ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Επισκόπηση των απειλών και προκλήσεων ασφάλειας των Ραδιο-Δικτύων που καθορίζονται από Λογισμικό (Software Defined Radio- SDR). Μελέτη περίπτωσης με βάση το RTL-SDR

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

του

Ντούλα Δημήτριου

(ΑΕΜ: 2737)

Επιβλέπων : Νικολάου Σπυρίδων

Λέκτορας

Καστοριά, Δεκέμβριος 2022

ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Επισκόπηση των απειλών και προκλήσεων ασφάλειας των Ραδιο-Δικτύων που καθορίζονται από Λογισμικό (Software Defined Radio- SDR). Μελέτη περίπτωσης με βάση το RTL-SDR

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

του

Ντούλα Δημήτριου

(ΑΕΜ: 2737)

Επιβλέπων : **Νικολάου Σπυρίδων**

Λέκτορας

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την ημερομηνία εξέτασης

.....	.....	.....
Ον/μο Μέλους	Ον/μο Μέλους	Ον/μο Μέλους
Ιδιότητα Μέλους	Ιδιότητα Μέλους	Ιδιότητα Μέλους

Καστοριά, Δεκέμβριος 2022

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τους γονείς μου και την οικογένειά μου, ιδίως τη σύζυγό μου Γεωργία, για την εμψύχωση και την υπομονή τους, για να φέρω εις πέρας το όνειρο που πάντα είχα.

Περίληψη

Το RTL-SDR είναι ένας ψηφιακός δέκτης τηλεόρασης DVB-T, ο οποίος μετά από reverse engineering που έγινε για να γραφτούν για αυτόν οδηγοί για το Linux, ανακαλύφθηκε ότι έχει τη δυνατότητα να βγάζει απευθείας ως έξοδο τα δεδομένα που λαμβάνει το tuner του. Αυτό οδήγησε την κοινότητα των hackers να το υιοθετήσουν και να το χρησιμοποιούν για τη λήψη ψηφιακών και αναλογικών σημάτων από τις συχνότητες των βραχέων κυμάτων μέχρι και τα μικροκύματα. Με τη λήψη αυτών των σημάτων έχουμε τη δυνατότητα να παρακολουθούμε απευθείας τα δεδομένα που μεταδίδονται επάνω στο φυσικό μέσο, δηλαδή στα ραδιοκύματα. Η δυνατότητα αυτή είναι πολύ χρήσιμη για να αναλύσουμε την ασφάλεια των ασύρματων δικτύων και των δεδομένων τους που κάνουν χρήση των παραπάνω ραδιοσυχνοτήτων.

Λέξεις Κλειδιά: *Software Defined Radio (SDR), RTL-SDR, DVB-T, Realtek RTL2832U , Πομπός-Δέκτης, Κεραίες, Ηλεκτρομαγνητικά Κύματα, Φάσμα Συχνοτήτων, GSM 900 MHz, Διαδίκτυο των Πραγμάτων (IoT), Ασφάλεια, Απειλή, Επίθεση, Replay attack, Brute-Force Attack*.

Abstract

The RTL-SDR is a DVB-T digital TV tuner, which after reverse engineering that had been done to be written Linux drivers for it, was discovered that it has the ability to output directly the data which are received by its tuner. This led the hacker community to adopt and use it to receive digital and analog signals from shortwave frequencies to microwaves. By receiving these signals we have the ability to monitor directly the data that are transmitted on the physical medium, which are the radio waves. This ability is very useful to analyze the security of wireless networks and their data that are making use of these former radio frequencies.

KeyWords: *SDR, Software Defined Radio (SDR), RTL-SDR, DVB-T, Realtek RTL2832U, Transceiver- Receiver, Antenna, Electromagnetic Waves, Spectrum, Frequencies, GSM 900 MHz, Intenet of Things (IoT), Security, Threat, Attack, Replay attack, Brute-Force Attack.*

Πίνακας Περιεχομένων

Πίνακας εικόνων

Εισαγωγή

Στο σημερινό ψηφιακό κόσμο έχουμε κατακλυστεί από ραδιοσυχνότητες. Τα πάντα γύρω μας μεταδίδουν δεδομένα και τις περισσότερες φορές ασύρματα. Υπάρχουν κυψελωτά (Cellular) δίκτυα κινητής τηλεφωνίας 3G/4G/5G, ασύρματα τοπικά δίκτυα (Wireless Local Area Networks – WLANs) όπως το IEEE 802.11x (WiFi), ασύρματα προσωπικά δίκτυα (Wireless Personal Area Networks – WPANs) που βασίζονται σε πρωτόκολλα όπως Bluetooth, IrDA και IEEE 802.15.x, καθώς και ασύρματα δίκτυα με μικρή κατανάλωση ενέργειας που βασίζονται σε πρωτόκολλα όπως ZigBee, Z-Wave, LoRa, κ.ά., τα οποία δημιουργούν δίκτυα μεταξύ υπολογιστών αλλά και μικρότερων συσκευών και αισθητήρων, όπως το Διαδίκτυο των Πραγμάτων (Intenet of Things – IoT) (Wright & Ball, 2020). Πώς όμως γίνεται αυτή η μετάδοση; Πώς λειτουργεί αυτή η ασύρματη μετάδοση; Θα μπορούσαμε να τα κάνουμε αυτά τα σήματα πιο κατανοητά, π.χ να τα οπτικοποιήσουμε και να τα επεξεργαστούμε;

Η τεχνική, της ασύρματης μετάδοσης, έχει από μόνη της μια δυσκολία στην κατανόηση και μια ασφάλεια απέναντι σε κάποιον επιτιθέμενο που δεν διαθέτει τον κατάλληλο εξοπλισμό. Χρειάζονται ειδικές διατάξεις κεραιών και συστημάτων για να γίνει η αξιοποίηση των δεδομένων που θα λάβουμε. Κάθε σύστημα μετάδοσης απαιτεί το δικό του εξειδικευμένο υλικό και λογισμικό για να γίνει επεξεργασία, τα οποία έχουν πάρα πολύ μεγάλο κόστος κτήσης αλλά και μεγάλη τεχνική δυσκολία στον χειρισμό τους. Αρκετά από αυτά τα συστήματα δεν είναι διαθέσιμα παρά μόνο σε ειδικές υπηρεσίας ασφάλειας ή σε στρατιωτικές υπηρεσίες.

Σήμερα, ονομάζουμε Hacker το μη εξουσιοδοτημένο άτομο το οποίο συνήθως εισβάλει σε υπολογιστικά συστήματα προκαλώντας κακόβουλες ενέργειες βλάβες, απώλειες ή καταστροφές στα δεδομένα ή και στους υπολογιστικούς πόρους του. Ωστόσο παλαιότερα είχε περισσότερο την έννοια του εξερευνητή, αυτού που επιχειρεί να ανακαλύψει το πως λειτουργεί ένα σύστημα και να το κάνει κτήμα του ή να το αλλάξει τροποποιώντας το για να το κάνει μια διαφορετική χρήση. Παράδειγμα τέτοιου καλοπροαίρετου White Hat Hacker (wikipedia.org, 2022) είναι ο MacGyver από την γνωστή τηλεοπτική σειρά.

Οι Hackers έχουν τις κατάλληλες γνώσεις και ικανότητες να διαχειρίζονται σε μεγάλο βαθμό διάφορα συστήματα. Συνήθως οι Hackers είναι μηχανικοί, ηλεκτρονικοί προγραμματιστές, σχεδιαστές συστημάτων αλλά και άτομα τα οποία ενώ δεν ασχολούνται επαγγελματικά με τομείς της πληροφορικής και της τεχνολογίας, ο τρόπος σκέψης τους είναι δημιουργικός και καινοτόμος.

Για παράδειγμα, προκειμένου να κάνουμε λήψη ραδιοκυμάτων θα πρέπει να έχουμε κάποιο δέκτη, ενώ αν θέλουμε να επικοινωνήσουμε αμφίδρομα με κάποιο δίκτυο θα πρέπει να έχουμε και εκπομπή, οπότε χρειαζόμαστε έναν πομποδέκτη. Πέρα

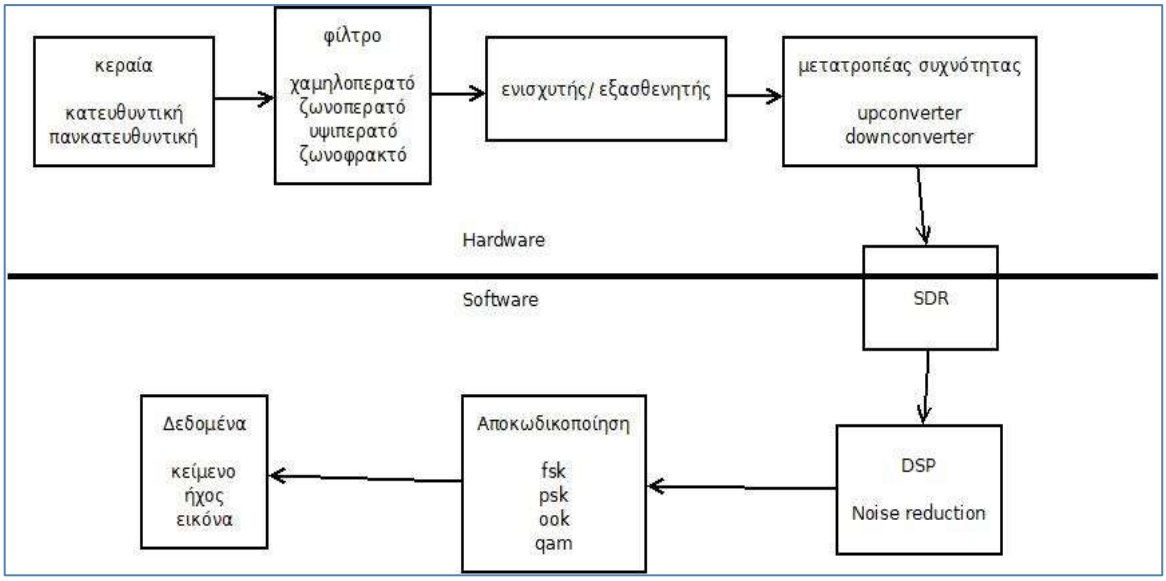
από τον πομποδέκτη θα πρέπει να διαμορφώσουμε κατάλληλα τα δεδομένα μας έτσι ώστε να είναι κατανοητά και να περιέχουν πληροφορίες συμβατές με το δίκτυο. Να χρησιμοποιήσουμε τεχνικές κωδικοποίησης, πολυπλεξίας κατάλληλες για το κάθε δίκτυο.

Αν θέλουμε να πειραματιστούμε και να εκπέμψουμε νόμιμα σε συχνότητες πέρα από τις ISM, πρέπει να έχουμε μία άδεια ραδιοερασιτέχνη (ΜΑΓΚΡΙΩΤΗΣ, 2011). Ο ραδιοερασιτεχνισμός είναι μια υπηρεσία ραδιοεπικοινωνίας, που έχει ως σκοπό την αυτοδιδασκαλία, την αλληλοεπικοινωνία, την τεχνολογική έρευνα των ραδιοερασιτεχνών καθώς και την τηλεπικοινωνιακή υποστήριξη επιχειρήσεων βοηθείας σε περιπτώσεις καταστάσεων έκτακτης ανάγκης και καταστροφών. Η υπηρεσία αυτή διεξάγεται από ραδιοερασιτέχνες, οι οποίοι ασχολούνται με τη ραδιοηλεκτρική τεχνική αποκλειστικά για προσωπικό σκοπό χωρίς όφελος. Προκειμένου να γίνει κανείς ραδιοερασιτέχνης είναι απαραίτητο α) να αποκτήσει πτυχίο ραδιοερασιτέχνη και β) να του χορηγηθεί άδεια ερασιτεχνικού σταθμού ασυρμάτου.

Είναι σημαντικό να ξεχωρίσουμε την ερασιτεχνική χρήση ασυρμάτου από αυτή του ραδιοφώνου, του CB (citizens band radio), του walkie talkie ή των υπηρεσιών ραδιοταξί, γιατί υπάρχει πολλές φορές σύγχυση των εννοιών. Ο ραδιοερασιτεχνισμός είναι ένα αυστηρό και υπεύθυνο χόμπι που ορίζεται από τον Κανονισμό λειτουργίας ερασιτεχνικών σταθμών ασυρμάτου και διεξάγεται αποκλειστικά σε συχνότητες που έχουν εκχωρηθεί για αυτό τον σκοπό από την πολιτεία και ορίζονται από τον Εθνικό Κανονισμό Κατανομής Ζωνών Συχνοτήτων (ΛΙΒΑΝΙΟΣ & ΠΑΝΑΓΙΩΤΟΠΟΥΛΟΣ, 2021). Η ραδιοερασιτεχνική άδεια δεν μας επιτρέπει να κάνουμε παρεμβολές ή να υποκλέπτουμε σήματα τα οποία δεν προορίζονται για το ευρύ κοινό.

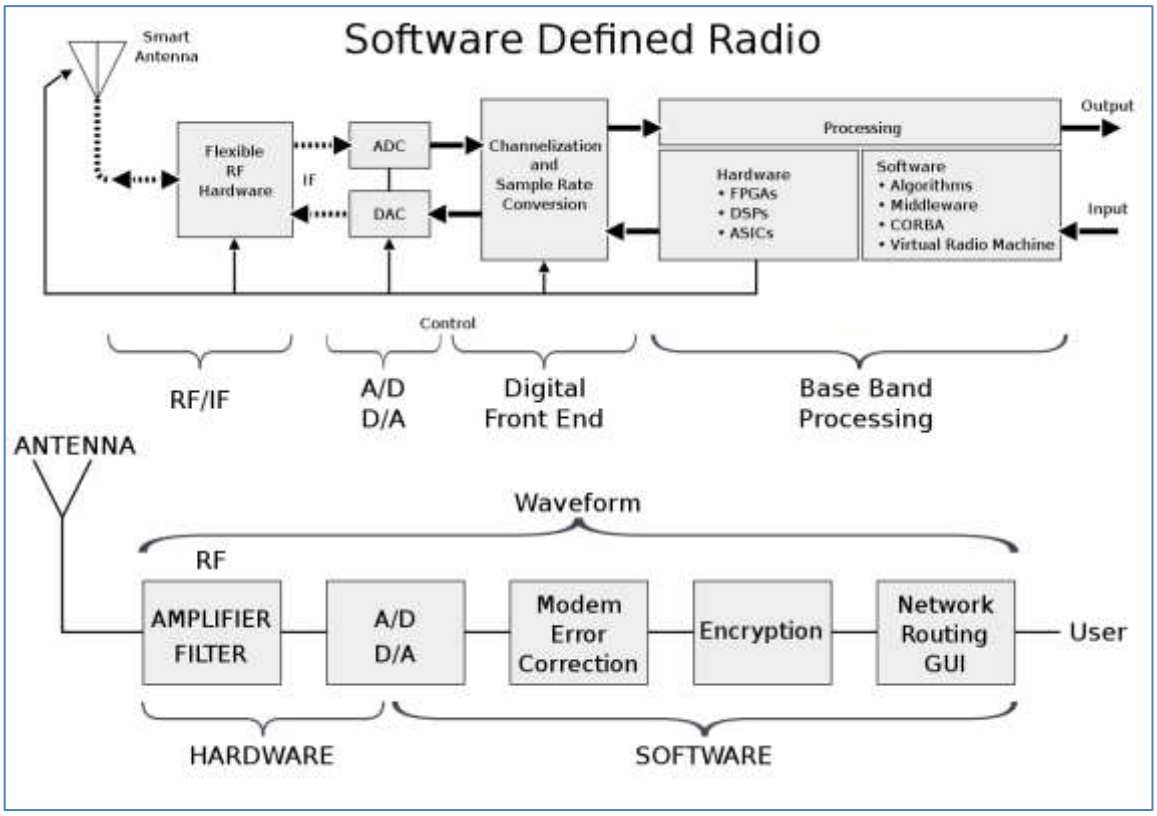
1. Το Software Defined Radio (SDR)

Software Defined Radio (Vachhani & Mallari, 2015) ή απλά SDR ονομάζουμε το υλικό το οποίο μπορεί να κάνει λήψη και έχει τη δυνατότητα να εξάγει το σήμα που λαμβάνει ο δέκτης απ' ευθείας προς χρήση παρακάμπτοντας την όποια αποδιαμόρφωση. Δηλαδή μπορεί να δώσει τα δεδομένα που λαμβάνει ο δέκτης από την συχνότητα που του έχει ορισθεί απευθείας στον χρήστη για επεξεργασία. Αυτή η λειτουργία είναι πάρα πολύ χρήσιμη και υφίσταται ήδη σε διάφορες ηλεκτρονικές συσκευές. Οι δέκτες αυτοί δεν υλοποιούν όλα τα τμήματα ενός δέκτη ραδιοκυμάτων με hardware αλλά και με software. Χρησιμοποιούν πολύπλοκους μαθηματικούς υπολογισμούς σε πραγματικό χρόνο και καταφέρνουν να αντικαταστήσουν τα υλικά τμήματα ενός δέκτη, όπου η παραδοσιακή σχεδίαση θα τα δρομολογούσε σε κυκλώματα με τρανζίστορ ή άλλης μορφής ηλεκτρονικά.



Εικόνα 1. Διάγραμμα διασύνδεσης SDR δέκτη

Το πλεονέκτημα δεν είναι μόνο ότι εξοικονομούμε μερικά δεκάδες ευρώ από την σχεδίαση αλλά ότι μπορούμε να μεταβάλουμε σύμφωνα με τις ανάγκες μας τον δέκτη. Έχουμε τη δυνατότητα να αλλάζουμε ταχύτατα την συχνότητα λήψης, το εύρος των φίλτρων, την διαμόρφωση, να συνδυάζουμε τα δεδομένα από πολλούς δέκτες και πολλά άλλα. Όλα αυτά σε πραγματικό χρόνο και με ελάχιστο κόστος.



Εικόνα 2. Αρχή λειτουργίας SDR

Πηγή: https://en.wikipedia.org/wiki/Software-defined_radio#/media/File:SDR_et_WF.svg

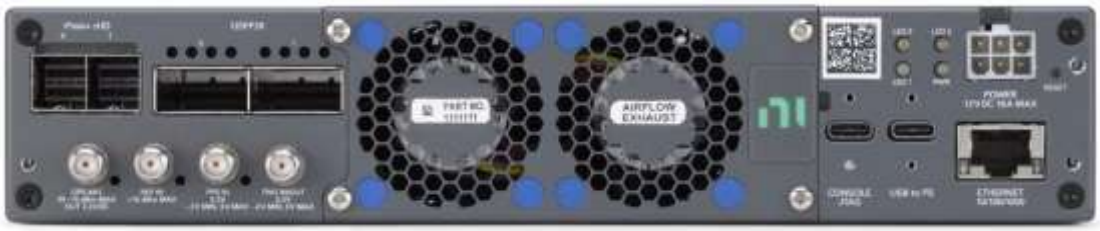
1.1. Εμπορικά SDR

1.1.1. SDR Γενικής Χρήσης

Υπάρχουν διαθέσιμες αρκετές εμπορικές υλοποιήσεις SDR γενικής χρήσης. Κορυφαία σε επιδόσεις είναι τα μοντέλα της σειράς USRP της εταιρίας Ettus, τα οποία είναι ιδανικά για έρευνα και για εργαστηριακές μετρήσεις. Τα κύρια χαρακτηριστικά τους που περιλαμβάνουν τη δυνατότητα λήψης και εκπομπής σε πολλαπλά κανάλια ταυτόχρονα, αλλά και το γεγονός ότι μπορούν να καλύψουν φάσμα συχνοτήτων από 1MHz μέχρι 7.2GHz τα κάνει αξεπέραστα σε δυνατότητες. Το μοντέλο ETTUS USRP X410 SDR έχει τη δυνατότητα χρήσης 4 ανεξάρτητων καναλιών εκπομπής και λήψης εύρους ζώνης 400MHz. Έχει πολλαπλές διασυνδέσεις με υπολογιστή και υποστηρίζεται από πολλά λογισμικά όπως το GnuRadio, Matlab, LabView, Simulink.

Εικόνα 3. ETTUS USRP X410 SDR Front panel

Πηγή: https://www.ettus.com/all-products/usrp-x410/



Εικόνα 4. ETTUS USRP X410 SDR Rear panel

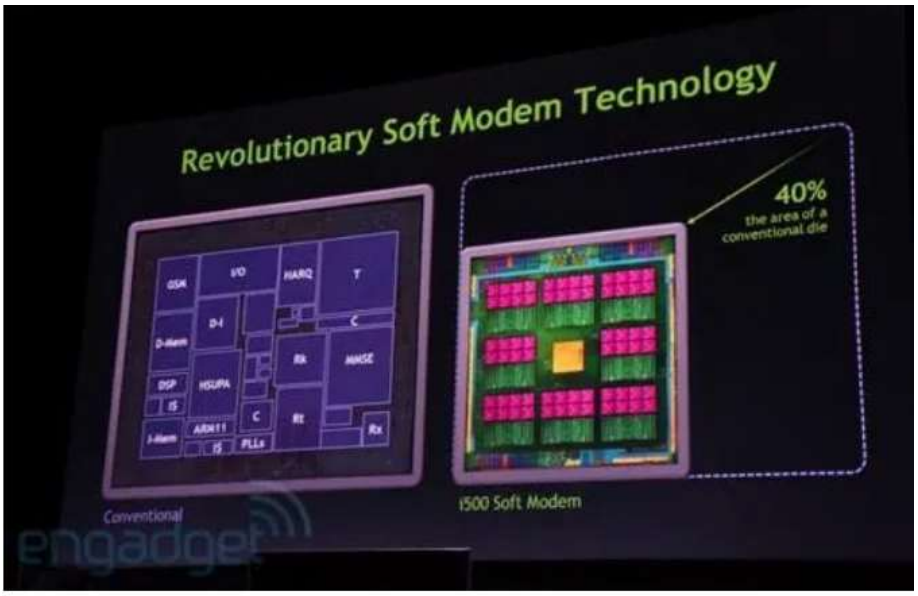
Πηγή: https://www.ettus.com/all-products/usrp-x410/

Φυσικά όλες αυτές οι δυνατότητες έρχονται και με αρκετό υψηλό κόστος, περίπου στα 25.000 ευρώ. Γεγονός που το καθιστά απαγορευτικό για χρήση από χομπίστες, φοιτητές και ερασιτέχνες.

Υπάρχουν και άλλα εμπορικά SDR, με διακυμάνσεις ως προς την τιμή και τις δυνατότητές τους και συνεχώς αναπτύσσονται νέες υλοποιήσεις με πιο εξελιγμένες πλακέτες που υποστηρίζουν περισσότερες δυνατότητες, γιατί το ενδιαφέρον αυξάνει σημαντικά (https://en.wikipedia.org/wiki/List_of_software-defined_radios).

1.1.2. SDR Ειδικού Σκοπού

SDR ειδικού σκοπού υπάρχουν στην αγορά και παράγονται για κατασκευαστές άλλων κυκλωμάτων, όπως σταθμών κινητής τηλεφωνίας, εκπομπή λήψη ψηφιακής τηλεόρασης και άλλων αναγκών όπου είναι επιθυμητή η μεγάλη ευελιξία στη συχνότητα συντονισμού και στο εύρος ζώνης. Παράδειγμα το Chip της NVIDIA i500 (NVIDIA, 2013) που χρησιμοποιείται στους επεξεργαστές NVIDIA Tegra 4 και αντικαθιστά παλαιότερες τεχνολογίες, όπου το κάθε τμήμα του modem υλοποιείται με διακριτές μονάδες hardware.



NVIDIA's apparently still not out of news from its CES 2013 presser -- the company just unveiled the i500 Soft Modem chip. The soft modem, which is the fruit of the company's purchase of Icera and is utilized with Tegra 4, is a baseband processor that can do 1.2 trillion operations per second and is reprogrammable with software to work with a lot of different networks. The modem, which is 40 percent the size of a conventional baseband chip, is sampling to manufacturers this month.

Εικόνα 5. Hardware VS Software Modem Πηγή Hardware VS Software Modem

Πηγή: https://www.nvidia.com/docs/IO/116757/NVIDIA_Quad_a15_whitepaper_FINALv2.pdf

NVIDIA Software Defined Modem

The **NVIDIA i500** is a revolutionary and power efficient, multi-mode soft-modem that supports advanced next-generation air interfaces and connectivity technologies. Built on the proven Icera **Software Defined Radio (SDR)** technology, the i500 enables significantly higher user throughput, advanced modem features, better voice quality and lower cost on one of the smallest, most power-efficient footprints in the industry.

Key Specifications of NVIDIA i500:

- Up to 1.3GHz 8 programmable, fully-gated cores (800 Gops/core), NVIDIA DXP® architecture
- 28nm HP High-K Metal Gate process, Ultra-low voltage
- 7 x 7mm package, 40% the size of comparable conventional 4G modem
- Multiband LTE UE Category 3 100Mbps, HSPA+ 42 Mbps, GSM/GPRS/EDGE,
- Fully integrated 2G/3G voice, CSFB and VoLTE support

Εικόνα 6. Πληροφορίες SDR NVIDIA i500 Πηγή Hardware VS Software Modem

Πηγή: https://www.nvidia.com/docs/IO/116757/NVIDIA_Quad_a15_whitepaper_FINALv2.pdf

1.2. Ερασιτεχνικά SDR

Υπάρχουν αρκετές προσπάθειες για κατασκευή SDR για τις ανάγκες πειραματισμού, οπότε έχουν αναπτυχθεί SDR που είναι διαθέσιμα είτε σε μορφή ολοκληρωμένου προϊόντος ή σε πλακέτα που πρέπει να συναρμολογηθεί do it yourself KIT. Αρκετά από αυτά έχουν δυνατότητες εκπομπής λήψης και πλούσιο API για προγραμματισμό.

Εικόνα 7. HackRF One SDR Kit

Πηγή: https://greatscottgadgets.com/hackrf/one/

Πίνακας 1. Σύγκριση RTL-SDR με εμπορικές υλοποιήσεις Wide band SDRs

Comparisons with other common Wideband Commercial Software Defined Radios

SDR	Tune Low (MHz)	Tune Max (MHz)	RX Bandwidth (MHz)	ADC Resolution (Bits)	Transmit? (Yes/No)	Price ($USD)
RTL-SDR (R820T)	24	1766	3.2	8	No	~20
Funcube Pro+	0.15 410	260 2050	0.192	16	No	~200
Airspy	24	1800	10	12	No	199
SDRPlay	0.1	2000	8	12	No	149
HackRF	30	6000	20	8	Yes	299
BladeRF	300	3800	40	12	Yes	400 & 650
USRP 1	DC	6000	64	12	Yes	700

Πηγή: https://www.rtl-sdr.com/about-rtl-sdr

1.3. Συστήματα που μπορούν να αντικατασταθούν από SDR

Πριν την εμφάνιση των SDR η λήψη των σημάτων γινότανε με τους γνωστούς δέκτες σημάτων. Όπως τα ραδιόφωνα βραχέων κυμάτων ή με ποιο εξειδικευμένους δέκτες βραχέων. Οι δέκτες αυτοί ενώ έχουν την δυνατότητα λήψης σε μεγάλο εύρος συχνοτήτων έχουν περιορισμό ως προς εύρος ζώνης. Έχουν δυνατότητα λήψης μόνο 2-3KHz και ελάχιστες δυνατότητες απεικόνισης και επεξεργασίας. Το δε κόστος τους είναι αρκετές εκατοντάδες ευρώ. Το RTL-SDR έχει δώσει νέους ορίζοντες στους πειραματισμούς και στην αντικατάσταση αυτών των δεκτών, καθώς δίνει υπερδιπλάσιες δυνατότητες και ένα κλάσμα του κόστους.

