αντίστοιχα configurations. Τελικώς το πρόβλημα της ασυμβατότητας επιλύθηκε, εισάγοντας τον handler php-fpm ως socket στον nginx, το οποίο επίλυσε πλήρως το πρόβλημα της ταχύτητας και της μη λειτουργικότητας.

Ο server που φιλοξενεί το API, το οποίο επικοινωνεί με το Android, δημιουργήθηκε με μεγαλύτερη ευκολία και σε λιγότερο χρονικό διάστημα, καθώς εγκαταστάθηκε cPanel®, το οποίο είχε ήδη εγκατεστημένες τις εκδόσεις php και τον web server. Τα μόνα προβλήματα που προέκυψαν ήταν επιπλέον modules της php που χρησιμοποιήθηκαν και τελικώς εγκαταστάθηκαν.

Εφόσον πλέον οι servers είχαν στηθεί και λειτουργούσαν σωστά, έπρεπε να ξεκινήσει η ανάπτυξη τόσο της web εφαρμογής, όσο και του API. Το μοναδικό πρόβλημα που προέκυψε και στους 2 servers, ήταν ότι ο χρήστης ο οποίος “έτρεχε” την php, δεν είχε επαρκή δικαιώματα να τρέχει shell commands που χρησιμοποιήθηκαν. Έγιναν οι απαραίτητες ενέργειες στους servers και πλέον δόθηκε το δικαίωμα εκτέλεσης εντολών στους χρήστες και επιπλέον, ορίστηκαν οι εντολές που μπορούν να τρέχουν. Στον server που φιλοξενεί το API, υπήρχε σχετική επιλογή μέσα από το cPanel® ενώ στον server της web εφαρμογής, ήταν απλώς να οριστεί ως χρήστης που τρέχει την php και τα commands, ο user του nginx.
Τελευταίο πρόβλημα που προέκυψε κατά τη διάρκεια δημιουργίας και παραμετροποίησης των servers, ήταν τα λογισμικά ασφαλείας που εγκαταστάθηκαν. Πιο συγκεκριμένα, για την αποφυγή στοχευμένων επιθέσεων κατά του server ή / και των php αρχείων, εγκαταστάθηκαν fail2ban και CSF Firewall. Τα 2 services, αποτρέπουν τις brute force επιθέσεις με πολλαπλά requests που περιλαμβάνουν cross-site scripting, MySQL και code injection και επιπλέον διαβάζοντας τα logs που καταγράφει ο server, αναζητούν μοτίβα επίθεσης σε αρχεία, πολλαπλά λανθασμένα logins και requests που δεν έχουν ως return code, 200 OK (για παράδειγμα code 400 bad request). Έπειτα από 3 requests όπως περιγράφονται παραπάνω, το fail2ban αναλαμβάνει να μπλοκάρει την IP μέσω του Firewall, για την αποφυγή περαιτέρω requests. Τέλος το CSF Firewall χρησιμοποιείται και από την web εφαρμογή, για αποκλεισμό IP που πραγματοποιούν περισσότερα από 400 requests σε λιγότερο από 30 λεπτά (μη φυσιολογική χρήση).

5.2.2 Προβλήματα σε επίπεδο σχεδίασης της web εφαρμογής

Για τα γραφικά της ιστοσελίδας, επιλέχθηκε να χρησιμοποιηθεί το bootstrap και το jQuery. Αρχικά είχε χρησιμοποιηθεί η έκδοση 3.3.0 και στη συνέχεια ολοκληρώθηκε αναβάθμιση στην έκδοση 4.1.0. Κατά την major αναβάθμιση από 3.3 σε 4.1, προέκυψαν προβλήματα καθώς τα ονόματα των κλάσεων, είχαν τροποποιηθεί και τα περισσότερα components της ιστοσελίδας δεν εμφανίζονταν ή εμφανίζονταν λανθασμένα. Έπειτα από δοκιμές και έρευνα στο documentation του bootstrap, τα προβλήματα επιλύθηκαν με την αλλαγή των κλάσεων και την εισαγωγή των σωστών ονομάτων. Γενικά κατά τη σχεδίαση των components της ιστοσελίδας, δεν υπήρξαν προβλήματα που αφορούσαν core δεδομένα του bootstrap ή του jQuery.

