

# RF The Forgotten Art

Mike Jones "H4unt3d Hacker"



H4UNT3D  
HACKER



# Who am I?

- Former Hacktivist
- Penetration Tester
- Security Researcher
- Podcast Host "H4unt3d Hacker"
- Founder of "The H4unt3d Hacker Community"
- Former SIGINT Operator US DoD
- Former FBI Informant
- Knight Ink Media screenplay writer "ransom"
- MDR Manager / Red Team / IR
- Board member (UAE and London)





# SIGINT

In God we trust.  
Everyone else we monitor.

# What is RF

- Radio Frequency is a band or bands used for telecommunications.
- Electronic emissions is energy put off from electronic devices (leak)
- Key fobs, wifi, BT, smart meters, electronic devices
- Radio transmissions
  - Voice
  - Video
  - Data

# Types of Antennas

- Array Antennas
  - Yagi
- Wire Antennas
  - Dipole
  - loop
- Reflector Antennas
  - Parabolic



# Hackrf One & DragonOS

- GSM Scanning for base stations (multiple frqs)
- Grgsm-Livemon scrolling through freqs to find active voice freqs
- Decoding for IMSI and SMS
- Recording of audio and text
- Identifies phone numbers and carriers based on MNC number

# GSM Details

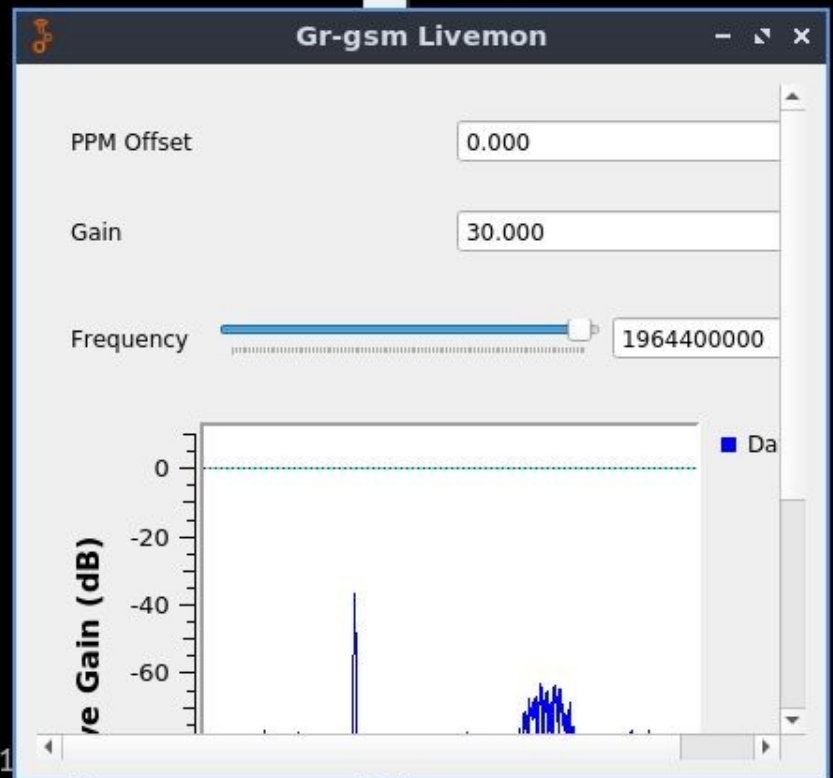
- MCC—Mobile Country Code
  - <https://cellidfinder.com/mcc-mnc>
- MNC—Mobile Network Code (ATT, Tmobile etc)
- Cell ID—Bast station Transciever
- LAC—Location Area Code
  