RECEIVER			
Circuitry		Double super heterodyne (except for W-FM) Single conversion (W-FM)	
Intermediate Frequency	A band	B band: FM/AM/SSB	B band: W-FM
1st IF	59.85MHz	57.60MHz	10.8MHz
2nd IF	450kHz	450kHz	
Sensitivity			
Main A band: 144/430MHz (FM 12dB SINAD)		Less than 0.18 µV	
Sub B band: AM (approximate)		7.08 µV (0.3 – 0.52MHz) 2.24 µV (0.52 – 1.8MHz) 0.89 µV (1.8– 50MHz) 0.40 µV (118 – 250MHz) 0.40 µV (380 – 500MHz)	
Sub B band: FM (approximate)		0.40 µV (5 – 108MHz) 0.28 µV (118 – 144MHz) 0.22 µV (144 – 225MHz) 0.89 µV (225 – 250MHz) 0.40 µV (380 – 400MHz) 0.22 µV (400 – 450MHz) 0.40 µV (450 – 520MHz) 7.08 µV (520 – 700MHz) 1.26 µV (800 – 950MHz) 0.40 µV (950 – 1300MHz)	
Sub B band: W-FM (approximate)		3.16 µV (50 – 108MHz) 2.82 µV (150 – 222MHz) 3.98 µV (400 – 500MHz)	
Sub B band: SSB (approximate)		0.45 µV (3 – 30MHz) 0.40 µV (30 – 50MHz) 0.22 µV (144 – 148MHz) 0.22 µV (430 – 450MHz)	
Squelch		Less than 0.13 µV	
Selectivity			
-6dB		More than 12kHz	
-40dB		Less than 28kHz	
Low frequency output (at 8 ohms, 10% distortion)		More than 300mW at 7.4V	

Εικόνα 8. Χαρακτηριστικά του δέκτη Kenwood TH-F7Radio Transceiver

Πηγή: https://www.kenwood.com/sg/com/amateur/th-f7e/

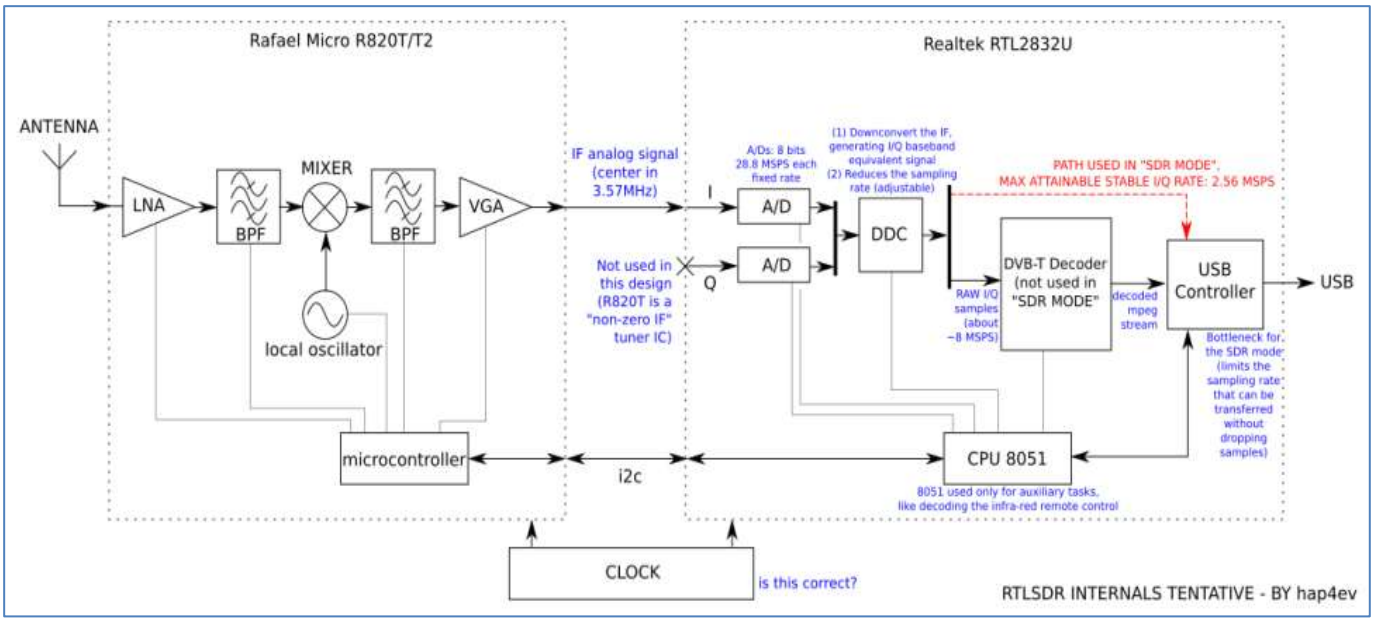
1.4. Το RTL-SDR project

Πριν κάποια χρόνια ο Eric Fry επεξεργαζόταν ένα DVB-T stick το οποίο προοριζόταν για λήψη ψηφιακής τηλεόρασης. Ήθελε να γράψει οδηγούς λειτουργίας για το λειτουργικό σύστημα Linux. Ο κατασκευαστής δεν διέθετε οδηγούς και οι πληροφορίες για την λειτουργία των εσωτερικών εξαρτημάτων του DVB-T stick ήταν περιορισμένες.

Οι οδηγοί των συσκευών συνήθως αποτελούνται από δύο μέρη. Ένα μέρος είναι το firmware, ο κώδικας ο οποίος ανεβαίνει στην συσκευή και τρέχει στον εσωτερικό επεξεργαστή της, έτσι ώστε να επικοινωνεί με τον υπολογιστή. Αυτό το κομμάτι είναι σχετικά εύκολο να το εξάγουμε από τον υπάρχοντα οδηγό των Windows. Διότι δεν έχει σχέση με το λειτουργικό σύστημα και μπορεί να χρησιμοποιηθεί αυτούσιο στο Linux. Το δεύτερο κομμάτι έχει να κάνει με το λογισμικό που τρέχει στο λειτουργικό σύστημα και διασυνδέει το hardware με τις κλίσεις του λειτουργικού αλλά και των προγραμμάτων

του χρήστη. Αυτό είναι το πιο δύσκολο κομμάτι καθώς το Linux και τα Windows, που προερχόταν ο driver, παρουσιάζουνε μεγάλες διαφοροποιήσεις μεταξύ τους.

Εικόνα 9. Realtek DVB-T+DAB+FM stick



Εικόνα 10. Διάγραμμα λειτουργίας μικροεπεξεργαστή Realtek RTL2832U

Πηγή: reddit.com χρήστης hap4ev

Κάνοντας λοιπόν reverse engineering στον οδηγό λειτουργίας (driver) του DVB-T stick για τα Windows και προσπαθώντας να αποκωδικοποιήσει τις λειτουργίες των ενσωματωμένων κυκλωμάτων (chips) μικροεπεξεργαστών που περιείχε μέσα του, ο Eric

Fry ανακάλυψε μια ακόμα ενδιαφέρουσα λειτουργία. Μπορούσε να λάβει άμεσα ψηφιακά δεδομένα RF από το tuner.

Στο ολοκληρωμένο κύκλωμα μικροεπεξεργαστή Realtek RTL2832U εντόπισε ότι μετά την ψηφιοποίηση του σήματος που λάμβανε ο δέκτης από το κύκλωμα του μετατροπέα A/D (Analog to Digital Converter) και την επεξεργασία της συχνότητας του από τον μετατροπέα DDC (Digital Down Converter) υπήρχε μία εναλλακτική δίοδος για την έξοδο των δεδομένων προς την διεπαφή USB και την αποστολή τους στον υπολογιστή. Η εναλλακτική αυτή έξοδος, παρέκαμπτε τη λειτουργία της αποκωδικοποίησης DVB-T του σήματος και έδινε σε RAW μορφή το αποτέλεσμα του μετατροπέαA/D στην έξοδο της θύρας USB. Αυτή η έξοδος είναι πιο περιορισμένη καθώς έχει δυνατότητα ρυθμού δειγματοληψίας μόνο 2.56 MSPS(Mega Samples Per Second) σε σχέση με τα 8 MSPS που διαθέτει για αποδιαμόρφωση DVB-T, αλλά είναι αρκετά για χρήση ως SDR (Stewart, και συν., 2015).

1.4.1. Οι οδηγοί λειτουργίας (drivers)

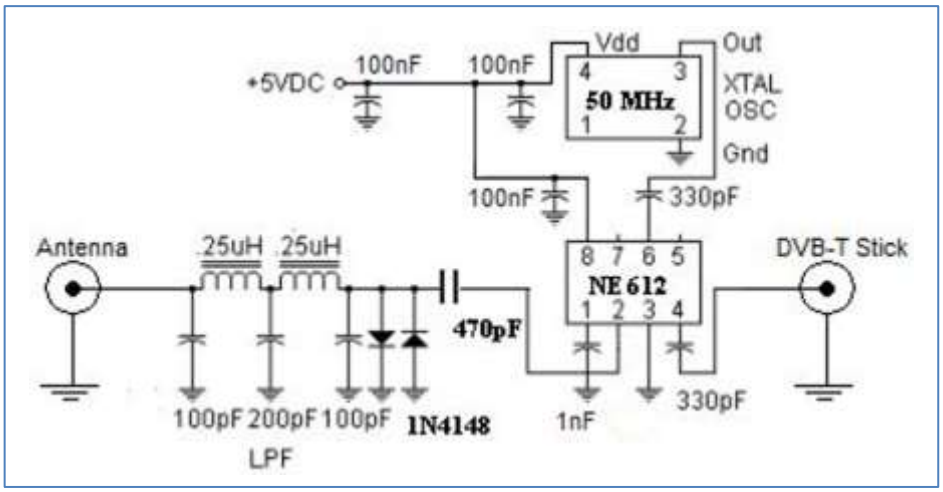
Μαζί με τον οδηγό λειτουργίας (driver) που τελικά αναπτύχθηκε για τη λειτουργία της κάρτας τηλεόρασης Realtek DVB-T+DAB+FM stick, γράφτηκε και ένας δεύτερος οδηγός (driver) για τη λειτουργία της κάρτας ως SDR. Ο οδηγός αυτός, αλλά και ολόκληρο το project ονομάστηκε RTL-SDR από το όνομα του chip RTL2832U (realtek.com, 2019) της κατασκευάστριας εταιρίας Realtek που έδωσε αυτή τη δυνατότητα. Με την ανάπτυξη του SDR driver δημιουργήθηκαν και οι πρώτες εφαρμογές για τη χρήση του στο λειτουργικό Linux και καθώς ήταν ανοιχτό λογισμικό αμέσως έγιναν compile και στα άλλα λειτουργικά συστήματα.

1.4.2. Μετατροπείς Upconverter - Downconverter

Το RTL-SDR έχει τη δυνατότητα λήψης σημάτων στο εύρος συχνοτήτων 24 – 1766 MHz. Υπάρχουν όμως αρκετές ενδιαφέρουσες επικοινωνίες κάτω από τα 24MHz. Για να μπορέσουμε να κάνουμε λήψη αυτών των χαμηλών συχνοτήτων υπάρχουν δύο λύσεις:

A) Κατασκευή ενός κυκλώματος μετατροπής upconverter όπου μπορούμε να ανεβάσουμε τις χαμηλές συχνότητες υψηλότερα, έτσι ώστε να είναι εντός των δυνατοτήτων του δέκτη μας.
B) Χρησιμοποίηση της τελευταίας έκδοσηςRTL-SDR Version 3 η οποία έχει δυνατότητα direct sampling, οπότε έχει τη δυνατότητα να λαμβάνει στο εύρος συχνοτήτων 0 – 1766 MHz.

Στα πλαίσια του πειρατικού μέρους της παρούσας πτυχιακής εργασίας επέλεξα την κατασκευή του upconverter γιατί το RTL-SDR που κατέχω είναι παλαιότερης έκδοσης και δεν υποστηρίζει direct sampling.

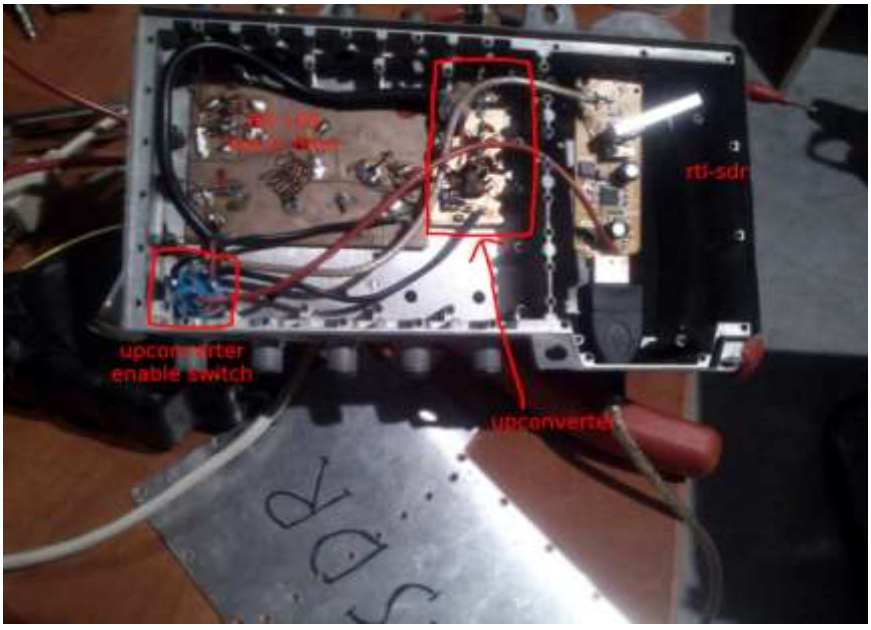


Εικόνα 11. Ηλεκτρονικό διάγραμμα Upconverter

Πηγή: https://www.elektroda.pl/rtvforum/topic2892355.html

Η αρχή λειτουργίας του upconverter είναι απλή. Στην είσοδο από την κεραία έχει ένα χαμηλοπερατό φίλτρο με αποκοπή στα 30MHz. Μετά υπάρχει ένα ψαλιδιστής σήματος με δύο διόδους (1n4148), για να αποτρέψει την υπερφόρτωση του μείκτη και ο πυκνωτής (470pF) κόβει το DC ρεύμα. Ο μείκτης (NE612) χρησιμοποιεί ένα ταλαντωτή (XTAL) στα 50MHz οπότε οι συχνότητες από 0 έως τα 30MHz ανεβαίνουν από 50 έως 80MHz και είναι εντός των δυνατοτήτων λήψης του RTL-SDR (James H. Mclellan, 2019).

Μετά την κατασκευή του upconverter έβαλα και έναν διακόπτη έτσι ώστε να μπορώ να τον ενεργοποιώ όποτε τον χρειάζομαι. Επιπλέον έχω κατασκευάσει ένα bandblock φίλτρο για να μειώσω την λήψη των ραδιοφωνικών σταθμών, που λόγο της μεγάλης του ισχύς κλείνουν (Auto Gain Control) την είσοδο του δέκτη με αποτέλεσμα να μην μπορούν να ληφθούν τα ασθενέστερα σήματα.



Εικόνα 12. Ιδιοκατασκευή RTL-SDR μαζί με Upconverter σε μεταλλικό κουτί

Ο downconverter έχει παρόμοια λειτουργία με τον upconverter με τη διαφορά ότι κατεβάζουμε τις συχνότητες πάνω από τα 1.7GHz σε πιο χαμηλές για να επιτευχθεί η λήψη τους από το RTL-SDR. Ο εξοπλισμός αυτός είναι αρκετά πιο πολύπλοκος και απαιτητικός για την κατασκευή, επειδή τα μικροκύματα έχουν διαφορετική συμπεριφορά από τα βραχέα. Ένα τυπικό παράδειγμα χρήσης downconverter είναι τα LNB που έχουν τα δορυφορικά πιάτα, τα οποία μετατρέπουν το εύρος των λαμβανόμενων συχνοτήτων από τα 10-12GHz στα 1-2 GHz.

Εικόνα 13. Satellite LNB (Downconverter)

Πηγή: https://el.wikipedia.org/wiki/LNB-LNBF

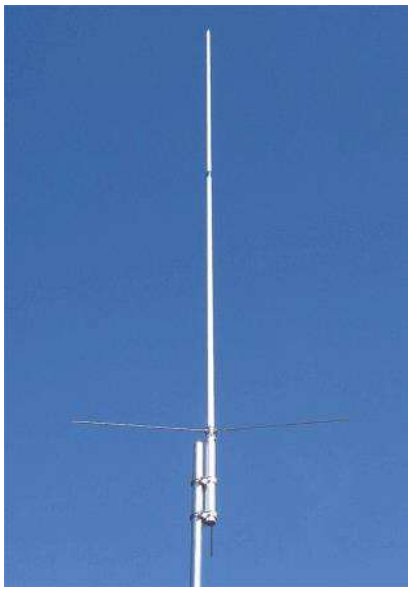
1.5. Κεραίες

Για να κάνουμε χρήση του RTL-SDR, εκτός από μια υπολογιστική συσκευή θα χρειαστούμε και εξειδικευμένες κεραίες. Κάθε κεραία έχει ιδιότητες που την κάνουν να εξειδικεύεται σε ένα εύρος συχνοτήτων που μπορεί να λάβει. Ακόμη οι κεραίες χωρίζονται σε δυο μεγάλες κατηγορίες. Σε κατευθυντικές (directional) και σε πανκαντευθυντικές (omnidirectional).

Οι κατευθυντικές κεραίες παρουσιάζουν μεγάλο κατευθυντικό κέρδος (directional gain) και μας βοηθάνε να κάνουμε λήψη κάποιου αδύναμου σήματος από κάποια συγκεκριμένη κατεύθυνση. Μπορούμε ακόμα, εφόσον μετρήσουμε το λαμβανόμενο σήμα από διάφορες κατευθύνσεις, να εντοπίσουμε την θέση εκπομπής του (γωνιομέτρηση).

Εικόνα 14. Κατευθυντική κεραία τύπου Yagi

Πηγή: https://en.wikipedia.org/wiki/Yagi%E2%80%93Uda_antenna



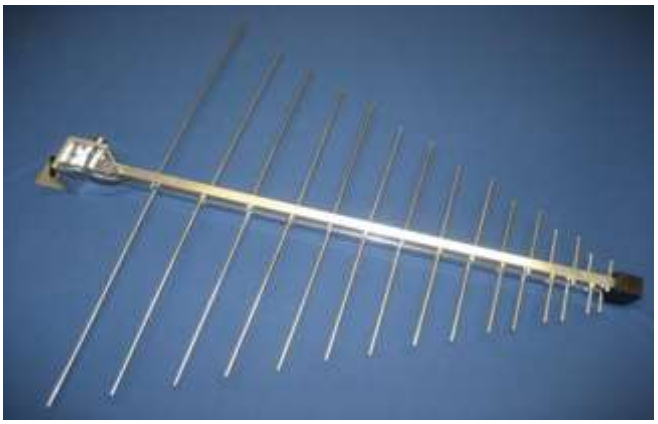
Εικόνα 15. Πανκατευθυντική κεραία

Πηγή: https://www.diamondantenna.net/x300a.html

Οι πανκατευθυντικές κεραίες (omnidirectional) είναι κεραίες που λαμβάνουν το ίδιο σήμα από όλες τις κατευθύνσεις. Η στάθμη σήματος είναι χαμηλότερη από μία κατευθυντική κεραία, αλλά είναι χρήσιμες όταν δεν γνωρίζουμε την θέση του εκπεμπόμενου σήματος ή αν ο σταθμός εκπομπής ή λήψης είναι σε κίνηση.

Εκτός από την κατευθυντικότητα σε μια κεραία έχουμε και το εύρος λειτουργίας, γιατί ανάλογα με την συχνότητα αλλάζει το μήκος κύματος και αλλάζει και κατασκευαστικά η κεραία. Για παράδειγμα στα μακρά – βραχέα έχουμε κεραίες πολύ μεγάλου μεγέθους τύπου σύρματος. Στις υψηλές συχνότητες οι κεραίες είναι περίπου στο ένα μέτρο και μικροκύματα είναι μερικά εκατοστά.

Υπάρχουν και κεραίες που συνδυάζουν τα παραπάνω και μπορούν να λάβουν ένα μεγάλο εύρος συχνοτήτων broadband antennas. Αυτές είναι οι logperiodic και οι discone antenna.



Εικόνα 16. Κεραία Logperiodic Εύρους συχνοτήτων 250-1000MHz

Πηγή: https://www.compeng.com.au/document-library/ce1000e-log-periodic-antenna/

Εικόνα 17 Κεραία Discone, εύρους συχνοτήτων 400 το 4000 MHz

Πηγή: https://www.winradio.com/home/ax24b.htm

1.5.1. Ιδιοκατασκευές Κεραιών

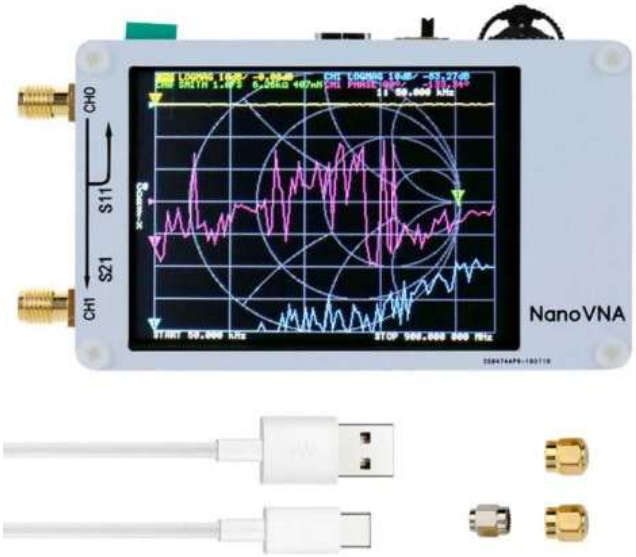
Στα πλαίσια του πειραματικού μέρους της παρούσας πτυχιακής εργασίας για να πραγματοποιήσω τις δοκιμές ευπάθειας με το RTL-SDRχρειάστηκε να κατασκευάσω μια σειρά από κεραίες, οι οποίες έπρεπε να έχουν ειδικά χαρακτηριστικά τα οποία να εξυπηρετούν τα δεδομένα της κάθε ευπάθειας. Οι κεραίες για μελέτη ευπαθειών ασφαλείας δεν είναι διαθέσιμες στο εμπόριο και το κόστος των κεραιών για εργαστήρια είναι μερικές χιλιάδες ευρώ.

Οι δυνατότητες των κεραιών που κατασκεύασα δεν είναι εφάμιλλη με αυτές που χρησιμοποιούνται από τα ειδικά εργαστήρια, ωστόσο, κατάφερα να έχω μετρήσιμα σήματα, έστω και από μικρότερη εμβέλεια. Για την κατασκευή τους χρησιμοποίησα :

- Διάφορα καλώδια από χαλκό, ατσάλι και αλουμίνιο.
- Έναν 3D εκτυπωτή Ender για να φτιάξω τις βάσεις στήριξης των κεραιών.

Εικόνα 18. Κατασκευή κεραίας με 3D εκτύπωση

- Ενσωματωμένη γέφυρα στάσιμων του πομποδέκτη Yaesu FT-857.
- Αναλυτή κεραιών Nano VNA

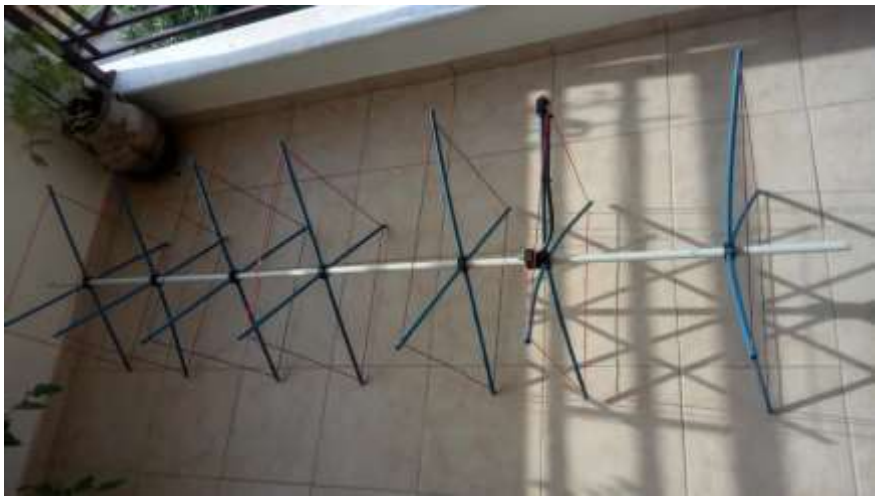


Εικόνα 19. Αναλυτής κεραίας Nano VNA

Πηγή:
https://www.ebay.com/itm/353765109796?hash=item525e0b3024:g:PHAAAOSw3BBeWpA0&amdata=enc%3AAQAHAAAA4KLgr0Jcu52SMFT5wOmJUTDjVpGKTlG6tO%2BcHCZc8%2BH3xZ8NRS%2BM%2FmPctihUrY44ijq2J9J%2F22oiGVivqJSYPIWdctQ3tbmgYQjgFMax%2FYLoSsFvhnEsoePtbML0AdssYqlr4fRNYHrsMnGHYNwCBJgj6kj9Zp4DoMVDcS4eCNfZgpL0Fe6kIDAu1njT0m4aJUmCPJ%2FtlwMaQO8bSqoLDnJObOBlsxAloO43LpFXS%2BM0STGcOeSUlll3AvAd8lSZ2QkD3Hp1RmEFX%2BybsfOeVLSNn5o6Ix%2B%2FhSuQfyRkOT2r%7Ctkp%3ABFBMqp7B345h

Για τις ανάγκες της εργασίας κατασκεύασα τις παρακάτω κεραίες :

- VHF Qubic Quad 145 MHz



Εικόνα 20. Κατασκευή κεραίας Qubic Quad με 3D εκτύπωση

- UHF Moxon 433 MHz

Εικόνα 21. Κατασκευή κεραίας UHF Moxon 433 MHz

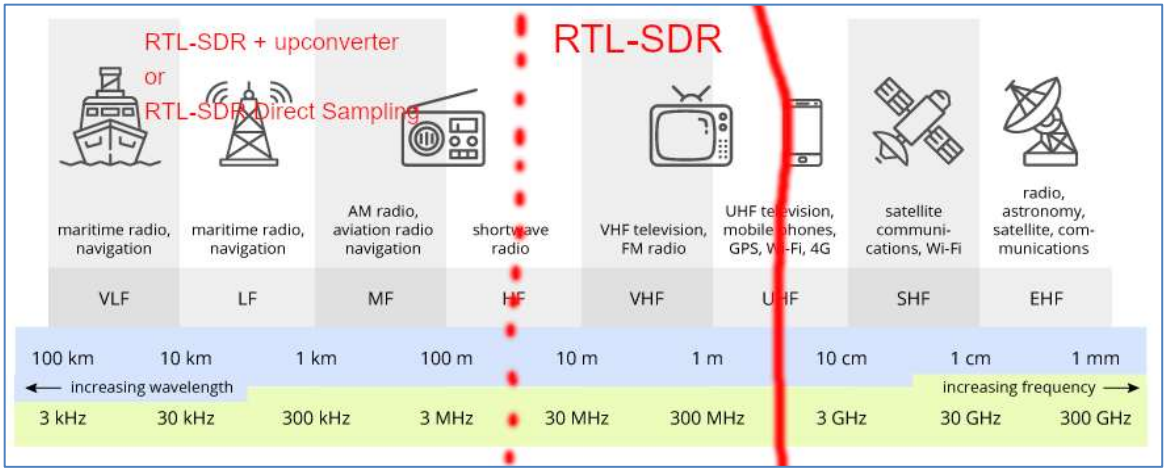
- HF wire dipole 1-50 MHz
- Multiband monopole 100MHz – 1000 MHz

Επίσης, χρησιμοποίησα τις κάτωθι εμπορικές κεραίες:

- Diamond X30 VHF, UHF (145 MHz, 433 MHz)
- Diamond SRH-771 VHF, UHF (145 MHz, 433 MHz)
- Proxel Pro-X1R (Multiband 1-30 MHz)

2. Χρήση και Εφαρμογές RTL-SDR

Στο μεγάλο εύρος συχνοτήτων που μπορεί να λάβει το RTL-SDR υπάρχει σχεδόν το σύνολο των ραδιοφωνικών εκπομπών, από τα μακρά (LW), μεσαία (MW), βραχέα (SW) κύματα του AM ραδιοφώνου, μέχρι το κλασικό FM ραδιόφωνο των 88-108 MHz.



Εικόνα 22. Φάσμα συχνοτήτων και υπηρεσίες RTL-SDR

Πηγή: https://terasense.com/terahertz-technology/radio-frequency-bands/

Είναι τρομερά εντυπωσιακό ότι μια κάρτα ψηφιακής τηλεόρασης, που δεν είχε κατασκευαστεί και δεν είχε κανένα κύκλωμα για να λαμβάνει αναλογικό ραδιόφωνο, μπορεί και λαμβάνει το σύνολο των εκπομπών του ραδιοφώνου σε όλες τις ραδιοφωνικές μπάντες με τη χρήση κατάλληλου λογισμικού.