5.2.3 Προβλήματα σε επίπεδο κώδικα (web εφαρμογής και API)

Στην αρχή είχαν προκύψει αρκετά προβλήματα με βιβλιοθήκες ή συναρτήσεις που δεν έβρισκε η php. Το πρόβλημα εντοπίστηκε στην έλλειψη των απαραίτητων modules που έπειτα από την εγκατάστασή τους ήταν πλέον διαθέσιμες οι συναρτήσεις που χρησιμοποιούνται στον κώδικα. Κατά την ανάπτυξη της εφαρμογής και του API, υπήρξε πρόβλημα σχετικά με τον αλγόριθμο κρυπτογράφησης που θα χρησιμοποιεί για την αποθήκευση των ευαίσθητων δεδομένων στην βάση δεδομένων. Λόγω της πλήρους αναβαθμισμένης έκδοσης της php (7.2), υπήρχε διαθέσιμο ο αλγόριθμος argon2[20] ο οποίος είναι ο πιο secure συγκριτικά με τους υπόλοιπους διαθέσιμους αλγόριθμους κρυπτογράφησης[21]. Για την χρήση του συγκεκριμένου αλγόριθμου, χρειαζόταν η εγκατάσταση ορισμένων επιπλέον βιβλιοθηκών, που έπειτα από επιτυχή εγκατάσταση, η χρήση του ήταν επιτυχής.
Τέλος, δημιουργήθηκαν ορισμένα εμφανισιακά προβλήματα, όταν έγινε πλήρης μετάβαση της ιστοσελίδας και του API, σε https. Αρχικά τα CSS και JS δεν φόρτωναν ή δεν φόρτωναν ολόκληρα. Το ζήτημα επιλύθηκε με την αλλαγή των url calls των εξωτερικών CSS και JS, και τις ανακατευθύνσεις που πραγματοποιούνται μέσα στην εφαρμογή, από http σε https.

5.2.4 Προβλήματα που προέκυψαν στην Android εφαρμογή

Το μεγαλύτερο πρόβλημα που υπήρξε, ήταν στο parsing των δεδομένων από το API, μέσα στα αντίστοιχα threads του Android, προς επεξεργασία και εμφάνιση των δεδομένων. Σε όλα τα activities υιοθετήθηκε συγκεκριμένη δομή των δεδομένων που λαμβάνονται σε μορφή json και αυτό αποκατέστησε μερικώς το πρόβλημα. Για να αποφευχθεί σπατάλη χρόνου στον έλεγχο όλων των δεδομένων, προστέθηκε ένα λεκτικό μέσα στα δεδομένα json, το οποίο ουσιαστικά είναι status code και δείχνει εάν υπάρχουν αποτελέσματα προς εμφάνιση και αντίστοιχα είτε δεδομένα και την μορφή τους (keys values) είτε τον λόγο του προβλήματος (πχ ανεπαρκή δεδομένα, λάθος στοιχεία κλπ).
Επιμέρους προβλήματα προέκυψαν με την ενσωμάτωση των χαρτών Google Maps, μέσα στην εφαρμογή, ωστόσο επιλύθηκε εισάγοντας το API key σε 2 διαφορετικά σημεία (manifest και gradle), αντί μόνο για το προκαθορισμένο που αναφέρει το σχετικό documentation.

[20] PHP RFC: Argon2 Password Hash. php.net. Weblog.
Available from: https://wiki.php.net/rfc/argon2_password_hash
[Accessed 7th Dec 2018]
[21] Zimuel E. – Protecting passwords with Argon2 in PHP 7.2. zend. Weblog.
Available from: https://framework.zend.com/blog/2017-08-17-php72-argon2-hash-password.html
[Accessed 7th Dec 2018]

5.3 Μελλοντικές αναβαθμίσεις / προσθήκες

Στην παρούσα ενότητα, παρουσιάζονται κάποιες ιδέες για αναβαθμίσεις και επεκτάσεις των εργαλείων που έχουν αναπτυχθεί, τόσο στην web εφαρμογή, όσο και στο Android application. Πολλές από τις προτάσεις που ακολουθούν και προκειμένου να υλοποιηθούν, χρειάζονται ιδιαίτερη προσοχή στον τρόπο υλοποίησης και στους περιορισμούς που θα πρέπει να τεθούν, ώστε να μην πραγματοποιηθεί κακόβουλη χρήση τόσο της ίδιας εφαρμογής, όσο και χρήση της εφαρμογής για επιθέσεις.

5.3.1 web εφαρμογή

Στην web εφαρμογή, υπάρχει πληθώρα αναβαθμίσεων στα ήδη υπάρχουσα εργαλεία, αναφορικά με την ασφάλεια των λειτουργιών σε επίπεδο κώδικα. Χαρακτηριστικό παράδειγμα, είναι η περαιτέρω διασφάλιση των όποιων κενών ασφαλείας υπάρχουν στην εφαρμογή και δεν έχουν ήδη αναλυθεί, βρεθεί και εφαρμοστεί τα απαραίτητα patches. Αυτά θα μπορούσαν να είναι code και MySQL injection μέσω url ή πεδίων εισαγωγής κειμένου, contact forms και εκμετάλλευση εργαλείων, για κακόβουλο σκοπό.
Αναφορικά με τις προσθήκες νέων δυνατοτήτων, ενδεχομένως και εφόσον κριθεί απαραίτητο, να προστεθούν οι αντίστοιχες επιλογές για πολλαπλές αναζητήσεις σε IPs, έλεγχο SPF, DKIM και DMARC records, port scan σε πολλαπλές πόρτες ή / και πολλαπλές IPs. Ενδεχομένως να προστεθεί ακόμη ένας slave server στο εξωτερικό για πιο αντικειμενικό port scan (με μοναδικό task το port scan) που ίσως περιορίζεται λόγω δικτύου ή / και Firewall.
Ορισμένες λειτουργίες θα μπορούσαν να στηθούν διαφορετικά και να πραγματοποιούνται μέσω API. Πιο συγκεκριμένα, θα μπορούσε να υπάρχει ως front end κάποιο JavaScript framework (React ή Angular) και να γίνονται οι έλεγχοι ασύγχρονα. Όποια αποτελέσματα είναι έτοιμα προς προβολή, να εμφανίζονται αμέσως και να μην περιμένει ο χρήστης έως ότου φορτώσει ολόκληρο το php script στον εκάστοτε έλεγχο που έχει ζητήσει.

5.3.2 Android app + API

Στην Android εφαρμογή θα μπορούσαν να προστεθούν επιπλέον ενέργειες όπως port scan, password generator, dig για πολλαπλά domains, επιλογή επικοινωνίας μέσα από την εφαρμογή και διάφορα άλλα, εφόσον κριθούν ότι είναι απαραίτητα ή τουλάχιστον επιθυμητά για τους χρήστες.
Μια φόρμα εγγραφής χρήστη, προκειμένου μέσω αυτοματοποιημένης διαδικασίας να ολοκληρώνεται η εγγραφή και να μην χρειάζεται ο μελλοντικός χρήστης να μεταβεί στην ιστοσελίδα, όπου μέσω της contact form, να πρέπει να κάνει αίτηση για account πρόσβασης στην Android εφαρμογή.
Είναι σπάνιο φαινόμενο να χρησιμοποιεί κάποιος χρήστης μια εφαρμογή για να του παράξει έναν κωδικό προκειμένου να τον χρησιμοποιήσει σε κάποια εγγραφή που επιθυμεί να ολοκληρώσει. Ωστόσο, εφόσον, χρειάζεται μπορεί να υλοποιηθεί native στην εφαρμογή, χωρίς ξεχωριστή επικοινωνία με το API. Επομένως με τον τρόπο αυτό δεν θα υπάρχει ιστορικό στις ενέργειες που ολοκλήρωσε ο χρήστης και δεν θα μπορεί να αποθηκευτεί ο κωδικός με αυτοματοποιημένο τρόπο.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Brain M. , Crawford S. – How Domain Name Servers Work. howstuffworks. Weblog. Available from: https://computer.howstuffworks.com/dns.htm