2.1. Εφαρμογές τερματικού – Application Programmable Interface (API)

Οι πρώτες εφαρμογές που γράφτηκαν ήταν για χρήση τερματικού :

- rtl_fm Αποδιαμορφώνει κατά FM και μπορούμε να ακούσουμε ήχο από ασύρματο ή μουσική από ραδιόφωνο
- rtl_sdr Εξάγει το σήμα σε RAW I/Q (Ramasubramanian, Banerjee, Roy, Pasiliao, & Mukherjee, 2021) για επεξεργασία από άλλο λογισμικό πχ GNU Radio
- rtl_tcp TCP server που μπορεί να στείλει το σήμα στο δίκτυο για να γίνει η επεξεργασία από άλλον υπολογιστή ή και να συνδυαστούν πολλά SDRs.
- rtl_power Δίνει την μέτρηση σήματος σε όποια συχνότητα του ζητηθεί. Χρήσιμο για χαρτογράφηση του φάσματος.

Για να ακούσουμε ένα ραδιοφωνικό σταθμό στα 96.3MHz θα τρέξουμε στο τερματικό:

```
rtl_fm -f 96.3e6 -M wbfm -s 200000 -r 48000 - | aplay -r 48k -f S16_LE
```

- Τρέχουμε το πρόγραμμα rtl_fm όπου θα κάνει λήψη της συχνότητας 96.3e6 σε Hz.

- Το baseband φίλτρο που έχουμε ορίσει είναι wbfm (Wideband FM)
- Η δειγματοληψία RF είναι 200000Hz.
- Η δειγματοληψία ακουστικής συχνότητας εξόδου είναι 48000Hz
- Τέλος στέλνουμε με piping τα δεδομένα σε έναν audio player για αναπαραγωγή (aplay).

Αυτές οι εφαρμογές αποτελούν και το Application Programmable Interface (API) του project όπου πάνω σε αυτές έχουν γραφτεί αρκετές άλλες εφαρμογές τύπου command line, αλλά και γραφικού περιβάλλοντος(GUI) όπως το GQRX.

Ακόμα στις 17/12/2020 ο Hayati Augen ανέφερε στο site του RTL-SDR project (https://www.rtl-sdr.com/tuning-an-r820t2-RTL-SDR-up-to-6-ghz-via-a-harmonic-mixing-driver-hack/) ότι κατάφερε να επεκτείνει το επάνω όριο συχνότητας στα 6GHz με τη χρήση των αρμονικών συχνοτήτων και υψηπερατών φίλτρων. Βέβαια η απόδοση είναι σχετικά χαμηλή αλλά με τη χρήση ενός 1.7 GHz highpass filter και ενός Low Noise Amplifier (LNA) στην είσοδο επιτυγχάνονται αποδεκτά αποτελέσματα.

2.2. Ραδιοερασιτεχνικές εφαρμογές

Για τους ραδιοερασιτέχνες ήταν φανταστικό ένα τέτοιο εργαλείο γιατί μπορούσαν να βλέπουν ένα τεράστιο εύρος από σταθμούς. Για παράδειγμα οι συχνότητες από 7MHz μέχρι 7.2MHz είναι ορισμένες για χρήση από ραδιερασιτεχνικούς σταθμούς ασυρμάτου με διαυλοποίηση 2.7Khz, αυτό περίπου δίνει 70 διαύλους επικοινωνίας. Ένας απλός ασύρματος μπορεί να ακούει μόνο έναν, ενώ πιο ακριβά μηχανήματα (Εικόνα) πάνω από 1000€ ακούνε 2 και εμφανίζουν οπτικά μία περιοχή φάσματος.

Εικόνα 23. Ραδιοερασιτεχνικός Ασύρματος Πομποδέκτης Yaesu FT-991

Πηγή:
https://www.yaesu.com/indexVS.cfm?cmd=DisplayProducts&ProdCatID=102&encProdID=490C4A71118AD0F4E825E89D821B73BB

Το RTL SDR είναι ικανό να ακούει από τα 6MHz μέχρι και τα 8MHz συνεχόμενα. Περίπου 670 διαύλους ταυτόχρονα! Άρα υπάρχει ένα πάρα πολύ δυνατό εργαλείο στα

χέρια των ραδιερασιτεχνών το οποίο έχει και ελάχιστο κόστος. Η αξία ενός τέτοιο DVB TV Tuner είναι περίπου 20 ευρώ.

Δεν είναι φυσικά ανθρωπίνως δυνατό να ακούσει κάποιος 670 συνομιλίες ταυτόχρονα αλλά μπορούν εύκολα να αποθηκευτούν και να επεξεργαστούν π.χ. από ένα νευρωνικό δίκτυο και να εξαχθούν οι όποιες πληροφορίες (Vildyaeva, Egorova, & Vavrenyuk, 2018).

2.3. Άλλες εφαρμογές

Στο μεγάλο εύρος που κάνει λήψη υπάρχουν σχεδόν όλες οι επίγειες επικοινωνίες εκτός από το Wifi 2,4GHz, 5GHz και οι δορυφορικές επικοινωνίες των 10GHz. Φυσικά κάποιες από αυτές με τη χρήση downconverter ή με τον νέο driver με χρήση των αρμονικών συχνοτήτων μπορούν να γίνουν λήψη.

Στις διαθέσιμες συχνότητες υπάρχουν οι σταθμοί Navtex, υπηρεσίες ραδιοπλοήγησης, ατομικά ρολόγια που εκπέμπουν σήματα συγχρονισμού ώρας, κρυπτογραφημένοι στρατιωτικοί σταθμοί, ραδιοτηλέτυπα, μετεωρολογικά FAX, καιρικά και μετεωρολογικά δεδομένα για ναυτιλία και αεροπλοΐας, beacons τηλεμετρίας, συσκευές τηλεχειρισμού, transponders αεροσκαφών και πλοίων, σήματα GPS, κινητή τηλεφωνία GSM 900, CB, Walkie Talkie, μετεωρολογικοί δορυφόροι, ραντάρ και άλλα πολλά.

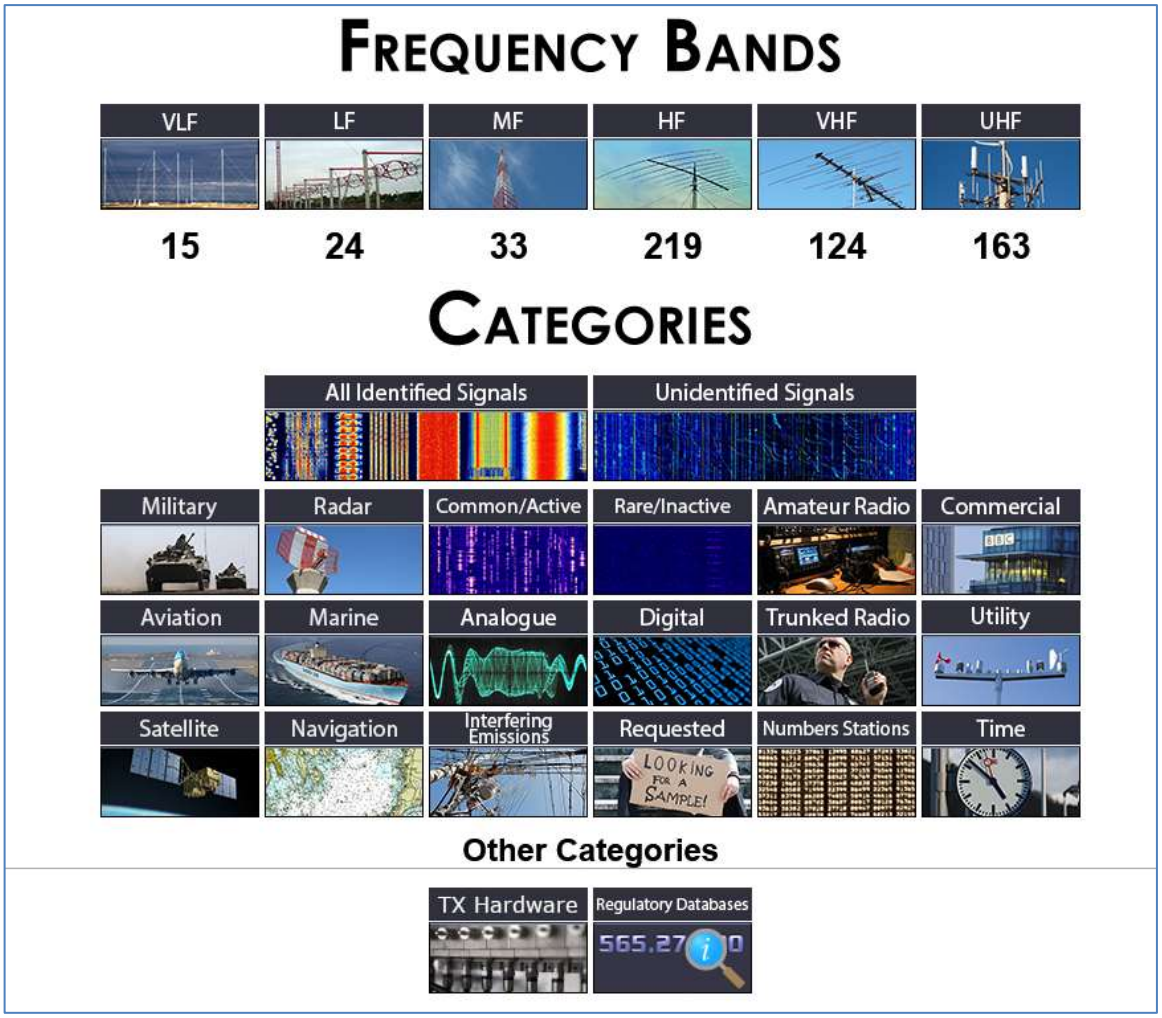
Έχει δημιουργηθεί ένα online wiki όπου χειριστές SDR μαζεύουν και προσπαθούν να αναγνωρίσουν ακουστικά αλλά και οπτικά τα σήματα που λαμβάνουν ανά τον πλανήτη, αλλά και έξω από αυτόν.

Τα RTL-SDR έχουν χρησιμοποιηθεί ακόμα και στην ερασιτεχνική ραδιοαστρονομία όπου έχουν δώσει την εικόνα του γαλαξία καθώς είναι ικανά να λάβουν την συχνότητα ταλάντωσης του υδρογόνου στα 1,2GHz όπως και με κατάλληλες κεραίες και ενισχυτικές διατάξεις έχουν ακούσει και περιστρεφόμενους αστέρες pulsars. (https://www.rtl-sdr.com/category/radio-astronomy-2/).

3. Συνεργατικότητα – opensource

Το project αγαπήθηκε από πολλούς hackers που ασχολούνται με τις ραδιοσυχνότητες και άρχισε να αναπτύσσεται. Εξερευνήθηκαν διάφορα παρόμοια DVB sticks για να διαπιστώσουν αν έχουν παρόμοια συμπεριφορά. Δόθηκαν αναφορές λειτουργίας και αποσφαλμάτωσης των drivers. Φτιάχτηκαν ειδικά προγράμματα για την απεικόνιση του φάσματος. Στα προγράμματα αυτά δημιουργήθηκαν από τρίτους χρήστες ειδικά πρόσθετα (plugins) για την περαιτέρω επέκταση των λειτουργιών τους (Argume, Coaguila, Yanyachi, & Chilo, 2021).

Στο διαδίκτυο σε διάφορα blogs ή wiki έχουν παρουσιαστεί έργα με τη χρήση του RTL-SDR τα οποία αν δεν ήταν το μικρό κόστος του SDR , οι δημιουργοί τους θα ήταν αδύνατο να τα υλοποιήσουν. Επέκτεινε την φαντασία αυτών που ασχολήθηκαν με νέους τομείς. Για παράδειγμα μια ομάδα συλλέγει διάφορα σήματα που υπάρχουν στον πλανήτη μας και προσπαθεί να τα χαρακτηρίσει ακουστικά αλλά και οπτικά.



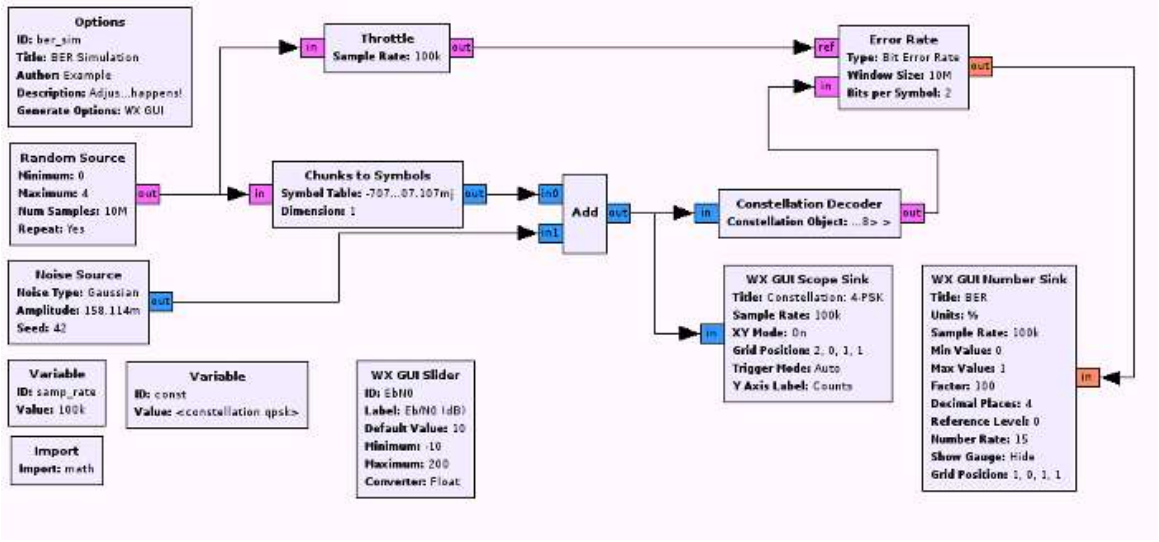
Εικόνα 24. Signal Identification Wiki

Πηγή: https://www.sigidwiki.com

Υπάρχουν αρκετοί που έχουν δημιουργήσει υλοποιήσεις Web-SDR. Μάλιστα, παρέχουν πρόσβαση στον εξοπλισμό τους μέσω του διαδικτύου και μπορούμε να δούμε και να ακούσουμε σήματα από οποιοδήποτε σημείο του πλανήτη. Αν συνδεθούμε σε ένα τέτοιο Web-SDR (http://websdr.org) στις ΗΠΑ θα μπορέσουμε να δούμε σήματα που υπάρχουν εκεί αλλά και να δούμε αν και το δικό μας σήμα από έναν πομπό βραχέων κυμάτων φτάνει ως εκεί. Με τη χρήση των δεκτών αυτών αρκετοί άρχισαν να δείχνουν ενδιαφέρον για το χόμπι του ραδιερασιτεχνισμού και την ενασχόληση του ηλεκτρομαγνητικού φαινομένου. Πολλά από τα περιφερειακά όπως κεραίες και φίλτρα είναι ιδιοκατασκευές οπότε αναπτύχθηκε η μηχανική, η φυσική αλλά και η ηλεκτρονική γνώση.

3.1 Linux

Στο Linux υπάρχει μια σουίτα επεξεργασίας σημάτων ανοιχτού κώδικα το GNU Radio το οποίο με τη χρήση blockδιαγραμμάτων, μπορεί να χειρίζεται δέκτες SDR, να επεξεργάζεται τα δεδομένα που λαμβάνει, να εκτελεί μετασχηματισμούς Fourrier, φίλτρα, μικτές, αποδιαμορφώσεις και να εξάγει τα δεδομένα σε διάφορες μορφές εικόνας, ήχου ή data, σε πραγματικό χρόνο. Ακόμα, υπάρχουν άλλα SDR πέρα του RTL τα οποία έχουν δυνατότητα εκπομπής σήματος οπότε μετατρέπεται σε μια πάρα πολύ δυνατή πλατφόρμα μελέτης ραδιοκυμάτων. Παράγει αρχεία με κώδικα Python και μπορεί φυσικά με piping να συνδεθεί με μια πληθώρα προγραμμάτων και software modems (modulator – demodulator).



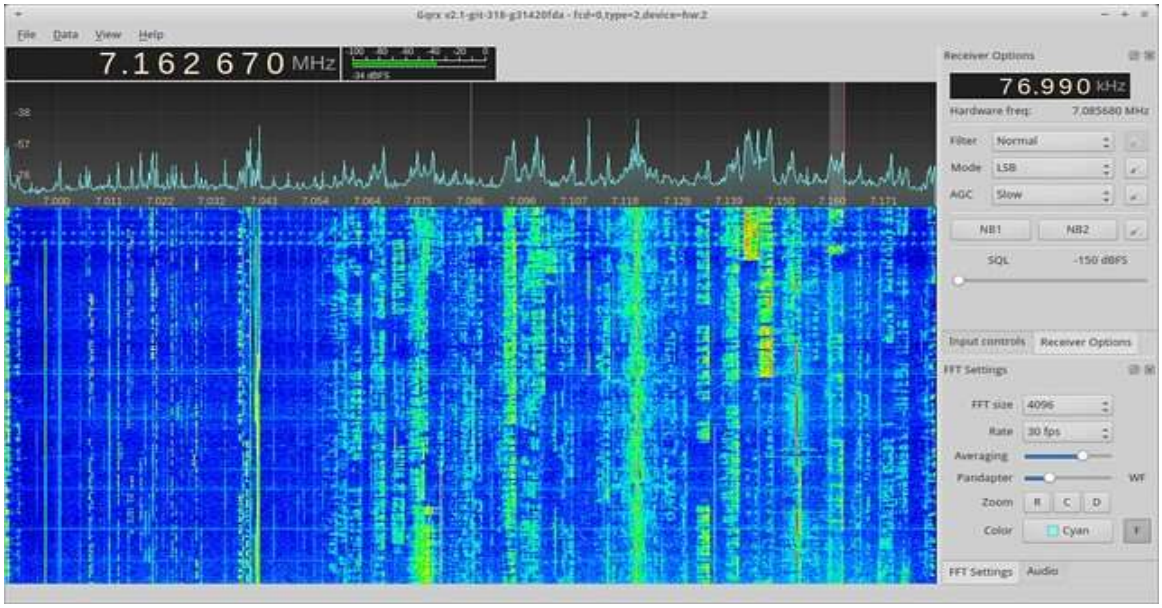
Εικόνα 25. GNU Radio is a free & open-source software development toolkit

Πηγή: https://www.gnuradio.org

Η δυνατότητα piping που δίνουν οι περισσότερες εφαρμογές command line του linux δώσανε την δυνατότητα να εισάγουμε τα δεδομένα σε διάφορους επεξεργαστές και αποκωδικοποιητές σήματος που υπήρχαν από χρόνια και να εξάγουμε άμεσα δεδομένα. Ένα χαρακτηριστικό παράδειγμα είναι το multimon. Που από ένα ακουστικό

σήμα μπορεί να αναγνωρίσει αυτόματα και να εξάγει δεδομένα από όλες τις παρακάτω κωδικοποιήσεις: POCSAG512, POCSAG1200, POCSAG2400, FLEX, EAS, UFSK1200, CLIPFSK, AFSK1200, AFSK2400, AFSK2400_2, AFSK2400_3, HAPN4800, FSK9600, DTMF, ZVEI1, ZVEI2, ZVEI3, DZVEI, PZVEI, EEA, EIA, CCIR, MORSE CW, X10

Εφαρμογές έχουν αναπτυχθεί σε γραφικό περιβάλλον όπου εμφανίζουν το φάσμα του σήματος εκτελώντας μετασχηματισμό Fourier και απεικονίζουν με μεγάλη ακρίβεια το λαμβανόμενο σήμα, όπως βλέπουμε παρακάτω την εφαρμογή GQRX να κάνει λήψη φωνής με διαμόρφωση LSB (Lower Side band) στην συχνότητα 7162.670Hz.

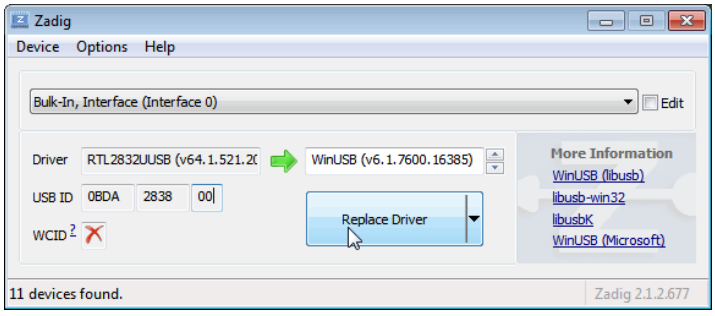


Εικόνα 26. Linux GQRX demodulator

Πηγή: https://gqrx.dk

3.2 Windows

Το project RTL-SDR είναι φυσικά opensource και ο κώδικας είναι διαθέσιμος για μεταγλώττιση σε οποιοδήποτε λειτουργικό, οπότε υπάρχει το API και για windows, απλά υπάρχει μια διαδικασία που πρέπει να γίνει έτσι ώστε να γίνει η χρήση του SDR driver και όχι του TV Tuner driver. Η διαδικασία αυτή γίνεται με το πρόγραμμα zadig και αλλάζουμε το οδηγό της συσκευής με αυτόν του SDR. Αυτό είναι απαραίτητο για να μην αναγνωρίζεται η συσκευή ως δέκτης τηλεόρασης αλλά ως SDR.



Εικόνα 27. Διαχείριση drivers για το RTL-SDR στα Windows

Πηγή: https://zadig.akeo.ie/

3.3 Android

Το android ως linuxοειδές μπορεί και κάνει χρήση του project απλά με την μεταγλώττιση του κώδικα για την αρχιτεκτονική ARM. Η χρήση του κινητού τηλεφώνου, ταμπλέτας ή androidbox αύξησε τις φορητές δυνατότητες του project. Είναι πλέον πολύ απλό να βάλουμε τον εξοπλισμό σε ένα αυτοκίνητο και να σαρώσουμε μια πόλη για να εντοπίσουμε μια παρεμβολή σε ένα σύστημα. Ακόμα με το Android και το rtl_tcp μπορούμε να έχουμε πολλούς μικρούς σταθμούς λήψεως σε ένα WAN δίκτυο και με μικρό κόστος να υλοποιήσουμε ένα πλέγμα για την λήψη και επεξεργασία σημάτων στην περιοχή αυτή.

Εικόνα 28. Android SDR

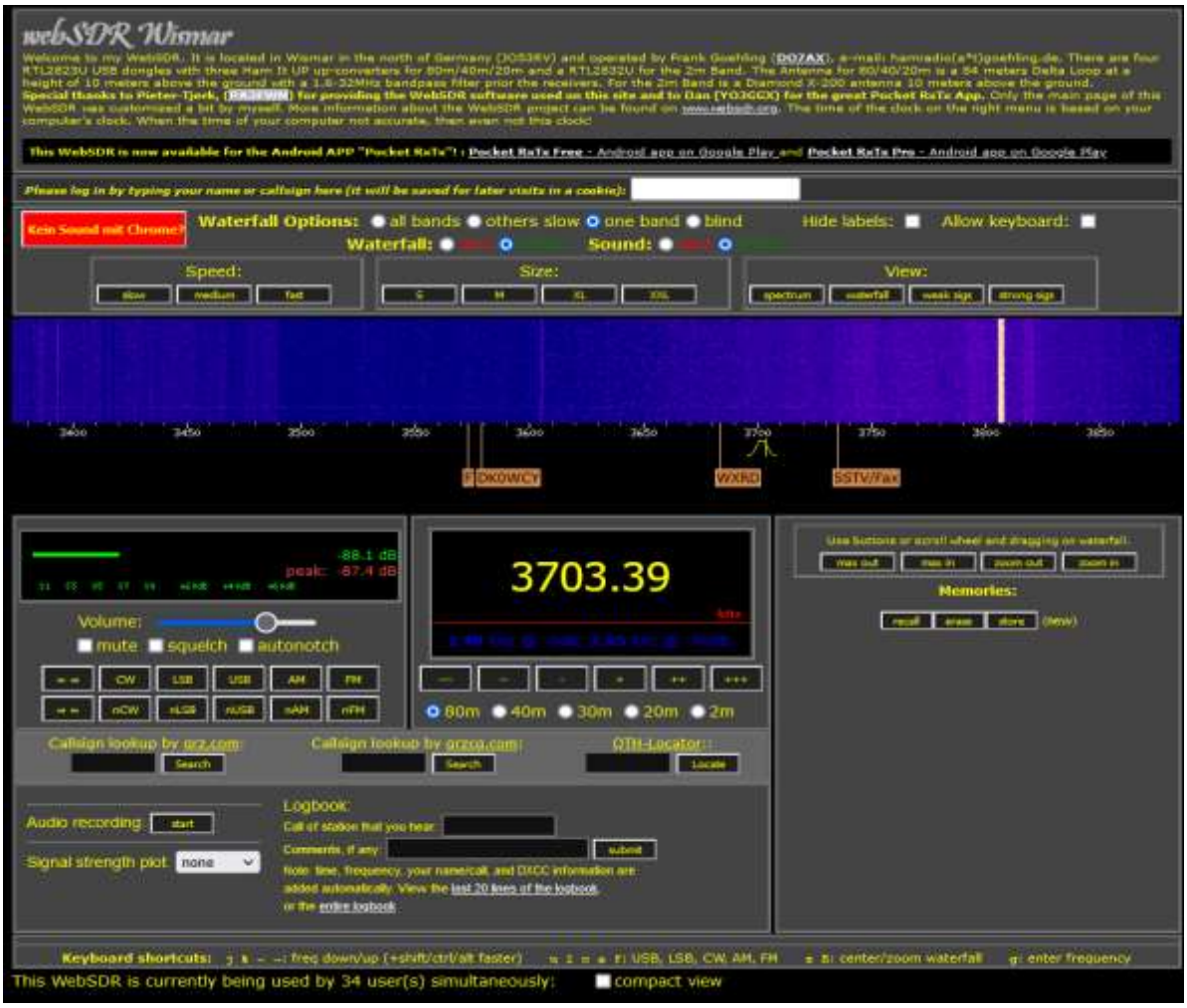
Πηγή: https://www.electronicsforu.com/electronics-projects/software-defined-radio-with-android-smartphones

3.4 WEBSDR

Το WEBSDR (S, J, H, R, & P, 2015) είναι ειδικό λογισμικό που σε συνδυασμό με hardware SDR, μπορούμε να φτιάξουμε servers που με τη χρήση ενός web interface να δούμε απομακρυσμένα ένα SDR.

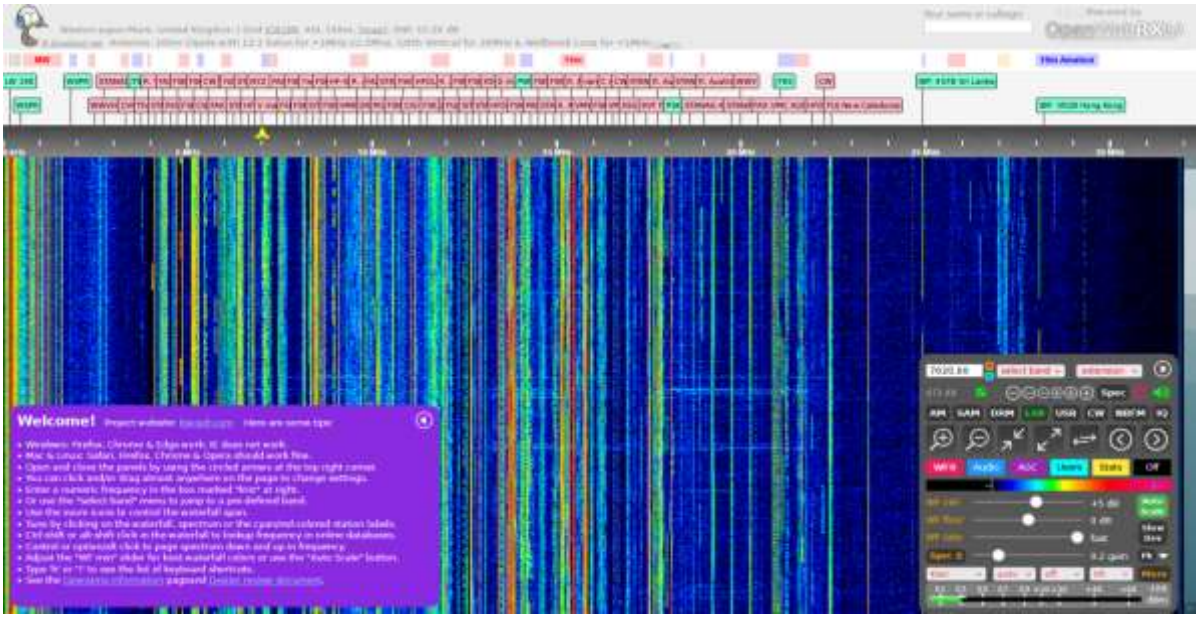
Υπάρχουν δύο αρκετά διαδεδομένα λογισμικά για αυτή τη χρήση, το WEBSDR στην πόλη Wismar της Γερμανίας και το OpenWebRx στο Ηνωμένο Βασίλειο.

Το project OpenWebRx (https://www.openwebrx.de) είναι ανοιχτού κώδικα οπότε μπορεί να το εγκαταστήσει κάποιος στον υπολογιστή του και να λαμβάνει άμεσα σήματα μέσο διαδικτύου από όπου επιθυμεί. Το project έχει μεγάλη κοινότητα χρηστών και συνεχώς αναβαθμίζεται με νέες δυνατότητες επεξεργασίας σημάτων.



Εικόνα 27. WEBSDR στην πόλη Wismar στην Γερμανία

Πηγή: http://dlwis-websdr.ham-radio-op.net:8901



Εικόνα 28. OpenWebRx στο Ηνωμένο Βασίλειο

ΠηγήQ http://radiogeek.co.uk/#freq=433275000,mod=nfm,sql=-150

4. Επισκόπηση των Απειλών και Προκλήσεων Ασφαλείας και Πειραματική Υλοποίηση Δοκιμών Ευπάθειας με τη χρήση του RTL-SDR

4.1 Αναλογικές επικοινωνίες φωνής FM, AM, SSB, digital

Οι αναλογικές επικοινωνίες είναι τελείως ευάλωτες σε κάθε απόπειρα ακρόασης καθώς δεν έχουν καμία κρυπτογράφηση και η μόνη δυσκολία που υπήρχε μέχρι σήμερα ήταν ότι απαιτούσαν έναν ειδικευμένο δέκτη για την ακρόασή τους. Με τη χρήση του SDR όμως έχει εξαλειφθεί η τεχνική αυτή δυσκολία και οι επικοινωνίες αυτού του είδους είναι πλέον εύκολα να αποκαλυφθούν.

Οι ραδιοερασιτέχνες απαγορεύεται από τον νόμο να χρησιμοποιήσουν κρυπτογραφημένες επικοινωνίες ή να μεταδίδουν δεδομένα με άγνωστους κώδικες.

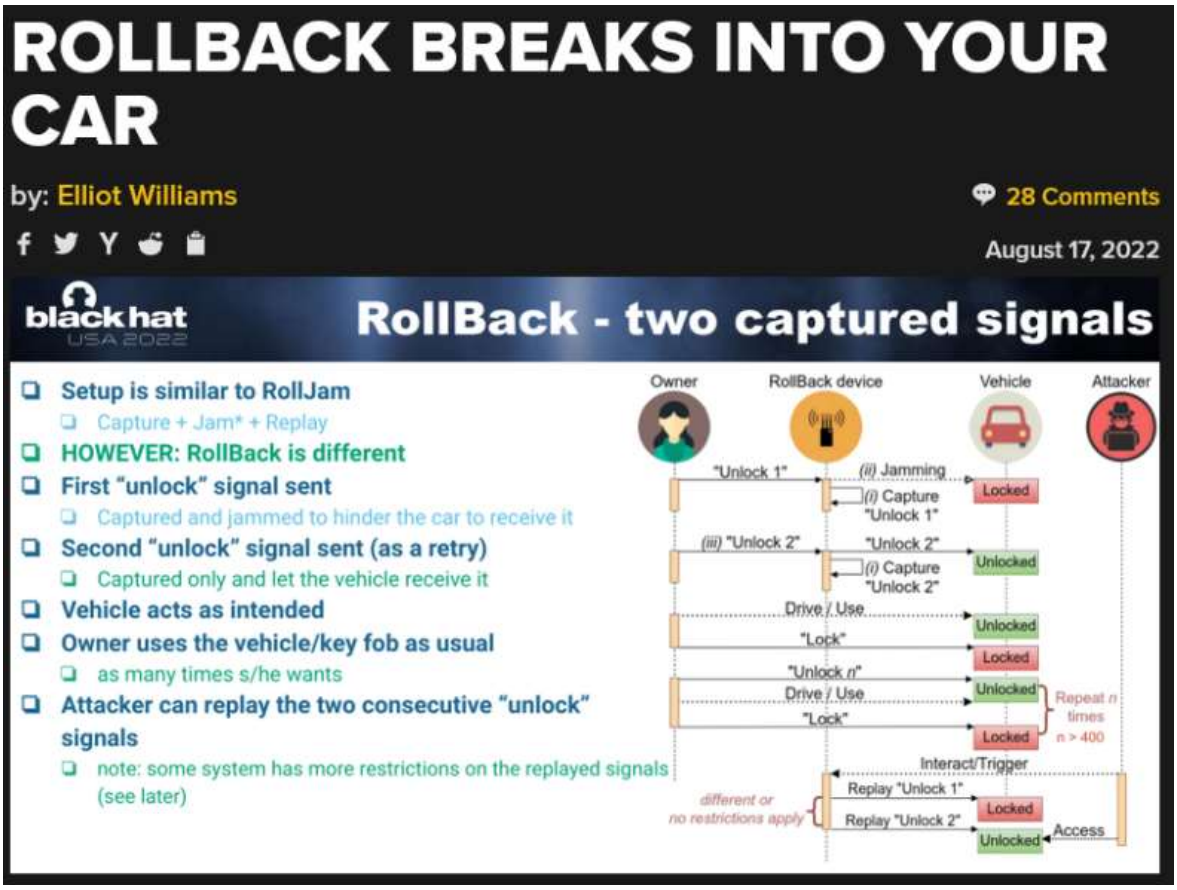
- Ραδιοερασιτεχνικές επικοινωνίες σε mode : FM, AM, LSB, USB, RTTY, PSK, FT8, SSTV, APRS κ.α.
- Επικοινωνίες μπάντας πολιτών CB 27MHz σε FM, AM, USB.
- Επικοινωνίες ιδιωτικών ραδιοδικτύων FM, DMR, P25, TETRA, MOTOTRBO

Οι ψηφιακές επικοινωνίες στα ιδιωτικά ραδιοδίκτυα έχουν δυνατότητα κρυπτογράφησης με πολύ καλά αποτελέσματα. Το γεγονός όμως, ότι υπάρχει αρκετός παλαιός αναλογικός εξοπλισμός που χρησιμοποιείτε ήδη και δεν είναι εύκολο να αγορασθεί νέος ψηφιακός εξοπλισμός κάνουν τα δίκτυα αυτά ευάλωτα σε διαρροή δεδομένων (Καραγιαννίδης Κ.Γεώργιος, 2017).

4.2 Κλειδί αυτοκινήτου

Αρκετά χειριστήρια αυτοκινήτων λειτουργούν στην συχνότητα 433MHz όπου στέλνουν ένα σήμα που κλειδώνει το αυτοκίνητο και ένα σήμα που το ξεκλειδώνει. Με την επίθεση τύπου **replay attack** όπου λαμβάνουμε το σήμα το καταγράφουμε και το ξαναστέλνουμε θα μπορούσαμε να καταγράψουμε το σήμα ξεκλειδώματος και να το στείλουμε όποτε θέλουμε για να ξεκλειδώσουμε ένα αυτοκίνητο.

Ευτυχώς όμως για τους ιδιοκτήτες αυτοκινήτου το σήμα περιέχει έναν κυλιόμενο κρυπτογραφημένο κωδικό οπότε, αν ξαναστείλουμε ένα παλαιότερο κωδικό ξεκλειδώματος αυτός δεν γίνεται δεκτός. Φυσικά και οι κυλιόμενοι κωδικοί παρουσιάζουν ευπάθεια με την διαδικασία που περιγράφεται στην παραπάνω εικόνα.



Εικόνα 29. Επίθεση τύπου Replay σε ραδιοσυχνότητα

Πηγή: https://hackaday.com/2022/08/17/rollback-breaks-into-your-car/

- Λαμβάνουμε των πρώτο κωδικό ξεκλειδώματος και μπλοκάρουμε τον δέκτη του αυτοκινήτου, έτσι ώστε να μην ξεκλειδώσει.
- Ο ιδιοκτήτης νομίζει ότι το αυτοκίνητο δεν έλαβε την εντολή και επαναλαμβάνει.
- Λαμβάνουμε τον δεύτερο κωδικό και πάλι μπλοκάρουμε τον δέκτη.
- Εκπέμπουμε με SDR εκπομπής τον πρώτο κωδικό που είχαμε λάβει και το αυτοκίνητο ανοίγει.
- Έχουμε όμως καταγράψει τον δεύτερο κωδικό, που είναι ενεργός κωδικός ξεκλειδώματος. Οπότε μπορούμε να το αποστείλουμε αν θέλουμε πχ με email σε κάποιο άλλο άτομο στο σημείο που θα κινηθεί το αυτοκίνητο για να το ξεκλειδώσει.

Αρκετοί κατασκευαστές ανακυκλώνουν τους κυλιόμενους κωδικούς οπότε αν εκπέμψουμε αρκετούς από αυτούς σε μια επίθεση εξαντλητικής αναζήτησης (brute force attack) κάποια στιγμή θα πετύχουμε τον σωστό κωδικό. Χαρακτηριστικό παράδειγμα είναι η ευπάθεια που εντοπίστηκε σε συγκεκριμένο κατασκευαστή αυτοκινήτων.

Εικόνα 30. Ευπάθεια CVE-2021-46145 στο χειριστήριο κλειδώματος της HONDA

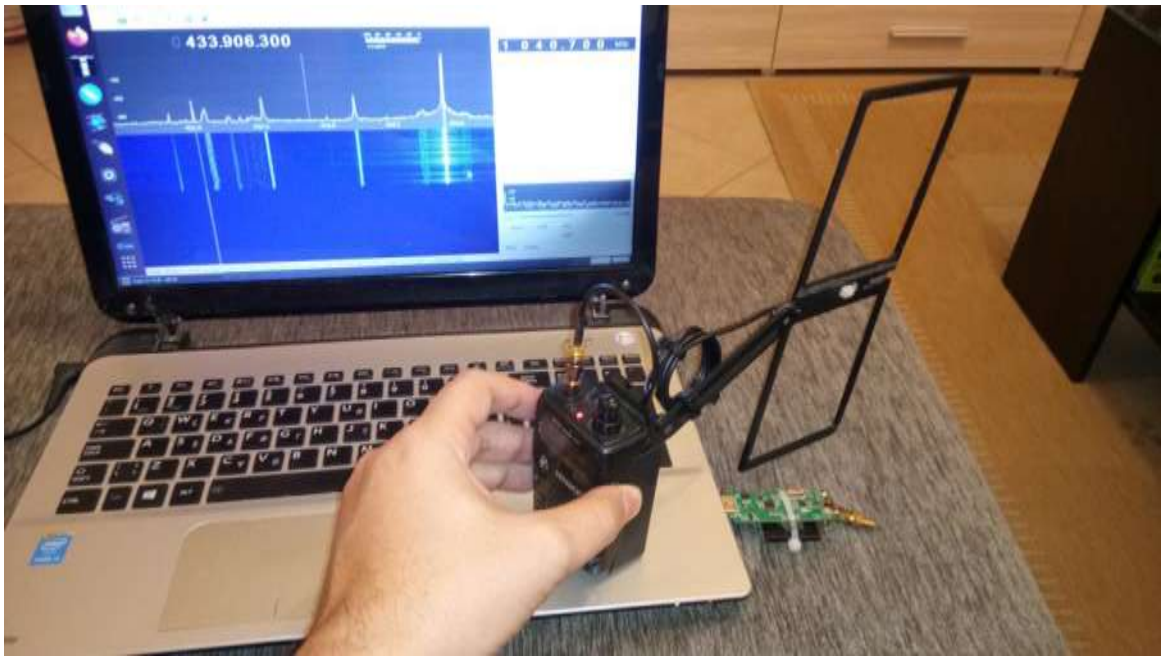
Πηγή: https://hackaday.com/2022/07/08/turns-out-you-can-just-unlock-any-honda-car/

Μπορούμε ακόμα, την ώρα που στέλνεται ο κωδικός από το χειριστήριο, να τυφλώσουμε (deny of service) με μία άλλη δυνατή εκπομπή τον δέκτη του αυτοκινήτου, οπότε ο κωδικός να μην ληφθεί. Επιπλέον πέρα από το γεγονός ότι το αυτοκίνητο θα

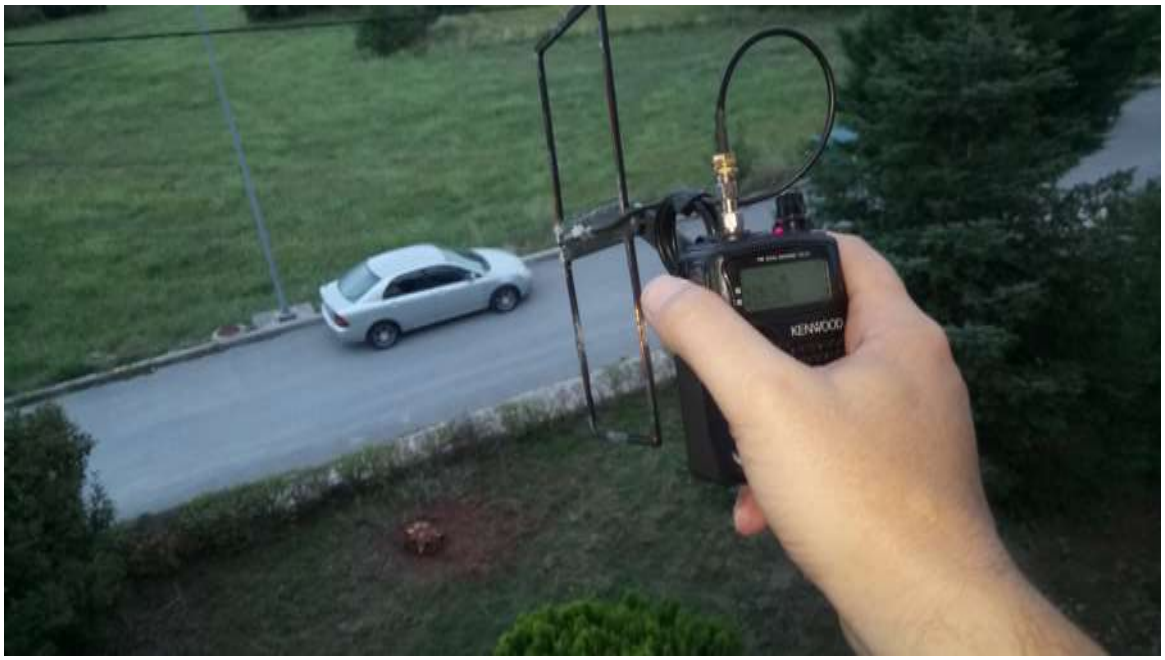
παραμείνει ξεκλείδωτο, αν δεν το παρατηρήσει ο ιδιοκτήτης του, θα έχουμε καταγράψει και έναν λειτουργικό κωδικό ξεκλειδώματος.

Εικόνα 31. Ανίχνευση της συχνότητας λειτουργίας του κλειδιού μου με το RTL-SDR

Στις παρακάτω εικόνες βλέπουμε την καταγραφή της συχνότητας του κλειδιού μου και μετά με τη χρήση ενός φορητού πομποδέκτη και μια ειδικής κατευθυντικής κεραίας υψηλής απόδοσης μπλοκάρω το σήμα κλειδώματος του αυτοκινήτου μου.



Εικόνα 32. Ρύθμιση του πομπού για εκπομπή επάνω στην συχνότητα του κλειδιού



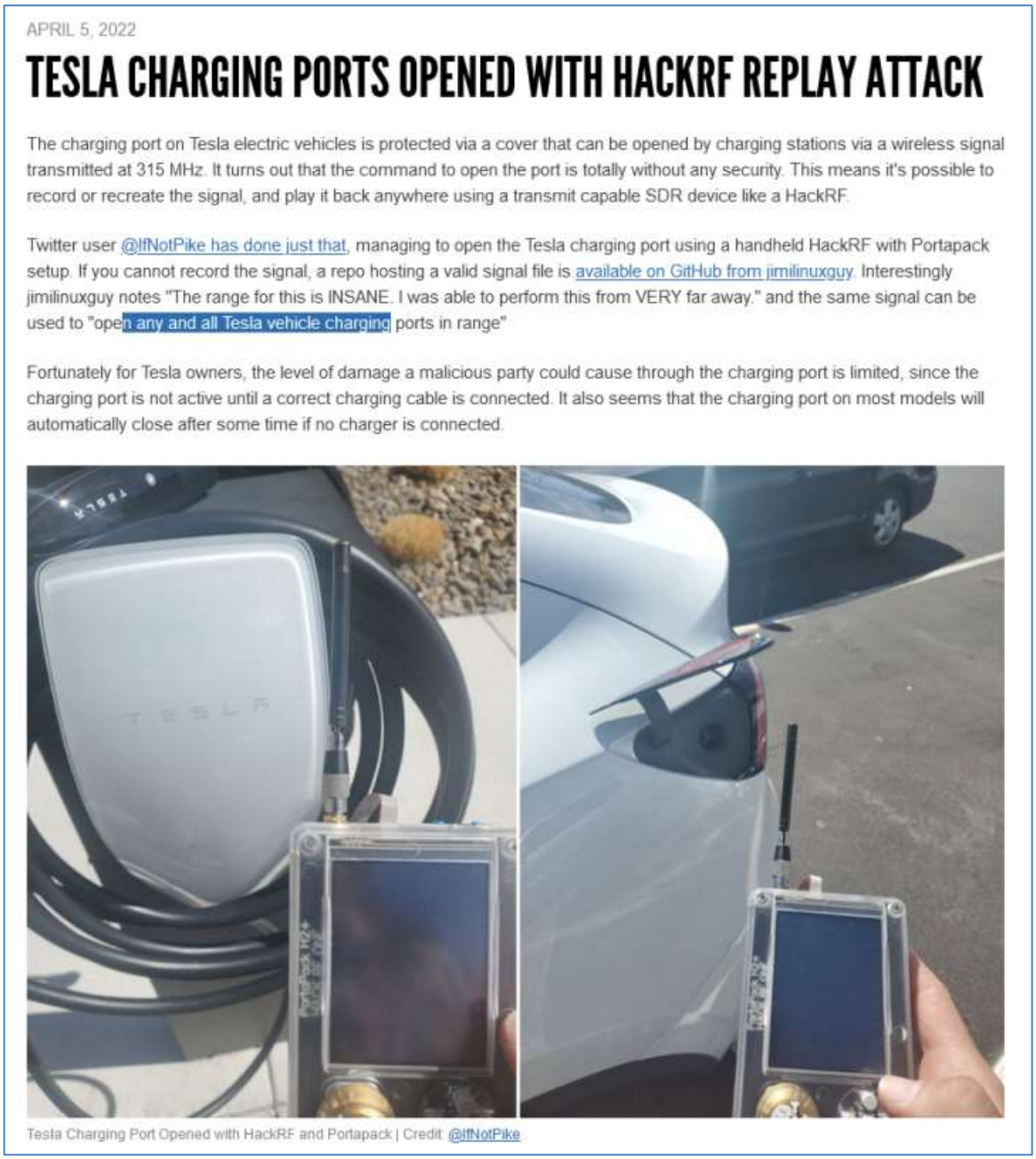
Εικόνα 33. Εκπομπή και μπλοκάρισμα της λειτουργίαε του κλειδιού

Το κλειδί πλέον δεν μπορεί να κάνει καμία ενέργεια στο αυτοκίνητο, ούτε να κλειδώσει, ούτε να ξεκλειδώσει, γιατί το σήμα του μπλοκάρετε από την πολύ ποιο ισχυρή εκπομπή και την κατευθυντική κεραία που στοχεύει τον δέκτη.

4.3 RF remote controls

Πολλά τηλεχειριστήρια για πόρτες γκαράζ στέλνουν σε ραδιοκύματα έναν σταθερό κωδικό, ο οποίος είναι διαφορετικός σε κάθε συσκευή για να μην μπερδεύονται μεταξύ τους, αλλά είναι τελείως μη ασφαλές, γιατί αν γίνει η υποκλοπή του κωδικού αυτού μπορεί να μεταδοθεί και να ανοίξει η πόρτα του γκαράζ. Ένα τέτοιο παράδειγμα ευπάθειας σε τηλεχειρισμό είναι το σύστημα φόρτισης των αυτοκινήτων της Tesla. Μία εταιρία που βρίσκεται στις κορυφαίες εταιρίες τεχνολογίας στον πλανήτη , αλλά παρόλα αυτά δεν εξασφάλισε σωστά την ασφάλεια σε αυτό τον αυτοματισμό στο πορτάκι φόρτισης των οχημάτων της.

Ο κωδικός που στέλνει για να ανοίξει το πορτάκι σε ένα όχημα της Tesla είναι ο ίδιος για όλα τα οχήματα που έχει κατασκευάσει. Αποτέλεσμα αν πάμε σε ένα σταθμό φόρτισης της εταιρίας και καταγράψουμε το σήμα με το RTL-SDR θα είμαστε μετά σε θέση να το αναπαράγουμε και να ανοίξουμε το πορτάκι φόρτισης. Ως θέμα ασφάλειας δεν φαίνεται σημαντικό αλλά αν αναλογιστούμε ότι κάποιος κακόβουλος μπορεί να έχει πρόσβαση στους συσσωρευτές του αυτοκινήτου σίγουρα εγείρει προβληματισμούς.



APRIL 5, 2022

TESLA CHARGING PORTS OPENED WITH HACKRF REPLAY ATTACK

The charging port on Tesla electric vehicles is protected via a cover that can be opened by charging stations via a wireless signal transmitted at 315 MHz. It turns out that the command to open the port is totally without any security. This means it's possible to record or recreate the signal, and play it back anywhere using a transmit capable SDR device like a HackRF.

Twitter user @IfNotPike has done just that, managing to open the Tesla charging port using a handheld HackRF with Portapack setup. If you cannot record the signal, a repo hosting a valid signal file is available on GitHub from jimilinuxguy. Interestingly jimilinuxguy notes "The range for this is INSANE. I was able to perform this from VERY far away." and the same signal can be used to "open any and all Tesla vehicle charging ports in range"

Fortunately for Tesla owners, the level of damage a malicious party could cause through the charging port is limited, since the charging port is not active until a correct charging cable is connected. It also seems that the charging port on most models will automatically close after some time if no charger is connected.

Tesla Charging Port Opened with HackRF and Portapack | Credit: @IfNotPike

Εικόνα 34. Ευπάθεια θύρας φόρτισης TESLA

Πηγή: https://www.rtl-sdr.com/tesla-charging-ports-opened-with-hackrf-replay-attack/

4.4 IOT data comms

Πολλές συσκευές IOT, όπως και πολλά arduino wireless modules μεταδίδουν δεδομένα σε μικρές αποστάσεις με διαμορφώσεις OOK, FSK, LORA. Όλα αυτά τα δεδομένα αν δεν μεταδοθούν κρυπτογραφημένα τότε μπορούν να ληφθούν στο σύνολό τους. Μπορεί τα δεδομένα αυτά να μην είναι μείζονος σημασίας όπως η μέτρηση ενός αισθητήρα. Αλλά με την υποκλοπή και επεξεργασία τους μπορούν να εξαχθούν αργότερα διάφορα συμπεράσματα.

Με τη χρήση της εντολής **`rtl_433`** μπορούμε να δούμε τα περισσότερα από αυτά τα σήματα και να αναλύσουμε τις πληροφορίες τους.

Στην εικόνα βλέπουμε 2 αισθητήρες θερμοκρασίας που λαμβάνω στην περιοχή μου. Όπου μεταδίδουν, ο ένας την εξωτερική θερμοκρασία Bresser-3C 64.6F που αντιστοιχεί σε 18.1C και 56% υγρασία και ο άλλος Nexus-TH την εσωτερική 21.2C με υγρασία 46%.

```
- - - - - - - - - - - - - - - - - - -

time      : 2022-05-12 08:44:16
model     : Bresser-3CH
Id        : 76
Channel   : 1
Battery   : 1
Temperature: 64.60 F
Humidity  : 56 %
Integrity : CHECKSUM
- - - - - - - - - - - - - - - - - - -

time      : 2022-05-12 08:44:45
model     : Nexus-TH
House Code: 163
Channel   : 2
Battery   : 1
Temperature: 21.20 C
Humidity  : 46 %
- - - - - - - - - - - - - - - - - - -

time      : 2022-05-12 08:45:13
model     : Bresser-3CH
Id        : 76
Channel   : 1
Battery   : 1
Temperature: 64.60 F
Humidity  : 56 %
Integrity : CHECKSUM
- - - - - - - - - - - - - - - - - - -

time      : 2022-05-12 08:45:52
model     : Nexus-TH
House Code: 163
Channel   : 2
Battery   : 1
Temperature: 21.30 C
Humidity  : 46 %
```

Εικόνα 35. Καταγραφή αισθητήρων 433MHz της περιοχής μου

Το κενό ασφάλειας στην περίπτωση των αισθητήρων δεν είναι άμεσο αλλά έμμεσο. Για παράδειγμα αν υποκλέψουμε τις θερμοκρασίες από το εσωτερικό των διαμερισμάτων μιας πόλης, θα μπορούμε να δούμε πόσο δαπανά το κάθε σπίτι για θέρμανση ή κλιματισμό και να υπολογίσουμε την οικονομική του κατάσταση και πως μεταβάλλεται αυτή.

Ειδικά στις μέρες μας όπου η αξία του ηλεκτρικού ρεύματος και του φυσικού αερίου έχει εκτοξευθεί τα αποτελέσματα από μία τέτοια στατιστική μελέτη θα είναι εντυπωσιακά. Ειδικά αν γίνουν καταγραφές σε βάθος χρόνου και συγκριθούν ανά έτος.

4.5 Avionics - Marine

4.5.1 Aircraft Transponders ADS-B, ACARS

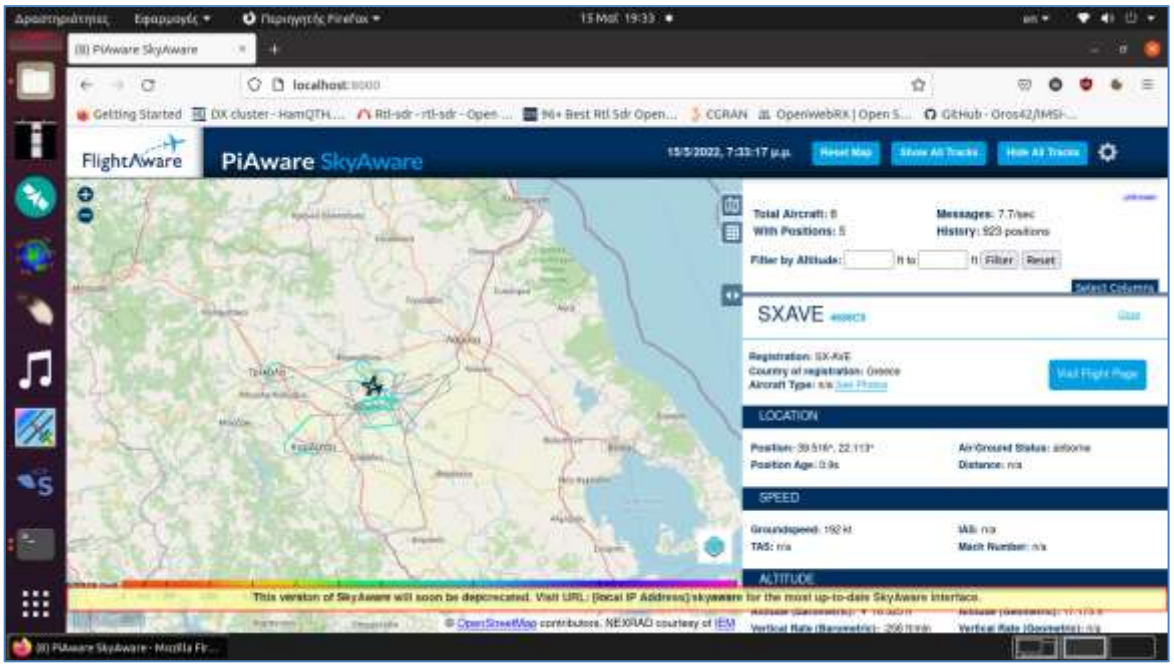
Λαμβάνοντας τα σήματα από Aircraft Transponders ADS-B (Shravan, Rakshit, Sanjana, Priya, & Kumar, 2020) και ACARS είναι εφικτό να προσδιορίσουμε σε πραγματικό χρόνο τα πολιτικά αεροσκάφη που κινούνται από πάνω μας και ανάλογα με την κεραία μας έως και 500 km ακτίνα.