How the Domain Name System (DNS) Works. Verisign. Weblog. Available from: https://www.verisign.com/en_US/website-presence/online/how-dns-works/index.xhtml

Abrams L.- What is Domain Name Resolution. bleepingcomputer. Weblog. Available from: https://www.bleepingcomputer.com/tutorials/what-is-domain-name-resolution/

ΓΑΒΑΛΑΣ Δ., ΚΑΣΑΠΑΚΗΣ Β., ΧΑΤΖΗΔΗΜΗΤΡΗΣ Θ., 2015. ΚΙΝΗΤΕΣ ΤΕΧΝΟΛΟΓΙΕΣ. εκδ. Νέων Τεχνολογιών. Αθήνα. σελ. 9

Wikipedia - Android. Weblog. Available from: https://el.wikipedia.org/wiki/Android

DEITEL P. DEITEL H.DEITEL A. , 2014. ANDROID ΠΡΟΓΡΑΜΜΑΤΙΣΜΟΣ. Μτφρ. Σαμαράς Γ. εκδ. Γκιούρδας. Αθήνα. σελ. 3

Statcounter - Mobile Operating System Market Share Worldwide. Weblog. Available from: http://gs.statcounter.com/os-market-share/mobile/worldwide

Apache – Apache License. Available from: https://www.apache.org/licenses/LICENSE-2.0

Αλέπης Ευ. – Activity Lifecycle and States. Πανεπιστημιακές Σημειώσεις. Πανεπιστήμιο Πειραιώς 12-07-2017

Felt AP, Chin E, Hanna S, Song D, Wagner D. Android permissions demystified. In: Proceedings of the 18th ACM conference on Computer and communications security - CCS '11 [Internet]. Chicago, Illinois, USA: ACM Press; 2011. p. 627. Available from: http://dl.acm.org/citation.cfm?doid=2046707.2046779

ΓΑΒΑΛΑΣ Δ., ΚΑΣΑΠΑΚΗΣ Β., ΧΑΤΖΗΔΗΜΗΤΡΗΣ Θ., 2015. ΚΙΝΗΤΕΣ ΤΕΧΝΟΛΟΓΙΕΣ. εκδ. Νέων Τεχνολογιών. Αθήνα. σελ. 200-204

What is an Extended Validation (EV SSL) Certificate? [Internet]. Available from: https://www.globalsign.com/en/ssl-information-center/what-is-an-extended-validation-certificate/

The SSL StoreTM is here to help you validate your SSL Certificates quickly & easily. Breeze through the SSL valiation process by following our validation checklist. [Internet]. Knowledge Base. Available from: https://www.thesslstore.com/knowledgebase/ssl-validation/

Réseaux IP Européens Network Coordination Centre. In: Wikipedia [Internet]. 2018. Available from: https://en.wikipedia.org/w/index.php?title=R%C3%A9seaux_IP_Europ%C3%A9ens_Network_Coordination_Centre&oldid=845590576

What is an SPF record? - DNSimple Help [Internet]. [cited 2018 Dec 16]. Available from: https://support.dnsimple.com/articles/spf-record/

What is a DKIM record? - DNSimple Help [Internet]. [cited 2018 Dec 16]. Available from: https://support.dnsimple.com/articles/dkim-record/

What is a DMARC record and how do I create it on DNS server? | SonicWall [Internet].
Available from: https://www.sonicwall.com/en-us/support/knowledge-base/170504796167071

JR – Install Nginx/PHP-FPM on Fedora 29/28, CentOS/RHEL 7.5/6.10. if-not-true-then-false. Weblog.
Available from: https://www.if-not-true-then-false.com/2011/install-nginx-php-fpm-on-fedora-centos-red-hat-rhel/

EPP Status Codes. icann. Weblog.
Available from: https://www.icann.org/resources/pages/epp-status-codes-2014-06-16-en

PHP RFC: Argon2 Password Hash. php.net. Weblog.
Available from: https://wiki.php.net/rfc/argon2_password_hash

Zimuel E. – Protecting passwords with Argon2 in PHP 7.2. zend. Weblog.
Available from: https://framework.zend.com/blog/2017-08-17-php72-argon2-hash-password.html