Υπάρχουν ιστοσελίδες στο διαδίκτυο που δείχνουν αυτήν την κίνηση των πολιτικών αεροσκαφών, αλλά το κάνουν με καθυστέρηση 10 λεπτών για λόγους ασφαλείας και δεν συμπεριλαμβάνουν όλα τα αεροσκάφη. Με τα δεδομένα αυτά μπορούμε να εξαιρέσουμε τις συνηθισμένες εμπορικές πτήσεις και να δούμε ειδικές πτήσεις από που ξεκινούν, τι πορεία έχουν και που καταλήγουν.

Εικόνα 36. SDRangel software με λήψη beacon της πολιτικής αεροπορίας

4.5.2 Airport VOR

Το VOR είναι ένα σύγχρονο σύστημα όπου τα αεροσκάφη μπορούν να προσδιορίσουν την γωνία τους ως προς κάποιον ραδιοφάρο. Οι ραδιοφάροι βρίσκονται συνήθως σε αεροδρόμια ή άλλα σημεία ενδιαφέροντος και με τη λήψη τουλάχιστον δύο εξ' αυτών μπορούν να εντοπίσουν την θέση τους. Παλαιότερα τα αεροσκάφη θα έπρεπε να διαθέτουν ένα πολύπλοκο σύστημα ραδιο-γωνιομέτρησης το οποίο απαιτούσε ειδικό χειριστή ραδιο-ναυτίλο για να κάνει τις μετρήσεις. Με το RTL-SDR μπορούμε να κάνουμε λήψη αυτού του σήματος και να προσδιορίσουμε με μεγάλη ακρίβεια την θέση κάποιου υπολογιστή που έχουμε hackάρει και διαθέτει το TV Tuner της Realtek. Έτσι ώστε να αξιοποιήσουμε κατάλληλα τα δεδομένα που θα λάβουμε από αυτόν.



Εικόνα 37. Λήψη από το RTL-SDR μου ερευνητικής πτήσης στον κάμπο της Λάρισας

4.5.3 Marine AIS

Το σύστημα Marine AIS είναι για την θάλασσα ότι είναι για τον αέρα τα Aircraft Transponders ADB-S, ACARS. Η παρακάτω εικόνα είναι από πλοίο το οποίο σταμάτησε να εκπέμπει την θέση του προκειμένου να μην εντοπίζεται η πορεία του. Φυσικά όμως επειδή έχει μεγάλο ενδιαφέρον για το που θα κατευθυνθεί έγινε αντιληπτό μόλις ελλιμενίστηκε και ενημερώθηκε ο διεθνής τύπος για τις κινήσεις του.

Εικόνα 38. Marine AIS Newsfeed

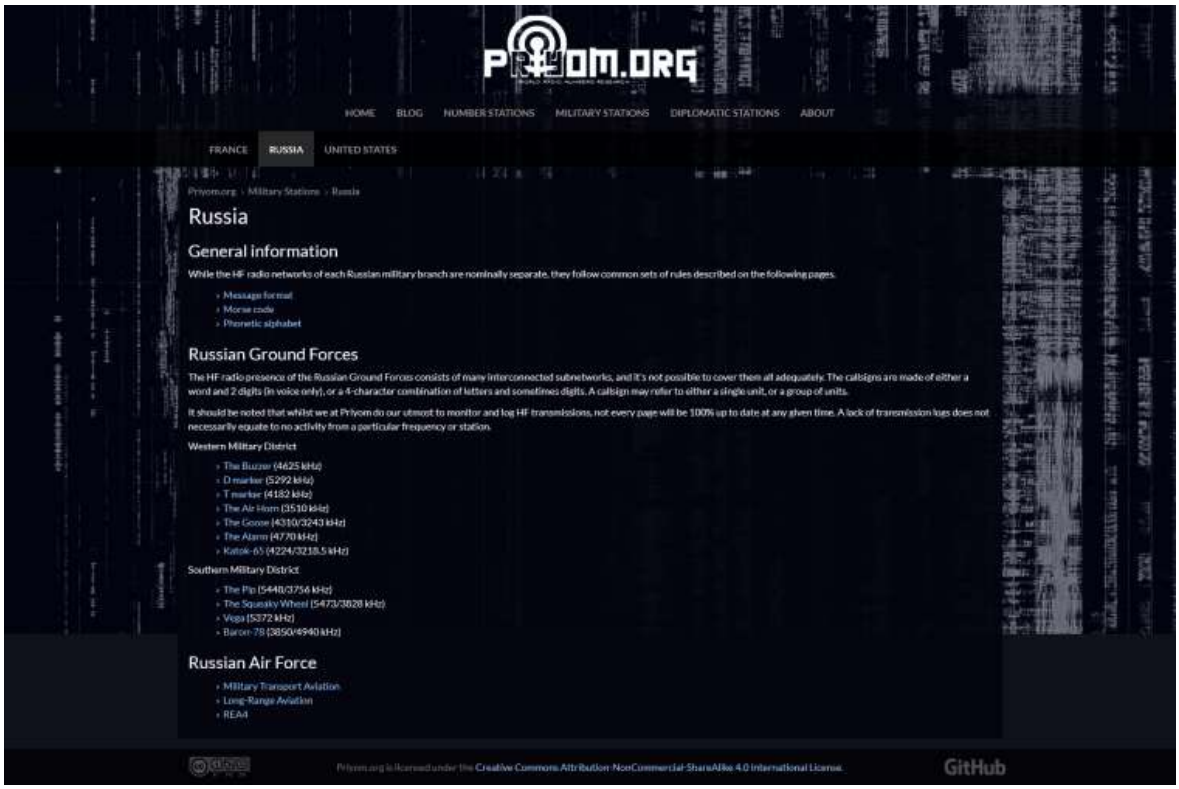
Πηγή: https://liveuamap.com/en/2022/11-july-russian-flag-sormovskiy-48-carrying-3000t-corn-from

4.6 Military coms

4.6.1 Voice channels

Όπως βλέπουμε από τα τελευταία γεγονότα οι επικοινωνίες είναι ζωτικής σημασίας στοιχεία για την διεξαγωγή στρατιωτικών επιχειρήσεων. Παρόλα αυτά όμως λόγο κόστους ή αδυναμία ανανέωσης του εξοπλισμού γίνετε χρήση απλών αναλογικών χωρίς κρυπτογράφηση.

Αυτού του είδους οι επικοινωνίες είναι τελείως ανασφαλείς και βασίζονται κυρίως στη χρήση συνθηματικών λέξεων που δεν είναι δύσκολο να βρεθεί η ερμηνεία τους. Υπάρχει ένα χαρακτηριστικό βίντεο με υπότιτλους στους New York Times (https://www.nytimes.com/video/world/europe/100000008266864/russia-army-radio-makariv.html



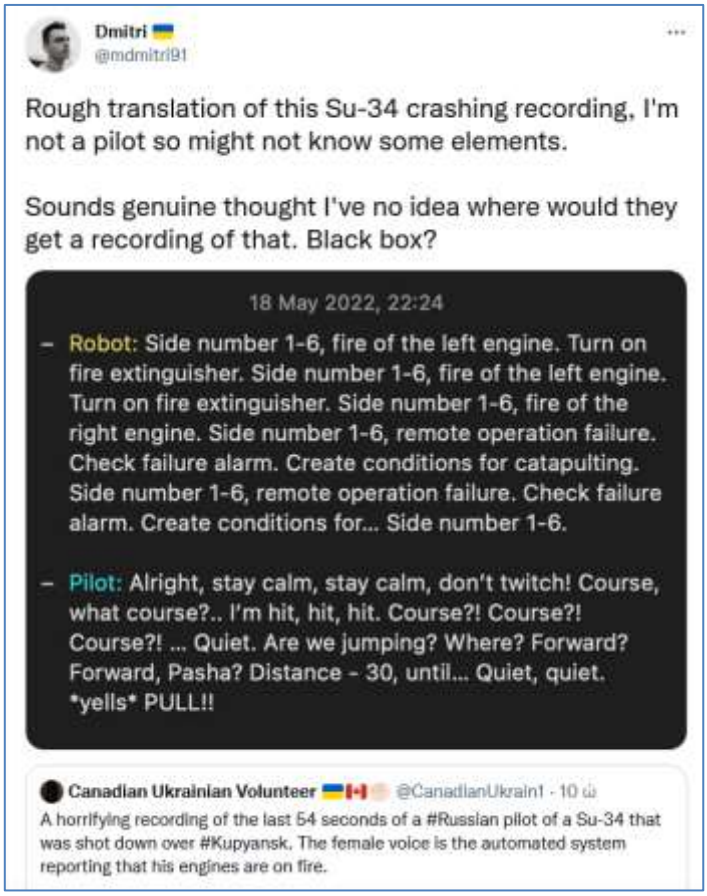
Εικόνα 39. Πληροφορίες για τις αναλογικές συχνότητες της Ρωσίας

Πηγή: https://priyom.org

4.6.2 HF Data channels

Οι συγκεκριμένες επικοινωνίες είναι με υψηλή κρυπτογράφηση αλλά με τη χρήση του RTL-SDR μπορούμε να εντοπίσουμε την θέση τους, όπου είναι εξίσου σημαντικό πλεονέκτημα, ειδικά σε περίοδο πολέμου. Ακόμα μπορούν να εξαχθούν συμπεράσματα παρακολουθώντας την συχνότητα των εκπεμπόμενων μηνυμάτων και παρακολουθώντας τα γεγονότα μετά από κάθε μήνυμα. Οι στρατιωτικές επικοινωνίες σε περιπτώσεις έκτακτης ανάγκης μπορεί να μην είναι κρυπτογραφημένες, έτσι ώστε να υπάρχει σχετική ενημέρωση των ομάδων διάσωσης.

Μπορούν να βρεθούν μοτίβα γεγονότων όπως μετά από κάποια επικοινωνία να εξαπολύετε μια πυραυλική επίθεση, οπότε μπορούν να παρθούν τα κατάλληλα αντίμετρα για την ανάσχεση της επίθεσης (https://www.sigidwiki.com/wiki/STANAG_4285)



Εικόνα 40. Μετάφραση ηχητικού αποσπάσματος που καταγράφηκε από HF Data Channel μέσω RTL-SDR
(Αφορά την κατάρριψη ρωσικού πολεμικού αεροσκάφους SU-34 πάνω από την περιοχή Kupyansk της Ουκρανίας στις 18/5//2022)

Πηγή https://twitter.com/wartranslated/status/1527037737303433223

4.7 Δίκτυα κινητής τηλεφωνίας 2ης γενιάς (GSM)

Σε ένα δίκτυο κινητής τηλεφωνίας 2ης γενιάς όπως το Global System for Mobile Communications (GSM) υπάρχουν οι παρακάτω μονάδες :

- Κινητός Σταθμός, ο χρήστης του δικτύου με την συσκευή του κινητού τηλεφώνου.
- Σταθμός βάσης. Σταθερές κεραίες που χρησιμοποιούνται για την εξυπηρέτηση της κινητής τηλεφωνίας. Αναφέρονται ως σταθμοί βάσης κυψελωτών επικοινωνιών ή πύργοι μετάδοσης κινητής τηλεφωνίας.

Για να επιτευχθεί η επικοινωνία των παραπάνω μονάδων γίνεται χρήση δυο ομάδων συχνοτήτων.

- Uplink για την ζεύξη του κινητού σταθμού με τον σταθμό βάσης.
- Downlink για την ζεύξη από τον σταθμό βάσης στο κινητό τηλέφωνο.

Το σύστημα λέγεται κυψελωτό, γιατί οι σταθμοί βάσης χωρίζονται σε γεωγραφικές περιοχές και δημιουργούν ένα πλέγμα που μοιάζει με κυψέλη. Κάθε κινητός σταθμός εντοπίζει τον πλησιέστερο σταθμό βάσης και επικοινωνεί μαζί του. Κατά την μετακίνηση του κινητού σταθμού είναι δυνατό να αλλάξει ο σταθμός βάσεως που επικοινωνεί με κάποιον άλλο που παρέχει καλύτερο σήμα. Επομένως αν και τα περισσότερα σχήματα παρουσιάζουν το κυψελωτό σχήμα ως αυστηρή εμβέλεια των σταθμών βάσεως, στην πραγματικότητα ένα κινητός σταθμός λαμβάνει αρκετούς σταθμούς βάσης ταυτόχρονα αλλά κλειδώνει σε αυτόν με την καλύτερη ποιότητα σήματος.Για το διαχωρισμό και την ταυτοποίηση των κινητών και των σταθμών βάσης, έχουν δοθεί από την ITU οι παρακάτω κωδικοί ταυτοποίησης :

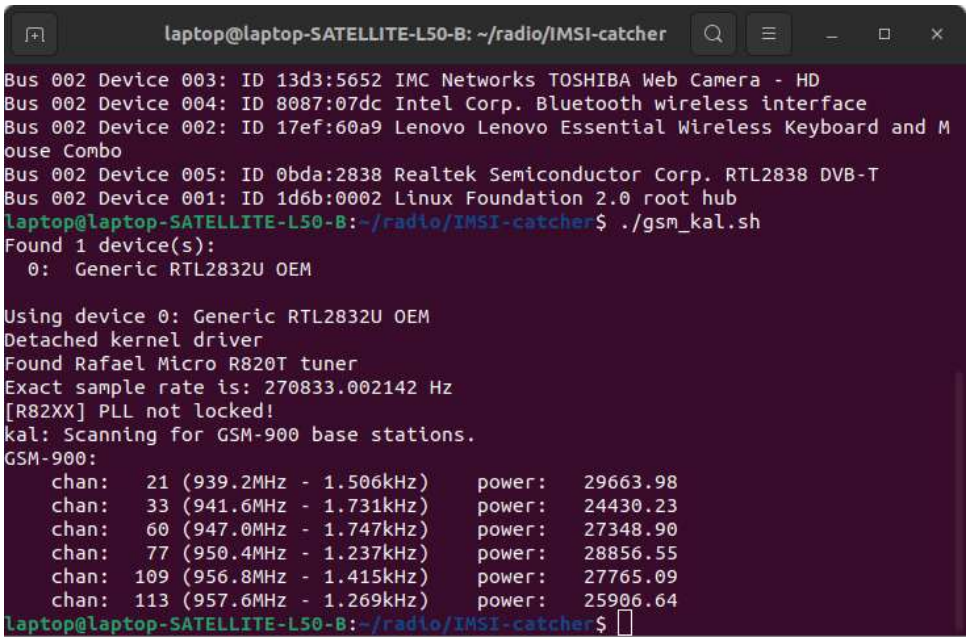
- Mobile Country Code (MCC) : Κωδικός 3 ψηφίων που χαρακτηρίζει την χώρα. Για την Ελλάδα είναι ο 202
- Mobile Network Code (MNC) : Κωδικός 2 ψηφίων που χαρακτηρίζει τον πάροχο του τηλεπικοινωνιακού δικτύου.
- Cell ID : Αναγνωριστικό εκπομπής κυψέλης

Οι κινητοί σταθμοί έχουν, μεταξύ άλλων, στην κάρτα SIM τους παρακάτω κωδικούς :

- International Mobile Subscriber Identity (IMSI) : Ένας αριθμός 15 ψηφίων που χαρακτηρίζει μοναδικά τον συνδρομητή.

Με την εντολή **`kal -s 900 -e 27`** μπορούμε να δούμε όλες τις κυψέλες της περιοχής.

Με τη χρήση του RTL-SDR είναι δυνατό να δούμε με το spectrum-analyzer και να εντοπίσουμε στα 930MHz το downlink σήμα ενός σταθμού βάσεως.

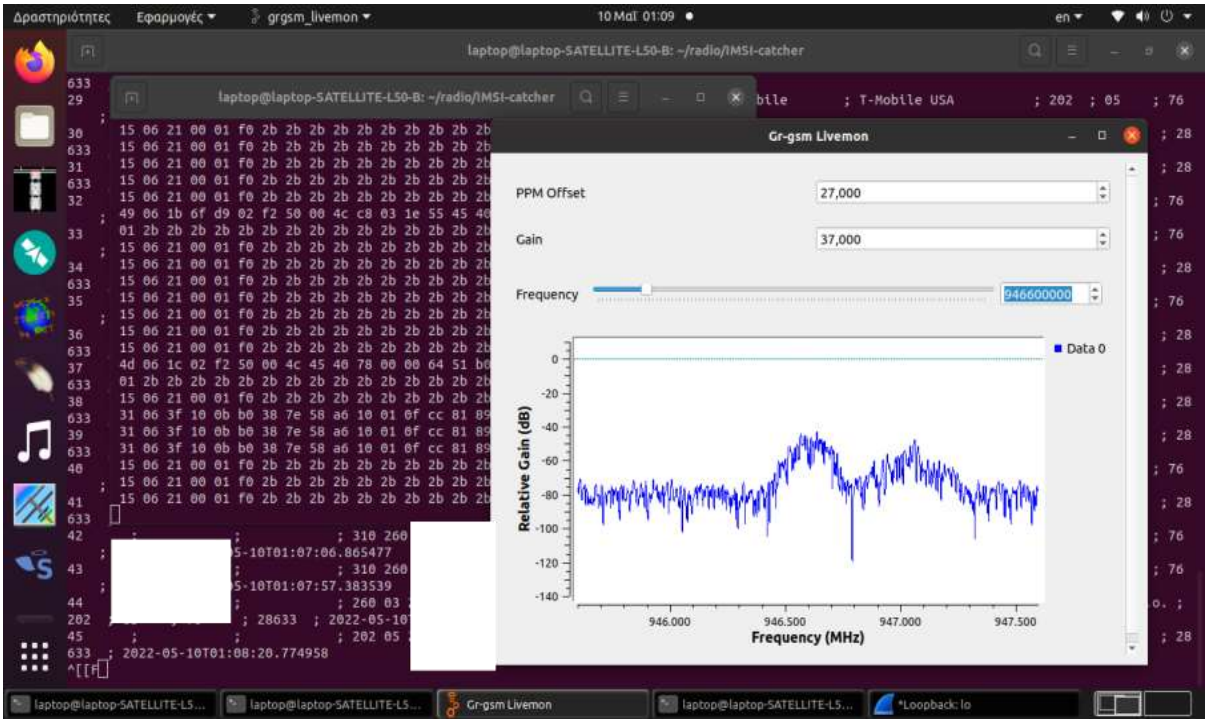


Εικόνα 41. Λήψη 6 κυψελών στην περιοχή μου

Αφού συντονιστούμε σε αυτό με τη χρήση των εργαλείων λήψης και αποδιαμόρφωσης του σήματος μπορούμε να εξάγουμε πληροφορίες για τα ποια κινητά τηλέφωνα είναι συνδεδεμένα σε αυτό τον σταθμό βάσεως και να δούμε όλα τα δεδομένα που ο σταθμός στέλνει σε αυτά.

Κάνοντας pipe τα δεδομένα που λαμβάνουμε στο Wireshark με το GSMTAP (Zecke, 2016) , μπορούμε να αναλύσουμε το πρωτόκολλο και να αναζητήσουμε πληροφορίες (Bulychev, Goncharov, & Babalova, 2018).

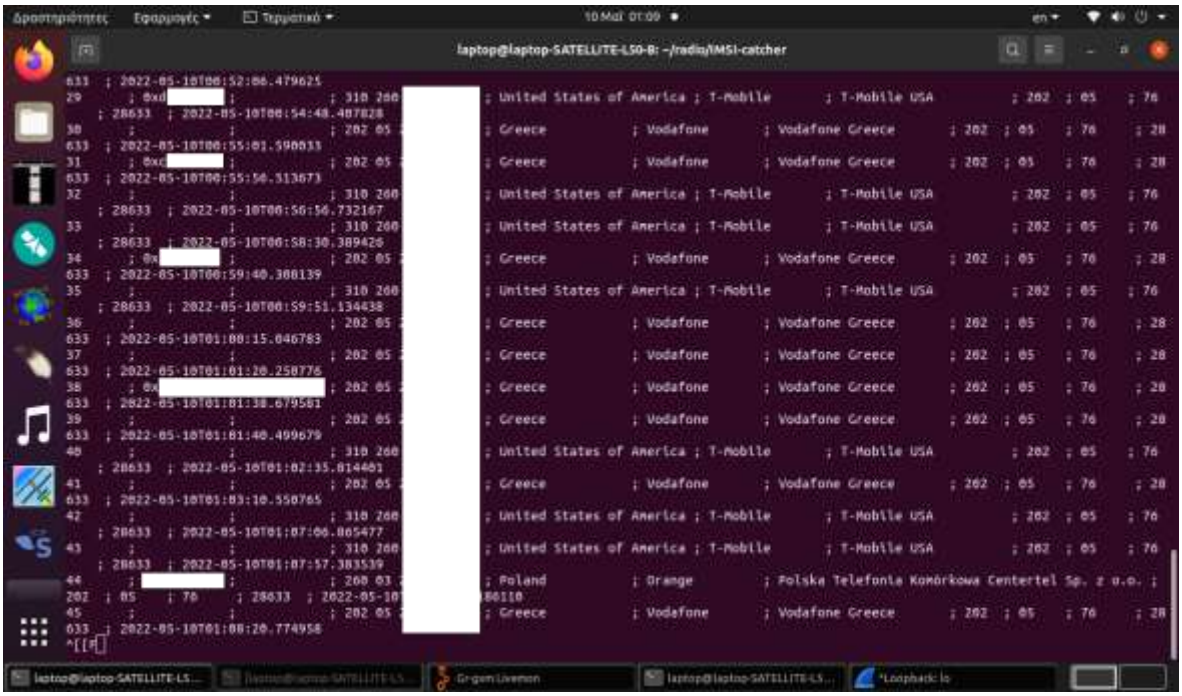
Εκτελούμε την εντολή **`sudo python3 ./simple_IMSI-catcher.py -s`** για να ξεκινήσουμε τη λήψη δεδομένων ψάχνοντας να βρούμε το downlink μιας κυψέλης.



Εικόνα 42. Συντονισμός σε κυψέλη και λήψη δεδομένων

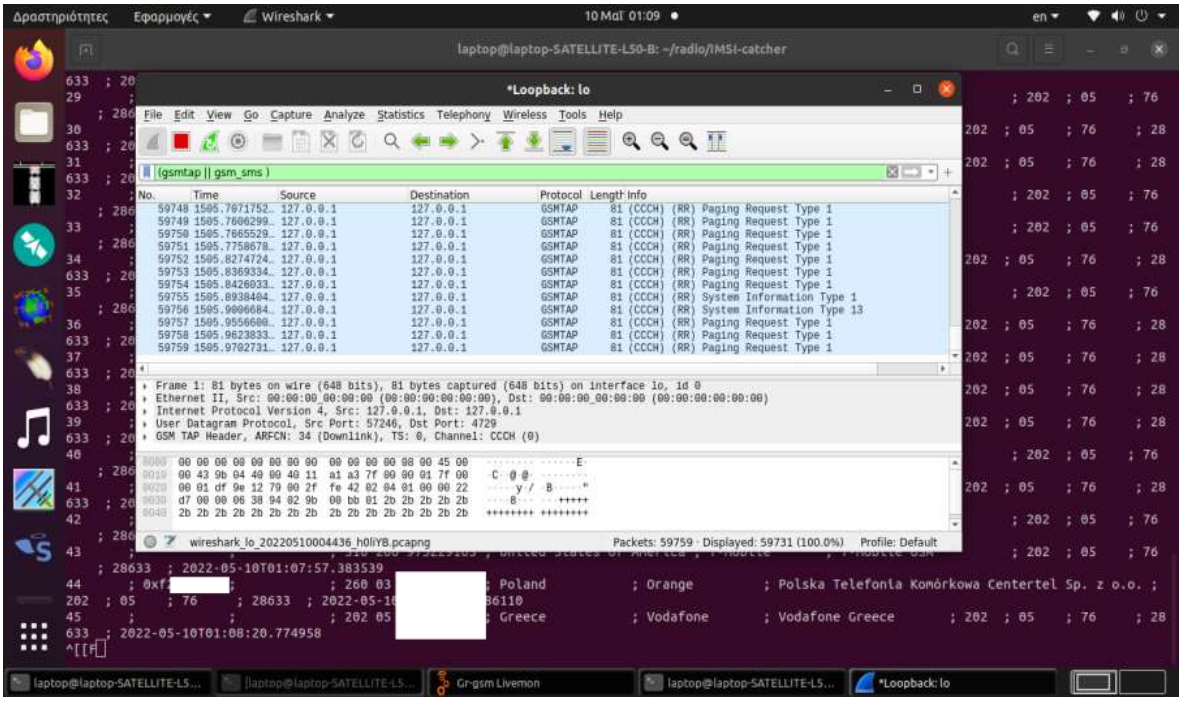
Αφού εντοπίσουμε κάποιο καλό σήμα στον φασματογράφο, περιμένουμε να αρχίσει η ροή των δεδομένων στον IMSI-catcher.

Μετά τρέχουμε την εντολή: **`grgsm_livemon`**
όπου τα δεδομένα αποκωδικοποιούνται και δημιουργεί μια UDP σύνδεση κατάλληλη για χρήση στο Wireshark.



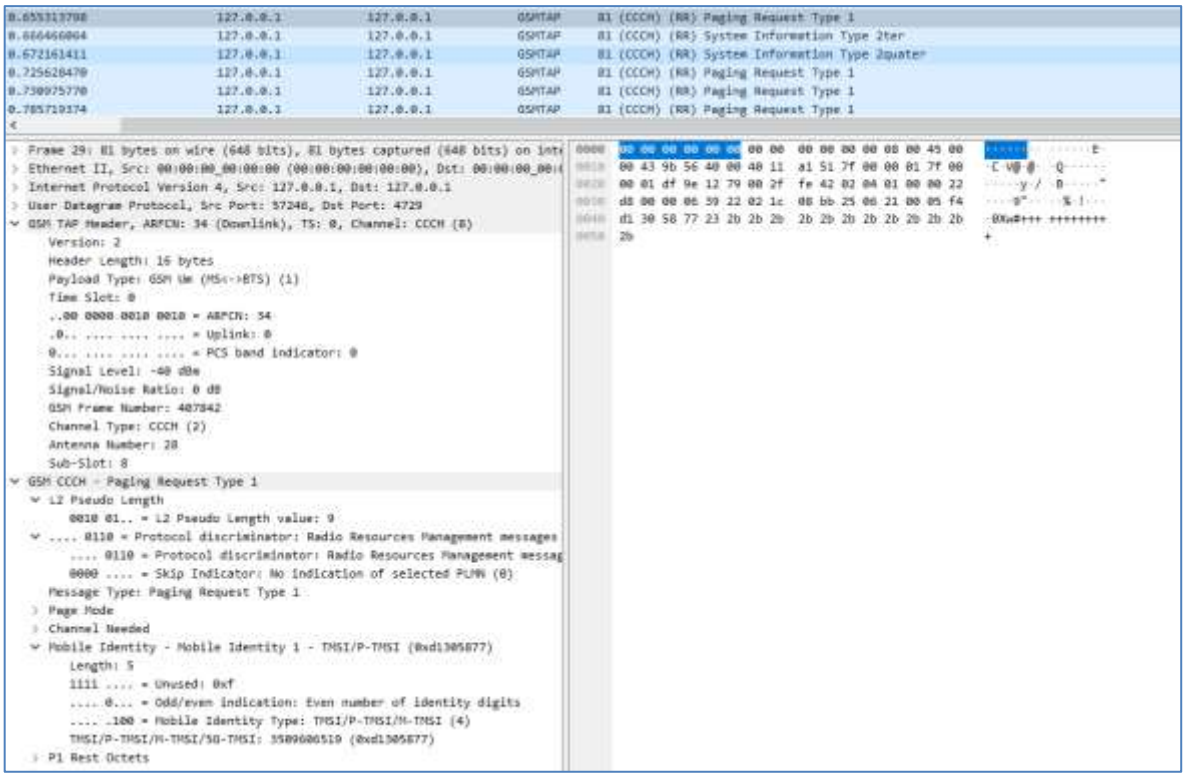
Εικόνα 43. Εμφάνιση κινητών τηλεφώνων που επικοινωνούν με την κυψέλη

Με το Wireshark μπορούμε να επεξεργαστούμε και να φιλτράρουμε τα δεδομένα σε μεγάλο βαθμό. Μπορούμε να αναλύσουμε πολλές ενδιαφέρουσες πληροφορίες από την κίνηση του δικτύου.

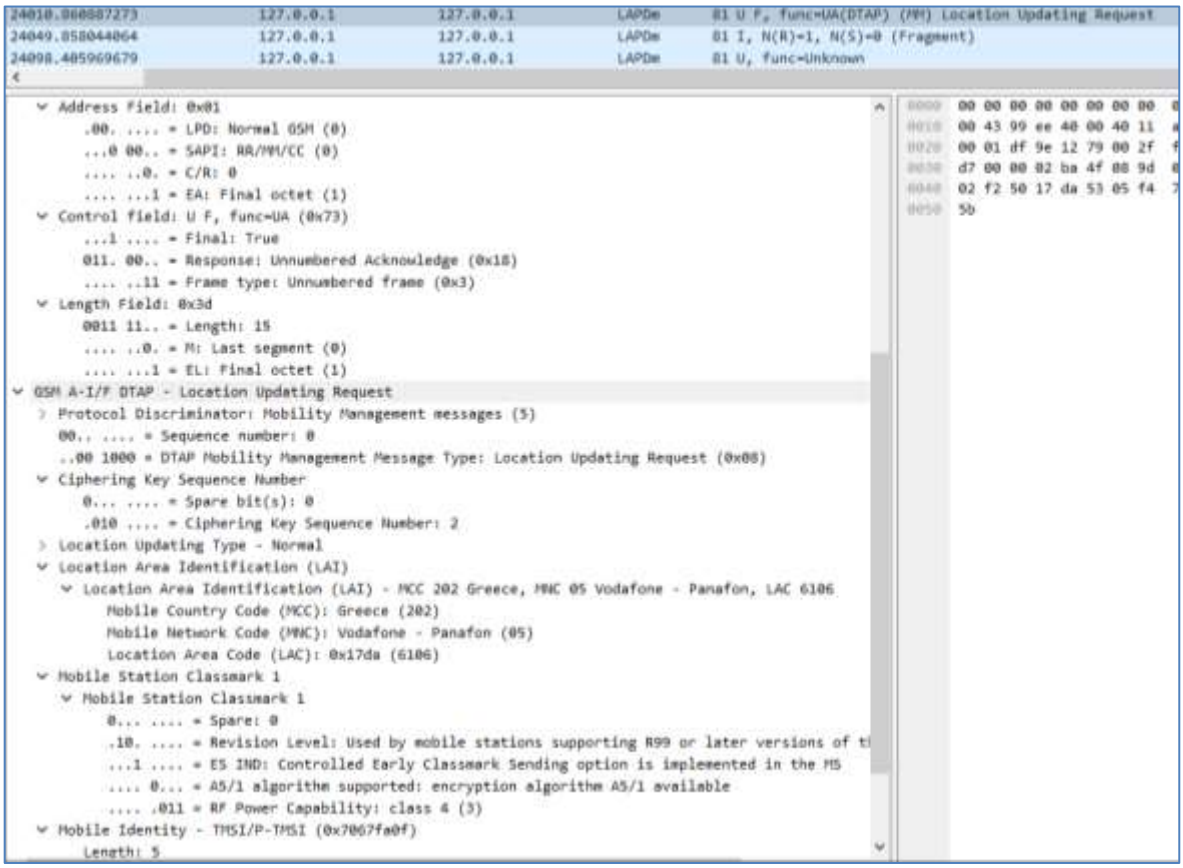


Εικόνα 44. Αποστολή των δεδομένων στο Wireshark για επεξεργασία

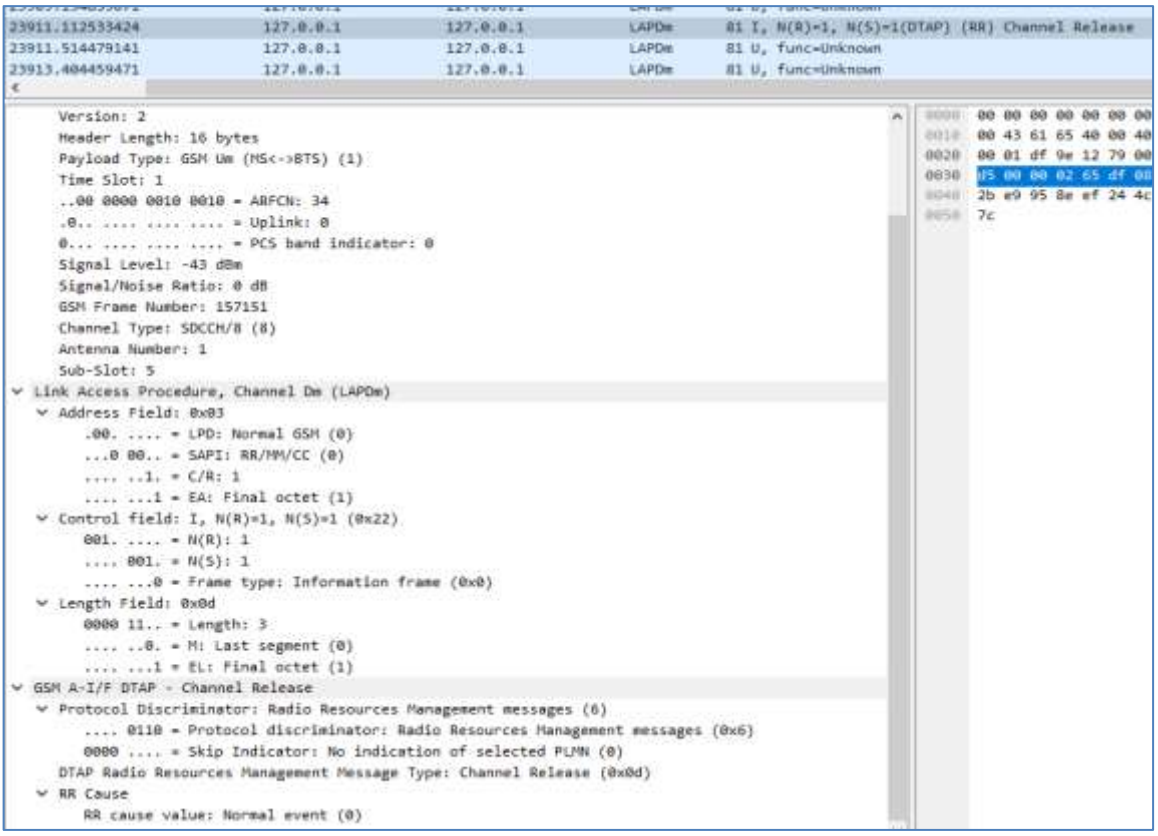
Μπορούμε να δούμε πακέτα System Information Type που ανάλογα με τον τύπο δείχνουν διάφορες χρήσιμες πληροφορίες.



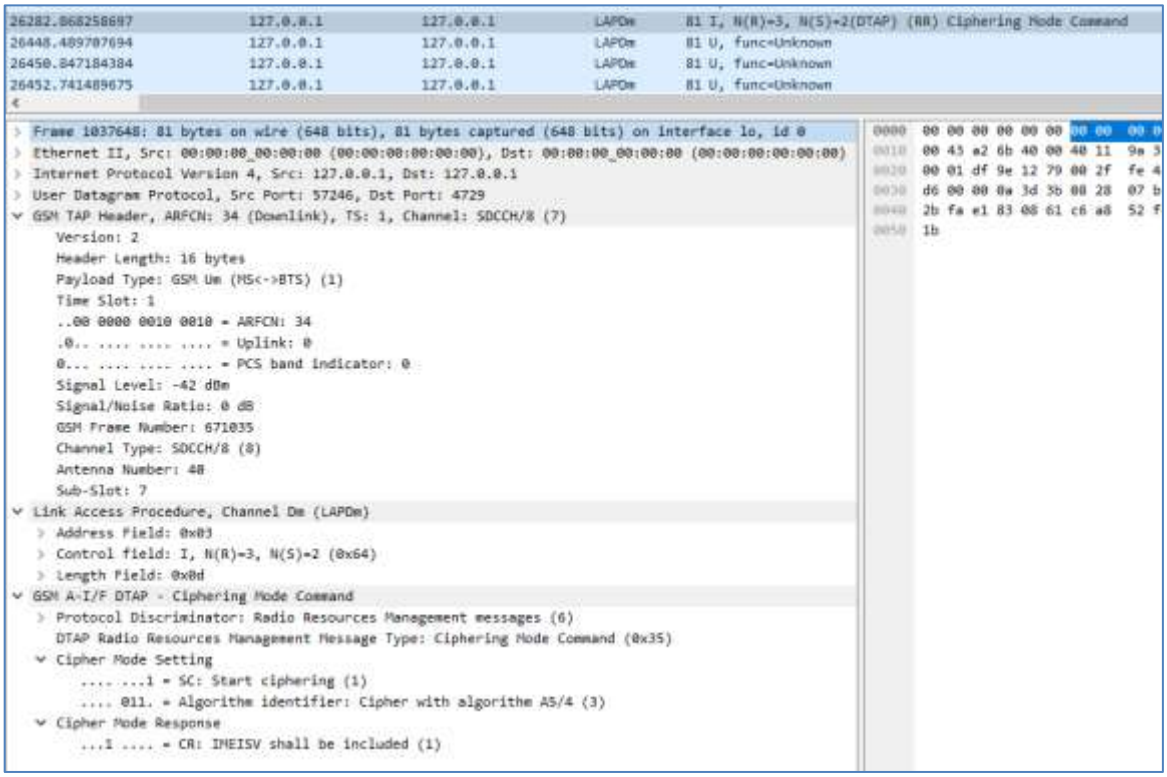
Εικόνα 45. Απόδοση TMSI σε συσκευή κινητού που εισήλθε στην κυψέλη



Εικόνα 46. Ενημέρωση θέσης της κυψέλης και αποστολή του LAI



Εικόνα 47. Αποδέσμευση καναλιού



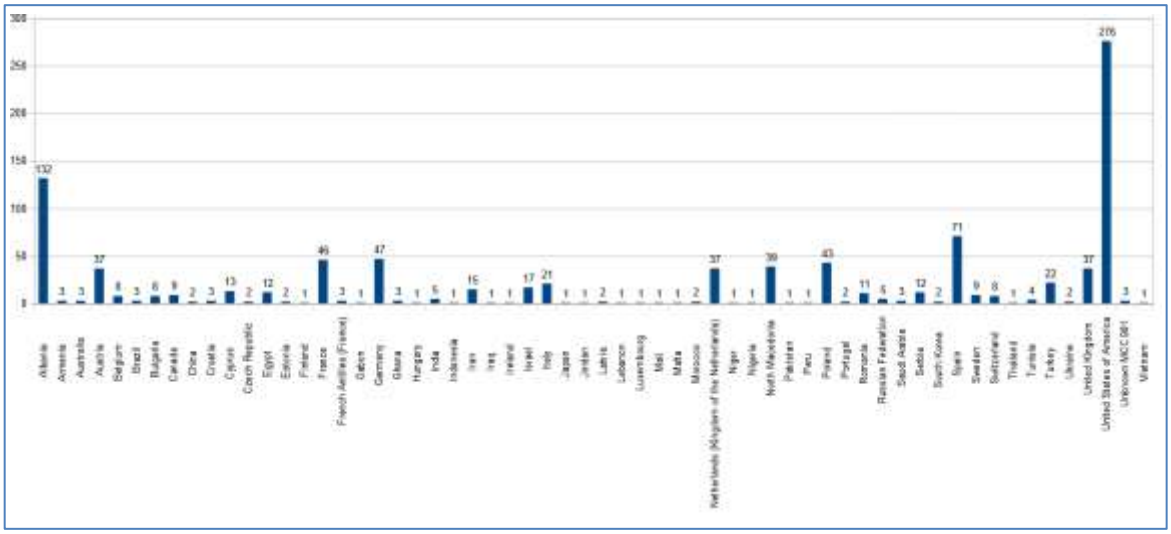
Εικόνα 48. Μετάβαση σε κρυπτογραφημένη επικοινωνία με τον αλγόριθμο A5/4

Με τα δεδομένα που θα λάβουμε μπορούμε να βρούμε στοιχεία για την κυψέλη και την κεραία από διάφορες ανοιχτές βάσεις δεδομένων. Όπως η Ενημερωτική Πύλη

Κατασκευών Κεραιών της Εθνικής Επιτροπής Τηλεπικοινωνιών & Ταχυδρομείων https://keraies.eett.gr/ και το portal της Ελληνικής Επιτροπής Ατομικής Ενέργειας https://eeae.gr/

Εικόνα 49. Καταγραφή θέσεων κεραιώναπό τον ιστότοπο keraies.eett.gr

Αλλά ακόμα να κάνουμε και δικά μας στατιστικά διαγράμματα σχετικά με τη συγκέντρωση των συνδρομητών πέραν της Ελλάδος. Ένα πολύ ενδιαφέρον στατιστικό γιατί μπορούμε να δούμε την μετακίνηση και να εποπτεύσουμε τον πληθυσμό. Πράγμα που έχει συμβεί ακόμα και για στρατιωτική χρήση.



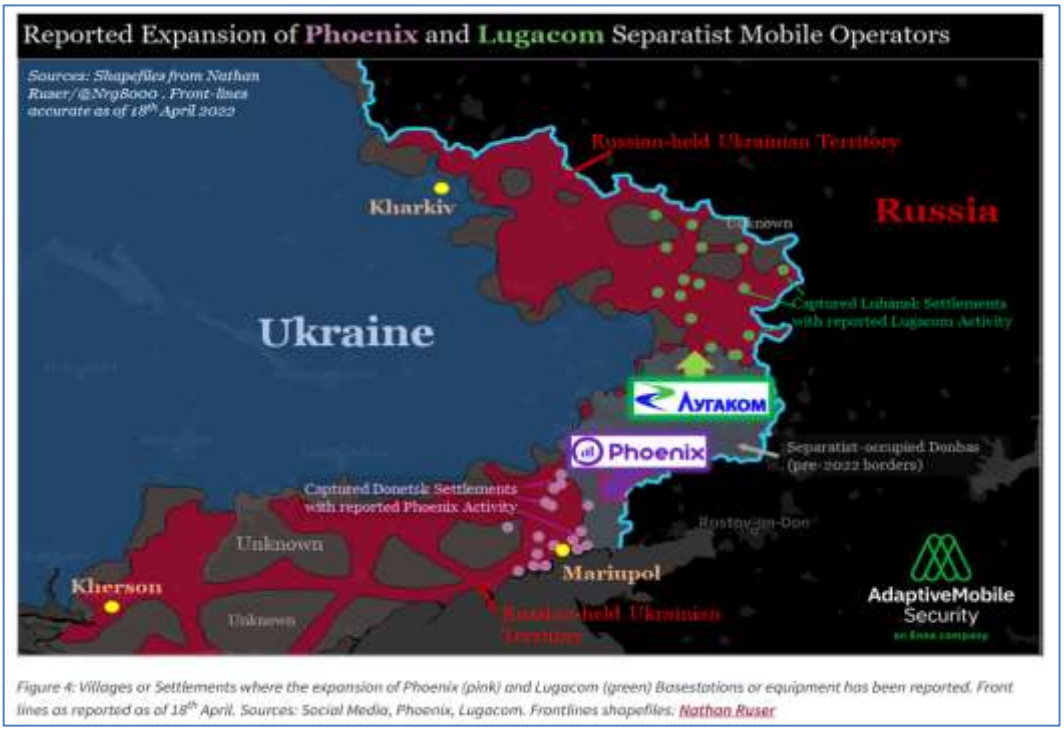
Εικόνα 50. Στατιστικό διάγραμμα συνδρομητών της κυψέλης που έλαβα με το RTL-SDR.

Εικόνα 51. Μέτρηση πυκνότητας ακτινοβολίας από τον ιστότοπο eeae.gr

Μπορούμε να δούμε στους παρακάτω χάρτες πως κινήθηκαν οι συνδρομητές πριν και μετά την έναρξη του πολέμου στην Ουκρανία. Γίνεται αμέσως αντιληπτό από που προέρχονται οι στρατιωτικές δυνάμεις, αλλά ακόμα είναι εμφανείς οι κινήσεις τους και το μέγεθός τους. Δεδομένα που έχουν τεράστια στρατιωτική αξία.

Εικόνα 52. Κανονική κατανομή συνδρομητών στην περιοχή της Ουκρανίας (πριν από τη Ρωσική εισβολή)

Πηγή: https://blog.adaptivemobile.com/the-mobile-network-battlefield-in-ukraine-part-3



Εικόνα 53. Μετακίνηση των συνδρομητών κατά τη Ρωσική εισβολή στην Ουκρανία

Πηγή: https://blog.adaptivemobile.com/the-mobile-network-battlefield-in-ukraine-part-3

Επιπλέον μπορούν να εντοπιστούν συγκεντρώσεις από συνδρομητές που λειτουργούν για διάφορους σκοπούς. Για παράδειγμα SIM-farms όπου υπολογιστές έχουν ρυθμιστεί να ελέγχουν εκατοντάδες κάρτες SIM έτσι ώστε να τις κάνουν να φαίνονται ως ξεχωριστούς συνδρομητές και ως ξεχωριστούς χρήστες στα διάφορα κοινωνικά δίκτυα. Μια ασυνήθιστη σταθερή βάση από συνδρομητές κινεί υποψίες, διότι το κινητό τηλέφωνο θα πρέπει να εναλλάσσει θέση και να μεταβαίνει σε διαφορετικές κυψέλες.

Εικόνα 54. Sim Farm υλικό που διαχειρίζεται εκατοντάδες κάρτες SIM

Πηγή: https://www.bleepingcomputer.com/news/security/ukraine-dismantles-5-disinformation-bot-farms-seizes-10-000-sim-cards/

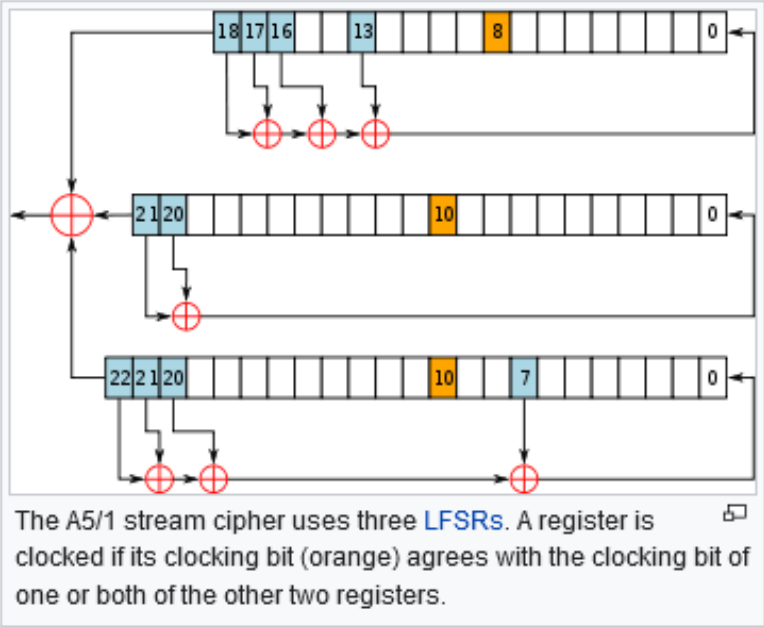
Στις παραπάνω φωτογραφίες αν δείτε προσεκτικά αυτό που φαίνεται ως καρτέλα αρχειοθέτησης, είναι μια πλακέτα που δέχεται κάρτα SIM και λειτουργεί ως κινητό τηλέφωνο. Διακρίνεται η κεραία της κάθε πλακέτας αν κοιτάξουμε με προσοχή. Κάθε «συρτάρι» περιέχει περίπου 60 κάρτες SIM.

Εικόνα 55. Λεπτομέρεια της παραπάνω εικόνας που διακρίνονται οι κεραίες

Εικόνα 56. Πολλαπλοί σταθμοί κινητής τηλεφωνίας.

Πηγή: υπηρεσία ασφαλείας της Ουκρανίας SSU

Τα δεδομένα της κίνησης του δικτύου GSM 900 είναι μη κρυπτογραφημένα, επομένως είναι τελείως ευάλωτα σε επιθέσεις του τύπου GSM Stingray ακόμα και παθητικού τύπου όπως γίνεται με το RTL-SDR. Τα δεδομένα των κλήσεων και των SMS είναι κρυπτογραφημένα με τους αλγορίθμους A5.



Εικόνα 57. Λειτουργία αλγορίθμου κρυπτογράφησης A5/1

Πηγή: https://en.wikipedia.org/wiki/A5/1

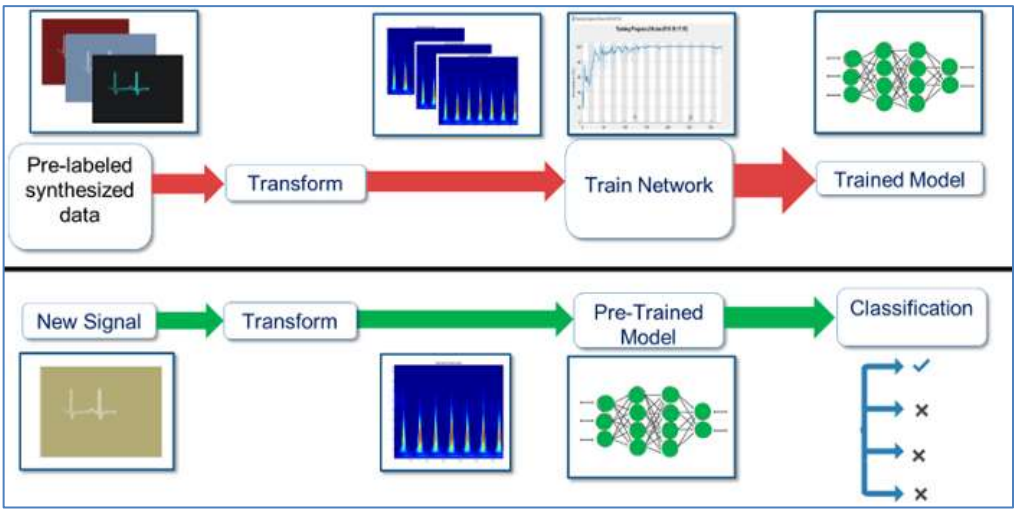
Αρκετοί όμως από τους αλγόριθμους κρυπτογράφησης έχουν ασθενή κρυπτογράφηση για τα σημερινά δεδομένα, ή έχουν ήδη σπάσει (https://en.wikipedia.org/wiki/A5/1)

Με τη χρήση εργαλείων όπως το Pytacle μπορούν να επεξεργαστούν και τα δεδομένα φωνής και μηνυμάτων (https://insinuator.net/2012/10/pytacle-alpha1-released). Τα κρυπτογραφημένα δεδομένα φωνής και SMS είναι δυνατό να αποκωδικοποιηθούν αν βρούμε το κλειδί κρυπτογράφηση Kc είτε με σπάσιμο κάποιου ασθενή αλγορίθμου είτε με κάποιο malware να εξάγουμε από την συσκευή το Ki που θέλουμε να παρακολουθήσουμε.

- Ki είναι ένα 128-bit Individual Subscriber Authentication κλειδί το οποίο χρησιμοποιείτε ως μυστικό κλειδί μεταξύ του κινητού σταθμού και του Home Location Register του παρόχου, το κλειδί αυτό βρίσκετε στην κάρτα SIM.
- Kc είναι ένα 64-bit κλειδί κρυπτογράφησης της ασύρματης επικοινωνίας. Kc το κλειδί δημιουργείτε από τον κινητό σταθμό με τυχαία δεδομένα που παρέχονται από το δίκτυο GSM και από το Ki της κάρτας SIM, με τη χρήση του αλγορίθμου A8.

4.8 Ηλεκτρομαγνητική ταυτότητα συσκευών

Κάθε συσκευή έχει εσωτερικά της κυκλώματα τα οποία δημιουργούν διάφορες ταλαντώσεις. Μπορεί να έχει κάποιον κρύσταλλο για την λειτουργία κάποιου CPU ή κάποια ταλάντωση για να κάνει δειγματοληψία κάποιο σήμα ή κάποια ταλάντωση για την έξοδο κάποιου σήματος.



Εικόνα 58. Χρήση RTL-SDR, RF Fingerprinting και Deep Learning

Πηγή: https://www.rtl-sdr.com/using-an-rtl-sdr-rf-fingerprinting-and-deep-learning-to-authenticate-rf-devices/

Με τη χρήση του RTL-SDR μπορούμε να πάρουμε δείγματα δεδομένων και αφού τα αναλύσουμε μπορούμε να κάνουμε το ηλεκτρομαγνητικό αποτύπωμα (fingerprinting) της συσκευής. Το αποτύπωμα αυτό μπορεί να χρησιμοποιηθεί για παρακολούθηση ή ακόμα και για στρατιωτικές εφαρμογές με τους πυραύλους τύπου Anti-Radiation (https://www.thedrive.com/the-war-zone/41798/first-live-fire-test-of-navys-new-long-range-anti-radiation-missile-was-a-success)

4.8.1 Local Oscillator detector

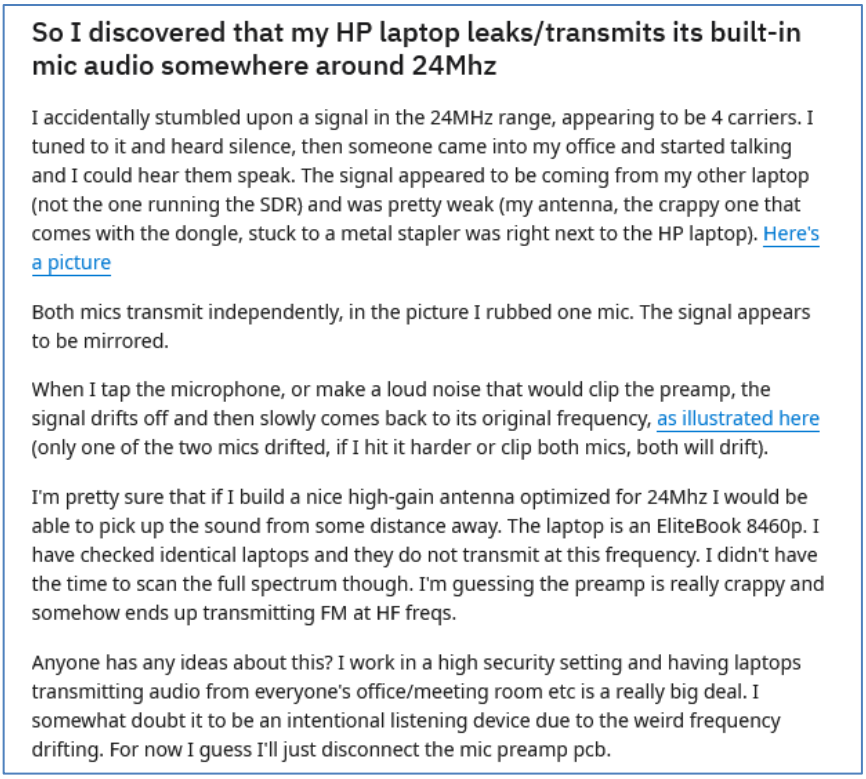
Παραδείγματα τέτοιων συσκευών που ανιχνεύουν τις συχνότητες εσωτερικής λειτουργίας υπάρχουν από πολύ παλιά. Στο δεύτερο παγκόσμιο πόλεμο χρησιμοποιήθηκε συσκευή η οποία άκουγε τον εσωτερικό ταλαντωτή που είχαν τα ραδιόφωνα για να λειτουργήσουν και τα εντόπιζαν. Δεν εντόπιζαν τον ραδιοφωνικό πομπό, αλλά τους πολίτες που είχαν κρυφά έναν ραδιοφωνικό δέκτη, από την εσωτερική ταλάντωση που έκαναν τα εξαρτήματα του ραδιοφώνου. (https://www.cryptomuseum.com/df/bc792a/index.htm)

4.8.2 Sound card leakage

Στις περισσότερες ηλεκτρονικές συσκευές που χρησιμοποιούμε σήμερα, κινητό τηλέφωνο, ηλεκτρονικός υπολογιστής, υπάρχει κάποιο ψηφιακό κύκλωμα κάρτας ήχου, το οποίο έχει κάποιον ταλαντωτή για να δουλέψει ο analog to digital converter (ADC) και έχει και κάποιο μικρόφωνο επάνω του. Το μικρόφωνο ακόμα και όταν δεν το χρησιμοποιούμε είναι σε λειτουργία με το κύκλωμα ενίσχυσης και το κύκλωμα ADC, αλλά είναι σε αποκοπή από το λογισμικό που τρέχει στην CPU, της συσκευής.

Παραμένει όμως σε λειτουργία και μπορούμε να το ακούσουμε ψάχνοντας την συχνότητα λειτουργίας του. Ο εσωτερικός ταλαντωτής δεν δίνει μεγάλη εμβέλεια αλλά

με αρκετή ενίσχυση και μια κατάλληλη κεραία για την συχνότητα, μπορούμε να το ακούσουμε από μερικά δωμάτια πιο πέρα.



So I discovered that my HP laptop leaks/transmits its built-in mic audio somewhere around 24Mhz

I accidentally stumbled upon a signal in the 24MHz range, appearing to be 4 carriers. I tuned to it and heard silence, then someone came into my office and started talking and I could hear them speak. The signal appeared to be coming from my other laptop (not the one running the SDR) and was pretty weak (my antenna, the crappy one that comes with the dongle, stuck to a metal stapler was right next to the HP laptop). Here's a picture

Both mics transmit independently, in the picture I rubbed one mic. The signal appears to be mirrored.

When I tap the microphone, or make a loud noise that would clip the preamp, the signal drifts off and then slowly comes back to its original frequency, as illustrated here (only one of the two mics drifted, if I hit it harder or clip both mics, both will drift).

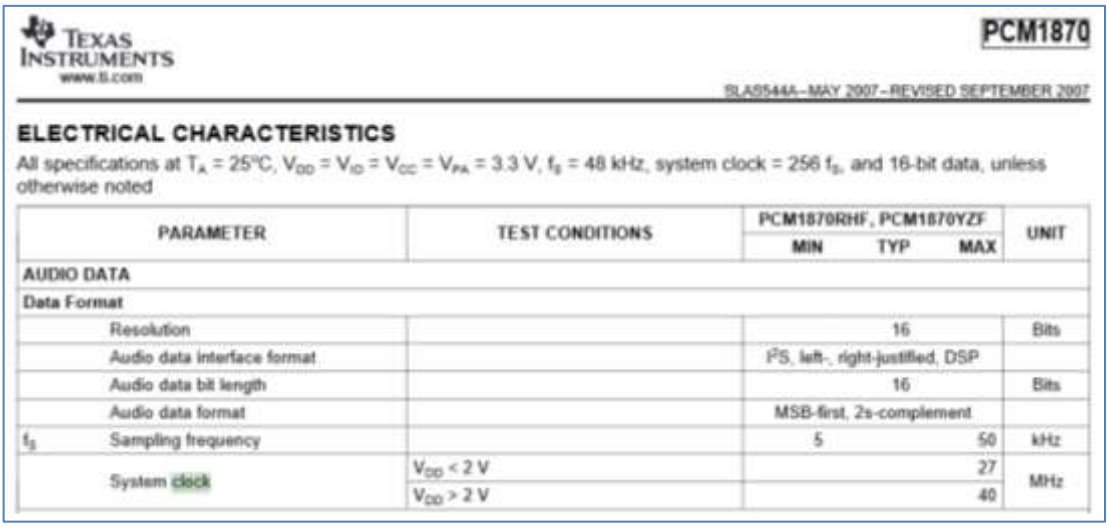
I'm pretty sure that if I build a nice high-gain antenna optimized for 24Mhz I would be able to pick up the sound from some distance away. The laptop is an EliteBook 8460p. I have checked identical laptops and they do not transmit at this frequency. I didn't have the time to scan the full spectrum though. I'm guessing the preamp is really crappy and somehow ends up transmitting FM at HF freqs.

Anyone has any ideas about this? I work in a high security setting and having laptops transmitting audio from everyone's office/meeting room etc is a really big deal. I somewhat doubt it to be an intentional listening device due to the weird frequency drifting. For now I guess I'll just disconnect the mic preamp pcb.

Εικόνα 59. Τυχαία ανακάλυψη της εκπομπής της κάρτας ήχου

Πηγή: https://www.reddit.com/r/RTLSDR/comments/1le3if/so_i_discovered_that_my_hp_laptop_leakstransmits/

Αν δούμε ένα από τα βασικά εξαρτήματα που χρησιμοποιεί η κάρτα ήχου το ADC PCM1870 (Texas Instruments, 2007) χρησιμοποιεί την συχνότητα αυτή για την λειτουργία του. Αν η τροφοδοσία του κυκλώματος είναι κάτω από 2 Volt η συχνότητα λειτουργίας είναι στα 27MHz, διαφορετικά είναι στα 40MHz. Αυτή η πληροφορία μας βοηθάει αρκετά, γιατί περιορίζει πάρα πολύ την έρευνα στο ραδιοφάσμα.



TEXAS INSTRUMENTS
www.ti.com

PCM1870

SLAS544A–MAY 2007–REVISED SEPTEMBER 2007

ELECTRICAL CHARACTERISTICS

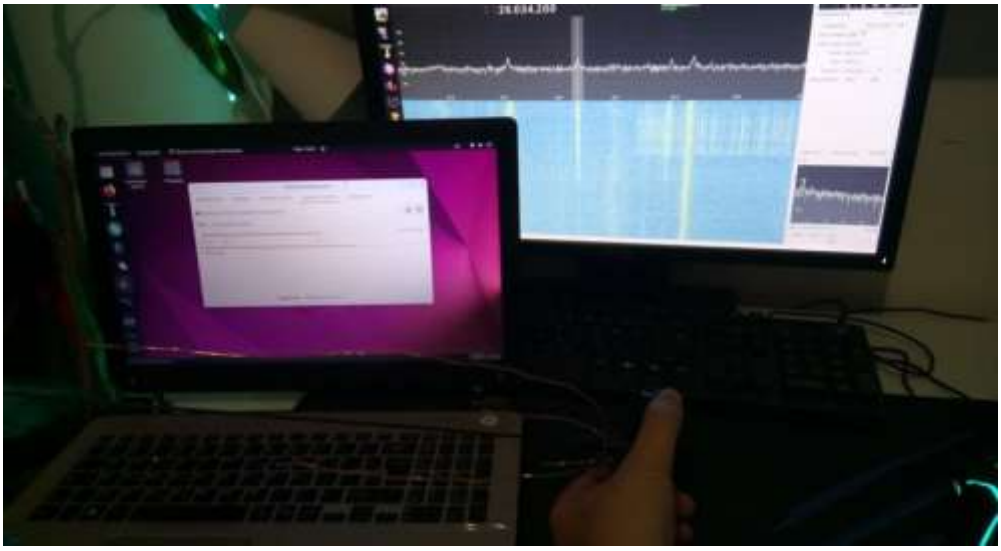
All specifications at T_A = 25°C, V_{DD} = V_{IO} = V_{CC} = V_{PA} = 3.3 V, f_s = 48 kHz, system clock = 256 f_s, and 16-bit data, unless otherwise noted

PARAMETER		TEST CONDITIONS	PCM1870RHF, PCM1870YZF			UNIT
			MIN	TYP	MAX	
AUDIO DATA						
Data Format						
	Resolution			16		Bits
	Audio data interface format			I²S, left-, right-justified, DSP		
	Audio data bit length			16		Bits
	Audio data format			MSB-first, 2s-complement		
f_s	Sampling frequency		5		50	kHz
	System clock	V_{DD} < 2 V			27	MHz
		V_{DD} > 2 V			40	

Εικόνα 60. Τεχνικά χαρακτηριστικά του ολοκληρωμένου PCM1870 της Texas Intruments

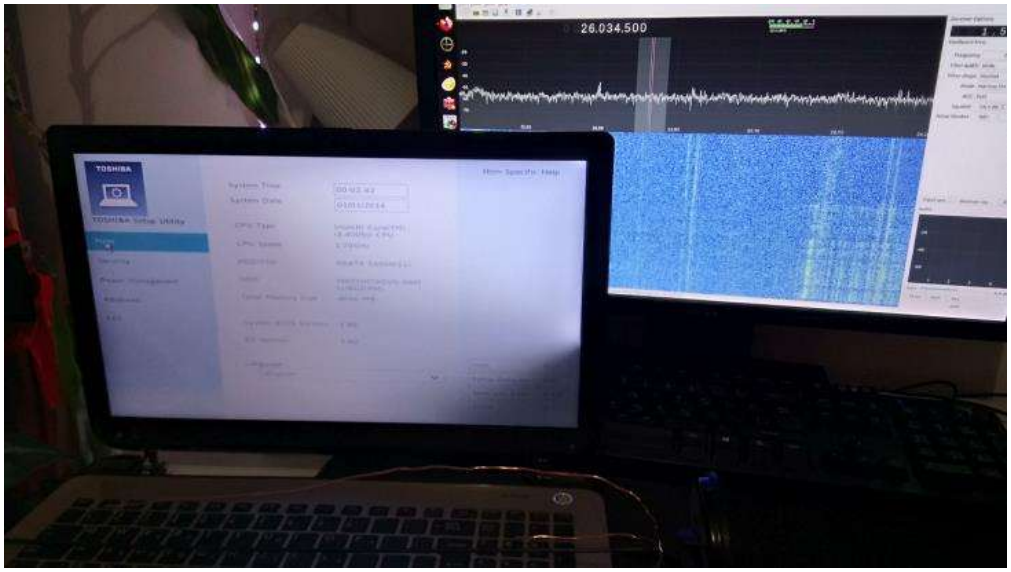
Πηγή: https://www.ti.com/lit/ds/symlink/pcm1870.pdf?ts=1668398242649

Μετά από μερικές δοκιμές εντόπισα την διαρροή και στο δικό μου laptop. Η οποία είναι στα 26,034MHz και κατάφερα να ακούω κανονικά την φωνή μου στο χώρο. Επιπλέον ανακάλυψα ότι η διαχείριση ενέργειας στο laptop κλείνει το ADC λίγα δευτερόλεπτα μετά από τη χρήση του για εξοικονόμηση ενέργειας. Οπότε αν δεν υπάρχει κάποια εφαρμογή που να κάνει ηχογράφηση δεν είναι σε λειτουργία η κάρτα και δεν υπάρχει εκπομπή.



Εικόνα 61. Λήψη ραδιοσυχνότητας της κάρτας ήχου

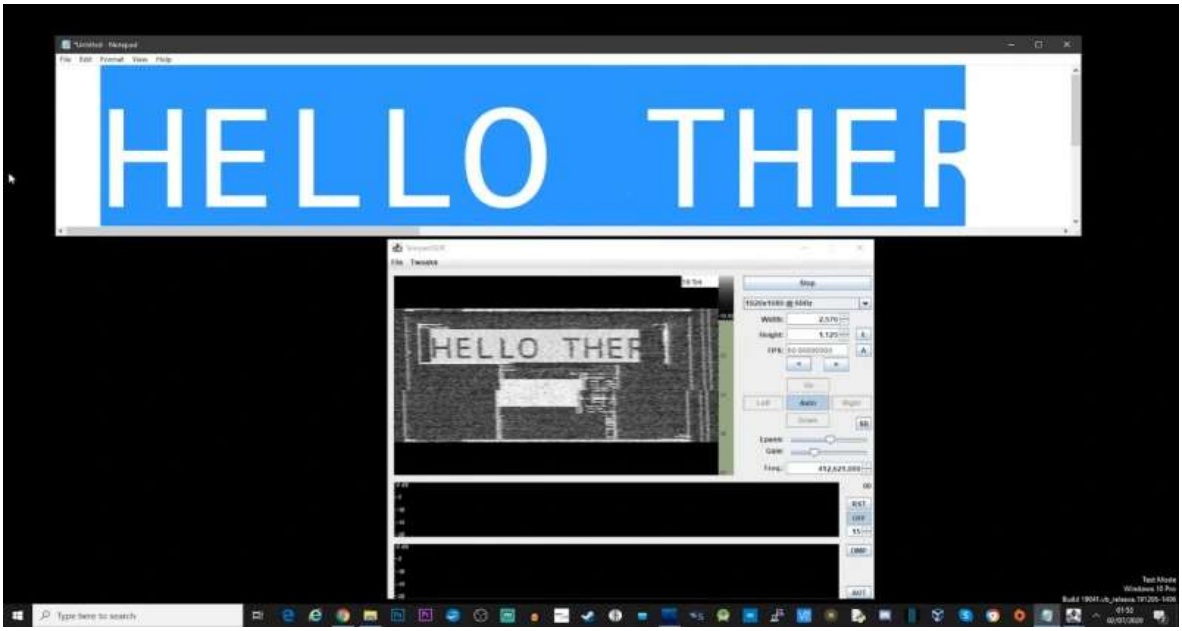
Όπως δεν υπάρχει και εκπομπή όταν ο υπολογιστής δεν έχει φορτώσει τους drivers του λειτουργικού και βρίσκετε στο BIOS. Κατά την εκκίνηση του υπολογιστή η κάρτα ενεργοποιείται και απενεργοποιείται κατά διαστήματα ανάλογα με τις διεργασίες που γίνονται στην φόρτωση του λειτουργικού και των οδηγών της κάρτας ήχου. Αυτή είναι μία ακόμα παράμετρος που μπορεί να μελετηθεί, έτσι ώστε να εξάγουμε κάποιο συμπέρασμα για το πόσο γρήγορα φορτώνει ο υπολογιστής και τι είδους λειτουργικό σύστημα διαθέτει.



Εικόνα 62. Έλεγχος της εκπομπής πριν την φόρτωση του λειτουργικού συστήματος

4.8.3 Exposing Computer Monitor Side-Channel Vulnerabilities with TempestSDR

Ακόμα, στις παλαιότερες οθόνες TV αλλά και υπολογιστή, τεχνολογίας CRT, είναι σχετικά απλό πλέον με το RTL-SDR να δούμε απομακρυσμένα το περιεχόμενο της οθόνης (Eck, 1983) . Η τεχνολογία CRT με τον καθοδικό σωλήνα και τη χρήση των ηλεκτρονικών πυροβόλων δημιουργούν φωσφορισμό στην επιφάνειά τους και χρησιμοποιούν υψηλές τάσης ρεύματος που με την σειρά τους δημιουργούν ισχυρά ηλεκτρομαγνητικά σήματα. Τα σήματα αυτά μπορούμε να τα λάβουμε και να αναδημιουργήσουμε απομακρυσμένα όπως στην εικόνα που προβάλετε.



Εικόνα 63. Υποκλοπή σήματος οθόνης

Πηγή: https://www.rtl-sdr.com/youtube-tutorial-spying-on-computer-monitors-with-tempestsdr/

Η τεχνική είναι πάρα πολύ παλιά και εφαρμόζεται χρόνια για την υποκλοπή δεδομένων από CRT οθόνες υπολογιστών, αλλά και να δούνε αν κάποιος παρακολουθεί κάποιο συγκεκριμένο πρόγραμμα στην τηλεόραση (https://en.wikipedia.org/wiki/Van_Eck_phreaking)

4.8.4 Password and encryption hack

Αν παρακολουθήσουμε και μπορέσουμε να δούμε συγκεκριμένες ταλαντώσεις που προκαλούνται από μετάδοση ή επεξεργασία δεδομένων, θα μπορέσουμε να δούμε τα δεδομένα αυτά. Παράδειγμα μπορούμε να καταγράψουμε το κύκλωμα του πληκτρολογίου και να δούμε κάποιο password την ώρα που πληκτρολογείτε. Ερευνητές του Πανεπιστημίου του Tel Aviv κατάφεραν να καταγράψουν ασύρματα, την εισαγωγή δεδομένων και κωδικών από το πληκτρολόγιο (keylogger) ενός laptop, υποκλέπτοντας τον ταλαντωτή του ελεγκτή του πληκτρολογίου επάνω στην μητρική πλακέτα. Όλος ο εξοπλισμός του RTL-SDR και του Raspberry που χρησιμοποιήθηκε χωρούσε μέσα στο ψωμάκι από ένα χάμπουργκερ.

Security researchers have figured out how to hack into laptops using pita bread and a radio

James Cook Jun 23, 2015, 6:32 AM

Researchers at Tel Aviv University have come up with a clever way to hack into laptops: using a radio receiver and a piece of pita bread.

The pita bread laptop-hacking device.
Tel Aviv University

The researchers published their findings online, showing that many laptop models give off electromagnetic radiation that can be manipulated into revealing the passwords stored on laptops.

Laptops running encryption programs could be fooled into revealing passwords when sent encrypted passages of text. Laptops would then encrypt the data, and researchers used components from a radio to pick up the changes in the electromagnetic radiation as the laptop's CPU works.

Here's the setup the researchers used to find the passwords:

Tel Aviv University

The laptop on the right is displaying a spectogram of the data received by the pita bread. The data is stored on a microSD card, which can be either accessed via Wi-Fi or manually retrieved.

INSIDER

Pita bread is used to disguise the components used in the hack, meaning it could be carried out in a restaurant or coffee shop without the target knowing.

It doesn't take hours to crunch the data and get the password, either. Researchers say the hack can show a password "within a few seconds."

Read the original article on Business Insider UK. Copyright 2015. Follow Business Insider UK on Twitter.

Εικόνα 64. Υποκλοπή κωδικών με ανίχνευση σημάτων πληκτρολογίου

Πηγή: https://www.businessinsider.in/security-researchers-have-figured-out-how-to-hack-into-laptops-using-pita-bread-and-a-radio/articleshow/47770898.cms

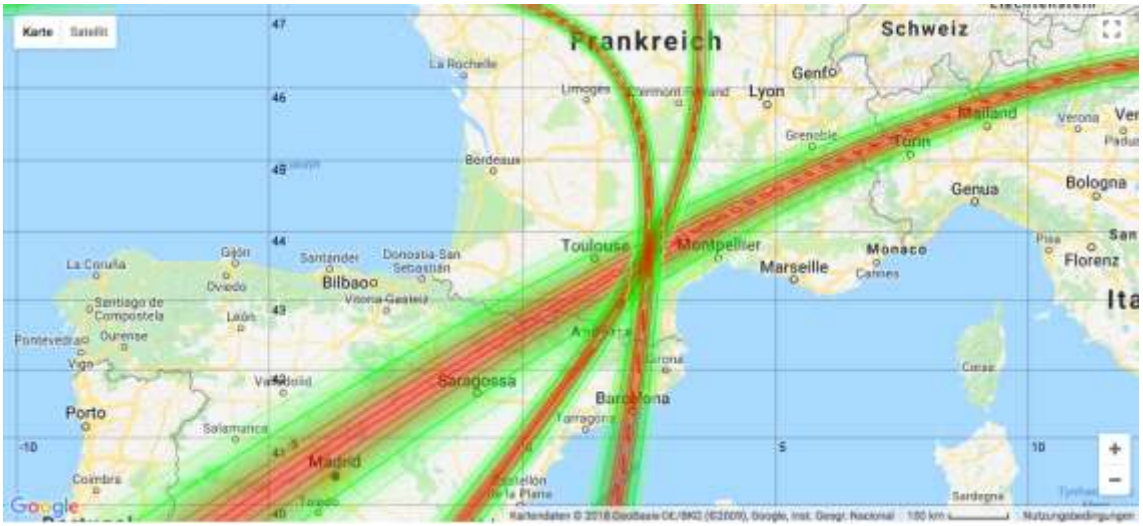
4.8.5 Data export

Μπορούμε να χρησιμοποιήσουμε την ακούσια εκπομπή ηλεκτρομαγνητικών σημάτων για να μεταδώσουμε πληροφορίες από συστήματα που δεν έχουν αυτή την δυνατότητα. Με αυτό τον τρόπο μπορούμε να θέσουμε υπό παρακολούθηση κάποια συσκευή ή να εξάγουμε δεδομένα από αυτή (https://github.com/funtenna/funtenna_2015).

Για παράδειγμα αν καθόμαστε σε ένα σταθμό εργασίας οποίος δεν επιτρέπει κανένα είδος δικτύωσης, δεν έχει κανένα αφαιρούμενο μέσο και δεν επιτρέπει ούτε έξοδο ήχου με την τεχνική αυτή να εξάγουμε δεδομένα ανοιγοκλείνοντας κάποιο κύκλωμα. Το ανοιγόκλειμα του κυκλώματος θα δημιουργήσει διάφορα τυχαία σήματα που με το RTL-SDR είναι εύκολο να τα εντοπίσουμε.

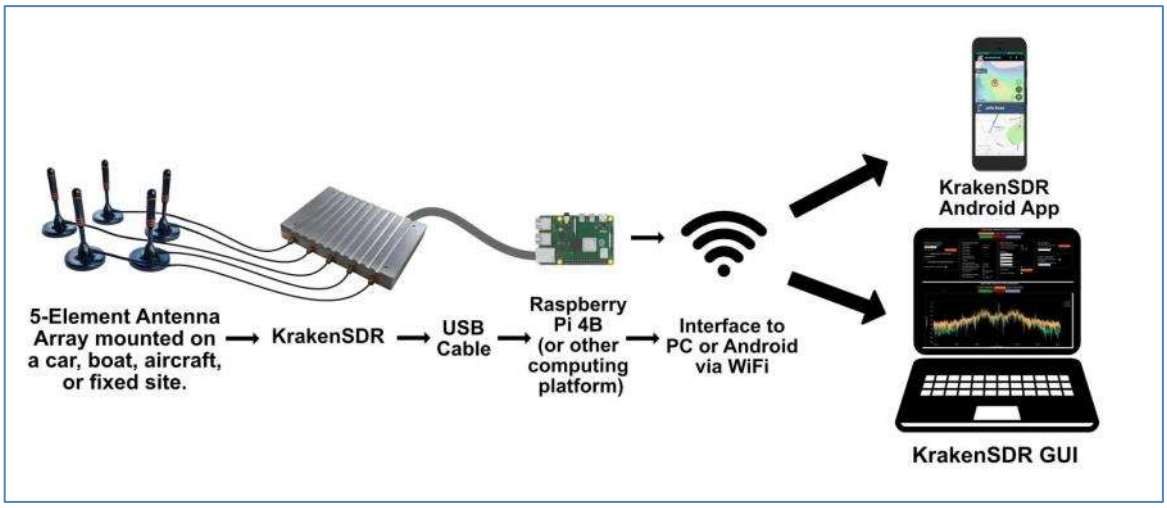
4.9 Μέθοδος προσδιορισμού θέσης πομπού Time Difference of Arrival (TDOA)

Με τη μέθοδο Time Difference of Arrival (TDOA) (Li & Zheng, 2022) μπορούμε να ανακαλύψουμε για κάθε σήμα, με πάρα πολύ απλό τρόπο το σημείο που γίνεται η εκπομπή ενός σήματος. Η μέθοδος TDOA έχει να κάνει με τη μικρή καθυστέρηση που λαμβάνει το σήμα από μία ομάδα από SDR που έχουν κατανεμηθεί στο χώρο. Λαμβάνοντας ένα σχετικό μικρό δείγμα εκπομπής μετά από επεξεργασία μπορεί να βρεθεί σε ποια απόσταση βρίσκεται από τον κάθε δέκτη και αν συνδυάζουμε τα γεωγραφικά δεδομένα των δεκτών , να βρούμε την ακριβή θέση του πομπού.



Εικόνα 65. Εντοπισμός σταθμού βραχέων κυμάτων με TDOA με 3 δέκτες με τη χρήση websdr

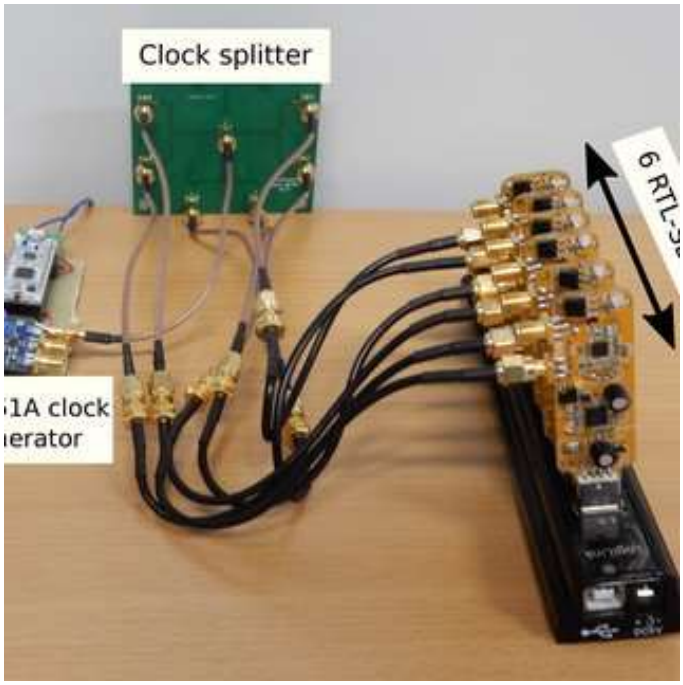
Η τεχνική μπορεί να εφαρμοστεί σε μικρή γεωγραφική κλίμακα με τη χρήση του KrakenSDR και να προσδιορίσει εκπομπές σε πραγματικό χρόνο μέσα σε μία πόλη ή σε μεγαλύτερη κλίμακα με τη χρήση ενός δικτύου από SDR (websdrs) που θα έχουν κατανεμηθεί σε διάφορες πόλεις, να γίνει ο εντοπισμός της πόλης της εκπομπής και μετά να γίνει ο ακριβής προσδιορισμός του πομπού.



Εικόνα 66. Σύστημα διαφορικής λήψης με 5 RTL-SDR (KrakenSDR)

Πηγή: https://www.crowdsupply.com/krakenrf/krakensdr

Πέρα από την μέθοδο TDOA που κάνει χρήση SDR που είναι τοποθετημένα στην ευρύτερη περιοχή του πομπού, υπάρχει και η μέθοδος direction finding η οποία με τη χρήση 4 SDR στο ίδιο σημείο υπολογίζεται ποιο SDR λαμβάνει με ελάχιστη διαφορά πρώτο το σήμα οπότε μπορεί να μας οδηγήσει προς το σημείο του πομπού. Αυτή είναι μια τεχνολογία που γίνεται χρήση ακόμα και στα σύγχρονα στρατιωτικά radar AESA.

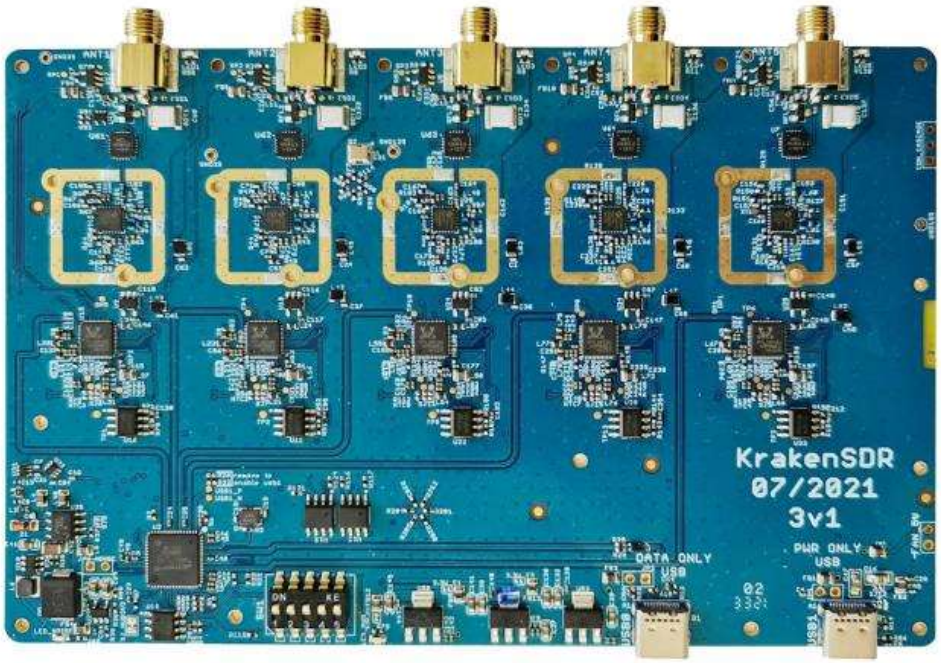


Εικόνα 67. Έξι RTL-SDR τα οποία έχουν συνδεθεί σε κοινό ταλαντωτή

Πηγή: https://www.researchgate.net/figure/RTL-Array-unit_fig3_332141599

Η επιτυχία της παραπάνω τεχνικής έχει φέρει νέες συσκευές στους hackers όπου σε μία πλακέτα υπάρχουν όλα τα SDR όπως το project KrakenSDR όπου 5 RTL-SDR έχουν

συνδεθεί με κοινό ταλαντωτή σε μια ποιοτική κατασκευή , η οποία έχει και μεγάλη ακρίβεια στα δεδομένα εντοπισμού που εξάγει.



Εικόνα 68. Πλακέτα του KrakenSDR

Πηγή: https://www.crowdsupply.com/krakenrf/krakensdr

5. Broken by design?

Θεωρίες ισχυρίζονται ότι το εν λόγω chip (Realtek RTL2832U) δεν είχε τυχαία αυτή τη δυνατότητα. Μια εταιρία που θα επενδύσει στην κατασκευή ενός ολοκληρωμένου κυκλώματος θέλει να καλύψει όσες περισσότερες δυνατότητες μπορεί με ένα ολοκληρωμένο κύκλωμα, αφού το κόστος παραγωγής είναι απειροελάχιστο σε σχέση με μια δεύτερη νέα γραμμή παραγωγής. Για ποιό λόγο επομένως να έχει μια γραμμή παραγωγής για το chip A και μία για το chip B όταν μπορεί να κάνει μία για το chip AB και αργότερα με λογισμικό να επιλέγει την λειτουργία A ή B;

Επομένως, προκύπτει πως υπάρχει κάποιο background στο chip και ότι τροφοδοτήθηκαν έτσι οι θεωρίες συνωμοσίας. Μία από αυτές είναι, αυτή που θέλει ουσιαστικά όλοι οι αγοραστές του εν λόγω TV Tuner, να μπορούν να γίνουν άθελά τους κατάσκοποι. Αφού θα μπορούσε κάποιος να ενεργοποιήσει την λειτουργία αυτή στον υπολογιστή τους απομακρυσμένα, εξάλλου ο driver των windows είναι κλειστό λογισμικό και δεν ξέρουμε τι κάνει. Θα μπορούσε να μεταδώσει κάποια ενδιαφέροντα δεδομένα από ραδιοσυχνότητες της περιοχής του που έκανε λήψη στον άτυπο “διαχειριστή” του Tuner. Τα δεδομένα θα μπορούσαν να μεταφερθούνε καλυμμένα με κρυπτογράφηση και κατά την διαδικασία κάποιου “update” να πάνε στον προορισμό τους. Με τη λίστα των “spygadgets” που δημοσίευσε ο Έντουαρντ Σνόουντεν τίποτα δεν είναι απίθανο πλέον.

Εικόνα 69. Διαρροή πληροφοριών από τον Έντουαρντ Σνόουντεν

Πηγή: https://en.wikipedia.org/wiki/ANT_catalog

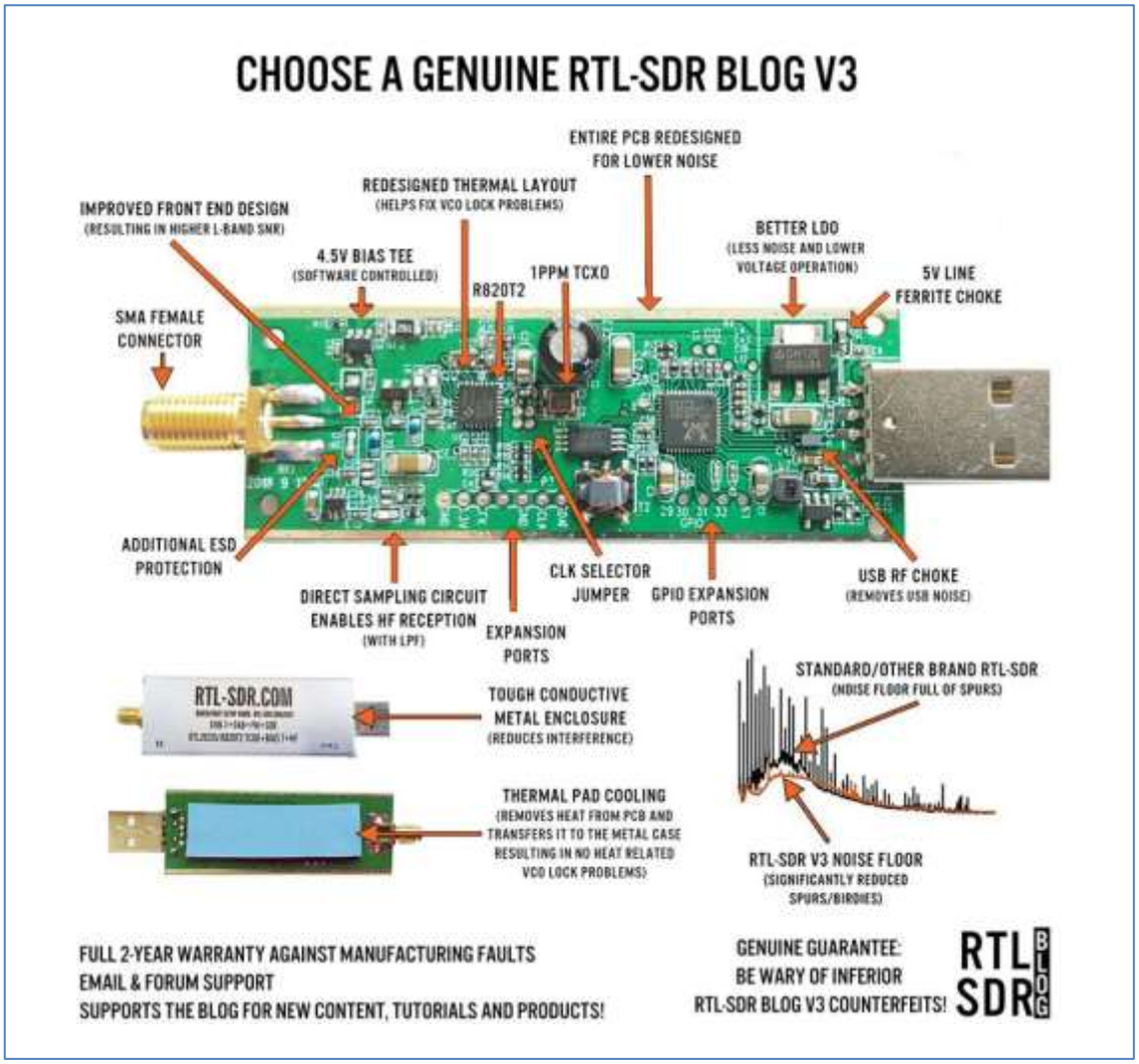
Στη λίστα των gadgets τα SDR κατέχουν την πρώτη θέση, καθώς τα περισσότερα από αυτά χρησιμοποιούν ραδιοσυχνότητες για να λάβουν τα ηλεκτρομαγνητικά σήματα που τους ενδιαφέρουν.

Τα κόστος το επαγγελματικών συσκευών είναι τεράστιο οπότε αναλογιστείτε πόσο σημαντικό είναι το γεγονός τι μπορεί κάποιος να κάνει με 20 ευρώ που κοστίζει το RTL-SDR.

6. Το μέλλον

Με τη μεγάλη επιτυχία του project, αρκετοί ήταν αυτοί που ήθελαν να αναβαθμίσουν τις δυνατότητες του RTL-SDR και έτσι σχεδίασαν και κατασκεύασαν νέα RTL-SDR με καλύτερες δυνατότητες που ως κύριο σκοπό δεν έχουν να είναι δέκτες ψηφιακής τηλεόρασης DVB-T αλλά να λειτουργούν ως SDR. Στην εικόνα βλέπουμε την 3ή έκδοση που έχει κατασκευαστεί με χαρακτηριστικά που σχεδίασαν οι χρήστες της σελίδας RTL-SDR.com, όπου εκεί βρίσκεται και η μεγαλύτερη κοινότητα του RTL-SDR project.

Στις βελτιώσεις που έχουν κάνει θέλουν να επιτύχουν καλύτερο ποσοστό σήματος έναντι θορύβου και σταθερότητα του εσωτερικού ταλαντωτή στις υψηλές συχνότητες.



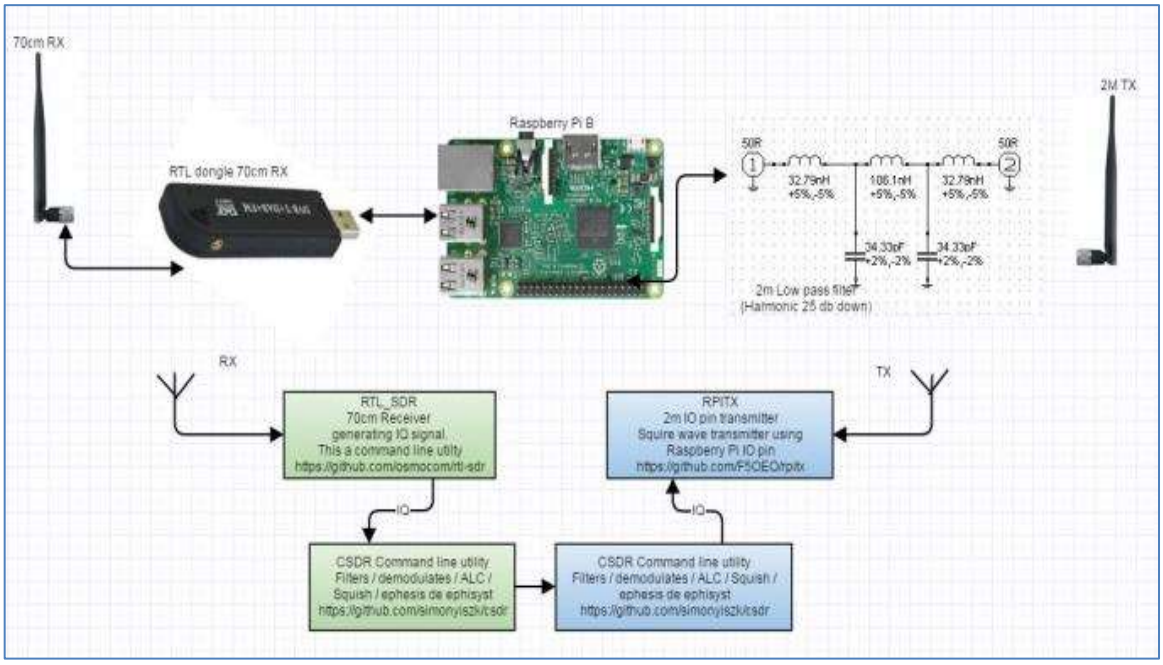
Εικόνα 70. Νέο RTL-SDR Version 3

Πηγή: https://www.rtl-sdr.com/buy-rtl-sdr-dvb-t-dongles

Ένα εξαιρετικό χαρακτηριστικό που φέρνει η έκδοση 3, είναι η δυνατότητα λήψης directsampling, όπου επιτρέπει την λήψη σημάτων κάτω των 24MHz χωρίς καμία τροποποίηση του υλικού. Επομένως με αυτή την σημαντική προσθήκη μπορεί να λάβει όλα τα βραχέα κύματα και το εύρος του να γίνει από 0Mhz έως 1700Mhz.

Φυσικά οι hackers δεν έχουν σταματήσει στο RTL-SDR και έχουν πάει σε άλλα projects τα οποία τους επιτρέπουν να έχουν νέες δυνατότητες.

Έχουν πετύχει εκπομπή ραδιοκύματος με το raspberrypi (projectrpitx), αλλά εντυπωσιακό είναι αυτό το οποίο έχουν κάνει μια USB κάρτα γραφικών (project FL2K), να λειτουργεί ως πομπός σε όλο το εύρος συχνοτήτων που λαμβάνει το RTL-SDR, με αποτέλεσμα αν κάνουμε χρήση των δύο συσκευών να έχουμε ένα πλήρες σύστημα πομποδέκτη.



Εικόνα 71. Συνδυασμός RTL-SDR και RPITX

Πηγή: https://www.rtl-sdr.com/building-a-homemade-fm-repeater-with-a-raspberry-pi-rpitx-and-rtl-sdr-dongle/

Με την USB κάρτα γραφικών που χρησιμοποιεί το chip FL2000, μπορούμε να πειράξουμε τον driver και να κάνουμε από ένα απλό αναλογικό ραδιοφωνικό σταθμό ή να προχωρήσουμε παραπέρα σε ένα ψηφιακό ραδιοφωνικό DAB ή έναν ψηφιακό τηλεοπτικό σταθμό DVB ή ακόμα και μια κυψέλη του δικού μας δικτύου κινητής τηλεφωνίας! (https://osmocom.org/projects/osmo-fl2k/wiki)

Εικόνα 72. GSM transmission

Πηγή: https://osmocom.org/projects/osmo-fl2k/wiki

Προσοχή!

Για την εκπομπή ραδιοσυχνότητας απαιτείται άδεια, οπότε όποιος πειραματισμός γίνει, θα πρέπει να γίνει χωρίς χρήση εξωτερικών κεραιών και με ελάχιστη ισχύ!

Ο υπεύθυνος φορέας για την εποπτεία του ραδιοφάσματος στην Ελλάδα είναι η Ε.Ε.Τ.Τ. (www.eett.gr) και για τη διεξαγωγή μετρήσεων, για τα όρια και την πυκνότητα του ηλεκτρομαγνητικού πεδίου, η αρμόδια αρχή είναι η Ελληνική Επιτροπή Ατομικής Ενέργειας (www.eeae.gr).

Συμπεράσματα

Συνοψίζοντας καταλήγουμε στο συμπέρασμα ότι η χρήση των πολύπλοκων ηλεκτρονικών συσκευών δεν περιορίζεται αποκλειστικά στα πλαίσια των εφαρμογών για τις οποίες κατασκευάστηκαν και η ασφάλεια των δεδομένων που διαχειρίζονται, δεν είναι δεδομένη. Μπορούν να τροποποιηθούν κατάλληλα για διαφορετικές χρήσεις από αυτές που τις προόριζαν οι κατασκευαστές τους.Αυτή η τροποποίηση επαληθεύεται στην περίπτωση του RTL-SDR project, όπου μπορεί η απόδοση της νέας χρήσης του εξοπλισμού DVB-T stick να μην μπορεί να ανταγωνιστεί συσκευές που έχουν φτιαχτεί αποκλειστικά για εφαρμογές SDR, αλλά στα πλαίσια του πειραματισμού και της ελάττωσης του κόστους κτήσης είναι αποδεκτή.

Η ασφάλεια των ραδιοεπικοινωνιών λόγω της δυσκολίας της πρόσβασης στο φυσικό μέσο καταργείται με τη χρήση SDR και είναι πλέον εφικτό να έχουμε εύκολη πρόσβαση σε ραδιοδίκτυα που βρίσκονται τριγύρω μας. Μόνο οι συσκευές που κάνουν χρήση ισχυρής κρυπτογράφησης μπορούν να διαφυλάξουν την ασφάλεια των επικοινωνιών. Η κρυπτογράφηση όμως δεν μπορεί να εμποδίσει μια επίθεση άρνησης εξυπηρέτησης, όπου παρεμβαίνει ένα ισχυρότερο σήμα και εμποδίζει ή καταστρέφει την πληροφορία που μεταδίδεται. Ακόμα και συστήματα με μεταπήδηση συχνότητας είναι ευάλωτα στα SDR της επαγγελματικής κατηγορίας, τα οποία έχουν δυνατότητες λήψης φάσματος πάνω από 60MHz ταυτόχρονα.

Οι σύγχρονες ηλεκτρονικές συσκευές κατακλύζονται από ολοκληρωμένα κυκλώματα τα οποία αν τα μελετήσουμε και τα κατανοήσουμε, τότε το μόνο όριο στη χρήση τους είναι η φαντασία μας. Για αυτό πέρα από το ανοιχτό λογισμικό, είναι εξίσου σημαντικό, και το ανοιχτό υλισμικό (hardware) το οποίο μας δίνει όλες τις πληροφορίες που θέλουμε για να πειραματιστούμε μαζί του, για την τεχνολογική ανάπτυξη, εκπαίδευση και ασφάλεια.

Ως προς τις μελλοντικές επεκτάσεις της εργασίας, προτείνεται η διεξαγωγή μίας μελέτη των δεδομένων από έξυπνους ασύρματους αισθητήρες εσωτερικής και εξωτερικής θερμοκρασίας. Για παράδειγμα, με βάση τα καταγεγραμμένα δεδομένα από τους έξυπνους αισθητήρες, θα μπορούσε να γίνει μια μελέτη (σε ετήσια βάση) σχετικά με το πόσο θερμαίνονται ή ψύχονται τα σπίτια και να το αντιπαραβάλουμε με διάφορα οικονομικά κριτήρια, όπως τιμή πετρελαίου, τιμή ρεύματος, κ.α.

Επίσης, με βάση δεδομένα από τις ραδιοσυχνότητες που λαμβάνει το RTL-SDR προτείνεται η ανάπτυξη ενός νευρωνικού δικτύου και η δημιουργία διαφόρων προφίλ καταστάσεων. Θα μπορούσαν να εξεταστούν τα προφίλ αυτά για πρόγνωση διαφόρων συμπεριφορών. Για παράδειγμα, αύξηση των εκπομπών ραδιοκυμάτων σε κάποιο συγκεκριμένο φάσμα ραδιοσυχνοτήτων και ταύτιση του με κάποιο συγκεκριμένο γεγονός.

Βιβλιογραφία

Argume, A., Coaguila, R., Yanyachi, P. R., & Chilo, J. (2021). NOAA Image Data Acquisition to Determine Soil Moisture in Arequipa, Perú. *IEEE Transactions on Nuclear Science* , 4.

Bulychev, R. V., Goncharov, D. E., & Babalova, I. F. (2018). Obtaining IMSI by software-defined radio (RTL-SDR). *2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)* (σ. 3). University MEPhI Russian Federation: IEEE.

Eck, W. v. (1983, Ιανουάριος). *Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?* Ανάκτηση Νοέμβριος 15, 2022, από https://cryptome.org/emr.pdf

James H. Mclellan, R. W. (2019). *Θεμελιώδεις Έννοιες της Επεξεργασίας Σημάτων.* Πάτρα: Εκδόσεις Gotsis.

Li, A., & Zheng, Y. (2022). Research and Implementation of Wireless TDOA Positioning Station Synchronization Based on RTL-SDR. *2022 IEEE 6th Information Technology and Mechatronics Engineering Conference (ITOEC)* (σ. 4). Chengdu, China: IEEE.

NVIDIA. (2013). *NVIDIA SDR (Software Defined Radio) Technology The modem innovation inside NVIDIA i500 and Tegra 4i.* NVIDIA Corporation.

Ramasubramanian, M., Banerjee, C., Roy, D., Pasiliao, E., & Mukherjee, T. (2021). Exploiting Spatio-Temporal Properties of I/Q Signal Data Using 3D Convolution for RF Transmitter Identification. *IEEE Journal of Radio Frequency Identification* , 113-127.

realtek.com. (2019). *DVB-T COFDM Demodulator + USB 2.0* . Ανάκτηση Νοέμβριος 15, 2022, από RTL2832U: https://www.realtek.com/en/products/communications-network-ics/item/rtl2832u

S, S., J, A. S., H, A. S., R, G., & P, S. K. (2015). Multicast WebSDR implementation using RTL-SDR. *2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)* (σ. 4). Coimbatore, India: IEEE.

Shravan, M., Rakshit, R., Sanjana, P., Priya, B. K., & Kumar, N. (2020). RTL SDR ADS-B Data Analysis for Predicting Airports and ATS Routes. *2020 International Conference for Emerging Technology (INCET)* (σ. 7). Amrita Vishwa Vidyapeetham, India: IEEE.

Stewart, R. W., Crockett, L., Atkinson, D., Barlee, K., Crawford, D., Chalmers, I., και συν. (2015, Σεπτέμβριος). A low-cost desktop software defined radio design environment using MATLAB, simulink, and the RTL-SDR. *IEEE Communications Magazine* , σσ. 64-71.

Texas Instruments. (2007, Σεπτέμβριος). *16-Bit Low-Power Stereo Audio ADC With Microphone Bias and Microphone Amplifier.* Ανάκτηση Νοέμβριος 15, 2022, από PCM1870: https://www.ti.com/lit/ds/symlink/pcm1870.pdf?ts=1666109388873&ref_url=https%253A%252F%252Fwww.ti.com%252Faudio-ic%252Fconverters%252Fadc%252Fproducts.html

Vachhani, K., & Mallari, R. A. (2015). Experimental study on Wide Band FM Receiver using GNURadio and RTL-SDR. *2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI)* (σ. 5). Ahmedabad, India: IEEE.

Vildyaeva, M. V., Egorova, E. A., & Vavrenyuk, A. B. (2018). Using a Neural Network to Convert a Radio Signal from an RTL-SDR Receiver to Text. *2018 International Conference on Signal, Image, Vision and their Applications (SIVA)* (σ. 3). Moscow: IEEE.

wikipedia.org. (2022, Νοέμβριος 6). *White_hat_(computer_security)*. Ανάκτηση Νοέμβριος 14, 2022, από wikipedia.org: https://en.wikipedia.org/wiki/White_hat_(computer_security)

Wright, D. P., & Ball, E. A. (2020). Highly Portable, Low-Cost SDR Instrument for RF Propagation Studies. *IEEE Transactions on Instrumentation and Measurement* , 12.

Zecke. (2016, Φεβρουαρίου 9). *GSMTAP*. Ανάκτηση Νοέμβριος 15, 2022, από osmocom.org: https://osmocom.org/projects/baseband/wiki/GSMTAP

Καραγιαννίδης Κ.Γεώργιος, Κ. Π. (2017). *Τηλεπικοινωνιακά Συστήματα.* Εκδόσεις Τζιόλα.

ΛΙΒΑΝΙΟΣ, Θ., & ΠΑΝΑΓΙΩΤΟΠΟΥΛΟΣ, Ν. (2021). Έγκριση Εθνικού Κανονισμού Κατανομής Ζωνών Συχνοτήτων (ΕΚΚΖΣ). *ΕΦΗΜΕΡΙΔΑ ΤΗΣ ΚΥΒΕΡΝΗΣΕΩΣ* , Τεύχος Β’ 6474/31.12.2021.

ΜΑΓΚΡΙΩΤΗΣ, Ι. (2011). Κανονισμός λειτουργίας ερασιτεχνικών σταθμών. *ΕΦΗΜΕΡΙΣ ΤΗΣ ΚΥΒΕΡΝΗΣΕΩΣ* , Αρ. Φύλλου 1969.

Παράρτημα Κώδικα

Έλεγχος λειτουργίας του driver του RTL-SDR (Linux, Windows)

```
rtl_test -t
```

Βασική λήψη σήματος ραδιοφωνικού σταθμού FM στα 96.6MHz (Linux)

```
rtl_fm -f 96.3e6 -M wbfm -s 200000 -r 48000 - | aplay -r 48k
-f S16_LE
```

Λήψη δεδομένων τηλεμετρίας από την ISMσυχνότητα 433MHz (Linux, Windows)

```
rtl_433 -A
```

Εύρεση κυψελών κινητής στα GSM 900MHz (Linux)

```
kal -s 900
```

Εμφάνιση transponder αεροσκαφών σε web interface http://localhost:8080

```
dump1090 --interactive –net
```

Αποκωδικοποίηση κώδικα morse από την συχνότητα 7,025MHz (Linux)

```
rtl_fm -f 7025000 -s 22050 | multimon-ng -t raw -a MORSE_CW
-
```

Γλωσσάρι όρων

API	Application programming interface – Διεπαφή προγραμματισμού εφαρμογών.
ARM	Αρχιτεκτονική επεξεργαστών που χρησιμοποιούνται σε κινητά τηλέφωνα ή ταμπλέτες
CB	Citizens Band – Ελεύθερο εύρος συχνοτήτων για επικοινωνία πολιτών (27MHz)
DAB	Digital Audio Broadcast – Ψηφιακή μετάδοση ραδιοφώνου
DVB-T	Digital Video Broadcast – Ψηφιακή μετάδοση επίγειας τηλεόρασης
driver	Λογισμικό οδήγησης συσκευής
firmware	Λογισμικό τμήμα οδηγού οδήγησης συσκευής
Fourrier	Μετασχηματισμός σήματος από την μονάδα του χρόνου στην μονάδα των συχνοτήτων
FM	Frequency Modulation – Διαμόρφωση σήματος κατά συχνότητας
GQRX	Λογισμικό ανοιχτού κώδικα για λήψη ραδιοκυμάτων με SDR.
ISM	Industrial Scientific Medical Radio Band συχνότητες που ορίζονται στον Εθνικό Κανονισμό Κατανομής Ζωνών Συχνοτήτων (ΕΚΚΖΣ)
IoT	Internet of thinks – Μικροσυσκευές με δυνατότητα σύνδεσης στο διαδίκτυο.
hardware	Υλικό που συνθέτει ένα υπολογιστή
HF	High Frequency – Υψηλές ραδιοσυχνότητες
Hz	Μονάδα μέτρησης συχνότητας. Πολλαπλάσια KHz, MHz, GHz
SDR	Software Defined Radio – Δέκτης ραδιοφώνου που υλοποιείτε με λογισμικό.
Linux	Λειτουργικό σύστημα υπολογιστών ανοιχτού κώδικα
LNA	Ενισχυτής χαμηλού θορύβου
LoRa	Long Range – Δίκτυο χαμηλής ισχύος μεγάλης εμβέλειας
Modem	Modulator Demodulator -Διαμορφωτής Αποδιαμορφωτήςσήματος
Navtex	Μηνύματα ενημέρωσης ναυτιλίας
Realtek	Εταιρία παραγωγής ολοκληρωμένων κυκλωμάτων
RAW I/Q	Read And Write data signal in time domain. Άμεση μετάδοση δεδομένων σήματος στην μονάδα του χρόνου.

Reverse engineering	Ανάστροφη μηχανική για να αποδομίσουμε την λειτουργία μιας συσκευής ή ενός λογισμικού.
RTL-SDR	Το project που μετατρέπει έναν δέκτη DVB-T με το chip RTL2832U της Realtek σε SDR.
Stingray	Συσκευή παρακολούθησης δικτύου GSM, που προσποιείτε την λειτουργία κυψέλης. (Man in the middle attack)
TCP	Δικτυακό πρωτόκολλο μετάδοσης δεδομένων.
Tuner	Δέκτης ραδιοσυχνοτήτων
Upconverter	Τεχνική αύξησης ραδιοσυχνότητας
UHF	Ultra High Frequency – Πάρα πολύ υψηλές ραδιοσυχνότητες
VHF	Very High Frequency – Πολύ υψηλές ραδιοσυχνότητες
VLF	Very Low Frequency – Πολύ χαμηλές ραδιοσυχνότητες
white hat hackers	Ηθικοί hackers
Windows	Λειτουργικό σύστημα υπολογιστών κλειστού κώδικα

Ιστοσελίδες ενδιαφέροντος

https://www.rtl-sdr.com

https://osmocom.org/projects/rtl-sdr/wiki/Rtl-sdr

https://gqrx.dk

https://github.com/osmocom/rtl-sdr

http://superkuh.com/rtlsdr.html

https://wiki.gnuradio.org/index.php/Main_Page

https://zadig.akeo.ie

https://openai.com/blog/whisper/

https://www.hackster.io/matjaz4/rf-modulation-recognition-with-gnu-radio-11b294

https://github.com/nihalpasham/fingerprinting_radios_w_ML

https://en.wikipedia.org/wiki/Types_of_radio_emissions

https://sudonull.com/post/68962-Analysis-of-GSM-network-traffic-in-Wireshark-Pentestit-Blog

https://osmocom.org/projects/baseband/wiki/GSMTAP

https://blog.fearcat.in/a?ID=01000-50a39f65-d25d-4204-a907-e2bb76ba0c63

https://www.ckn.io/blog/2015/11/29/gsm-sniffing-sms-traffic/

https://github.com/ninjhacks/gsmevil2/blob/master/GsmEvil.py

https://pa3fwm.nl/technotes/tn20.html

https://insinuator.net/2013/10/pytacle-alpha2/

https://www.cellmapper.net/arfcn?net=GSM&ARFCN=114&MCC=0

https://blog.adaptivemobile.com/the-mobile-network-battlefield-in-ukraine-part-1?hsLang=en

https://hackaday.io/projects?tag=SDR

https://www.cgran.org/