- GSM TAP--pseudo-header format, used to encapsulate frames from a GSM Um (air) interface into UDP/IP packets. It serves a similar purpose to that of radiotap in the 802.11 world.



```
mike@mike-IdeaPad-3-14IML05: /usr/src/gsmevil2
File Actions Edit View Help

mike@mike-IdeaPad-3-14IML05: /usr/src/gsmevil2
chan: 657 (1959.2MHz - 39.493kHz) power: 6791864.71
chan: 658 (1959.4MHz + 36.091kHz) power: 7750018.03
chan: 659 (1959.6MHz + 13.753kHz) power: 8495352.54
chan: 660 (1959.8MHz - 17.764kHz) power: 7505856.76
chan: 661 (1960.0MHz - 36.498kHz) power: 6865620.56
chan: 663 (1960.4MHz + 12.974kHz) power: 6986218.27
chan: 664 (1960.6MHz - 15.781kHz) power: 8052634.38
chan: 665 (1960.8MHz - 36.254kHz) power: 7253236.10
chan: 666 (1961.0MHz - 4.207kHz) power: 8356042.68
chan: 667 (1961.2MHz + 13.264kHz) power: 7186164.73
chan: 668 (1961.4MHz - 9.910kHz) power: 6578361.40
chan: 669 (1961.6MHz - 33.775kHz) power: 7792990.19
chan: 681 (1964.0MHz + 34.665kHz) power: 9219670.12
chan: 682 (1964.2MHz + 35.142kHz) power: 9196307.51
chan: 683 (1964.4MHz + 10.300kHz) power: 9280158.34
chan: 684 (1964.6MHz - 14.938kHz) power: 9356203.01
chan: 685 (1964.8MHz - 39.588kHz) power: 9385900.79
chan: 717 (1971.2MHz + 11.365kHz) power: 5022440.23
chan: 720 (1971.8MHz - 11.745kHz) power: 5256942.73
chan: 721 (1972.0MHz - 36.037kHz) power: 5113275.33
chan: 731 (1974.0MHz - 29.510kHz) power: 4600122.45

mike@mike-IdeaPad-3-14IML05: /usr/src/gsmevil2$
mike@mike-IdeaPad-3-14IML05: /usr/src/gsmevil2$
mike@mike-IdeaPad-3-14IML05: /usr/src/gsmevil2$ sudo grgsm_livemon -f 1
QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
[INFO] [UHD] linux; GNU C++ version 9.2.1 20200304; Boost_107100; UHD_3.15.0.0-2build5
gr-osmosdr 0.2.0.0 (0.2.0) gnuradio 3.8.1.0
built-in source types: file osmosdr fcd rtl rtl_tcp uhd miri hackrf bladerf rfspace airs
py airspyhf soapy redpitaya freesrp
[INFO] [UHDSoapyDevice] Opening HackRF One #0 f77c60dc2a20a1c3...
-- Using subdev spec '0:0'.
```





1900mhz.txt

base.jpg

Computer

mike

Network

Trash (Empty)

```

mike@mike-IdeaPad-3-14IML05: /usr/src/gsmevil2
File Actions Edit View Help
mike-IdeaPad-3-14IML05: /usr/src/gsmevil2
mike@mike-IdeaPad-3-14IML05: /usr/src/gsmevil2

  OSMOSEW

    * 丐爪 丐儿 | 千千毛尺 *

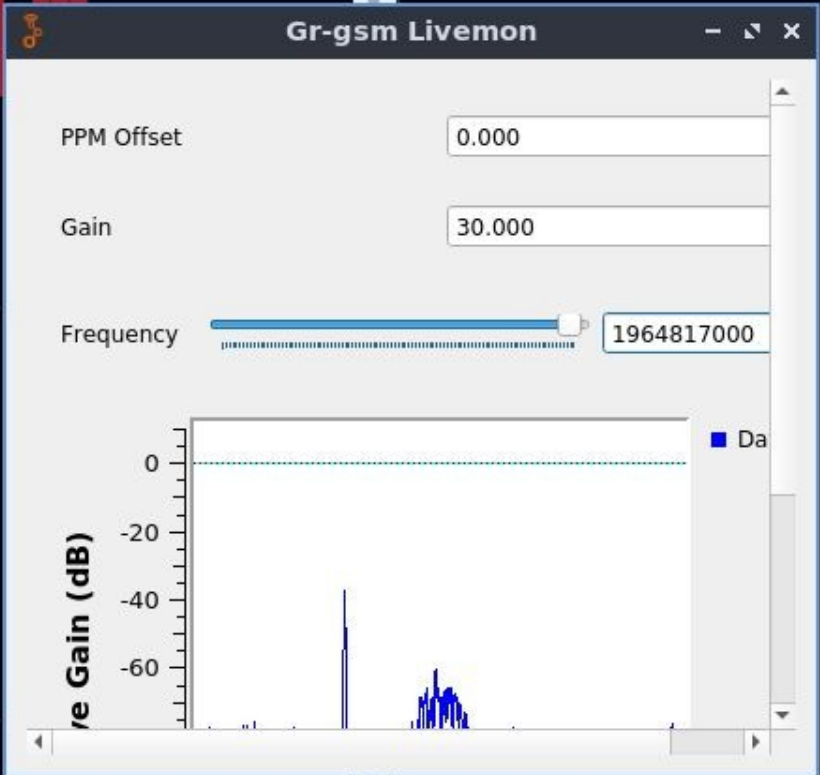
-----

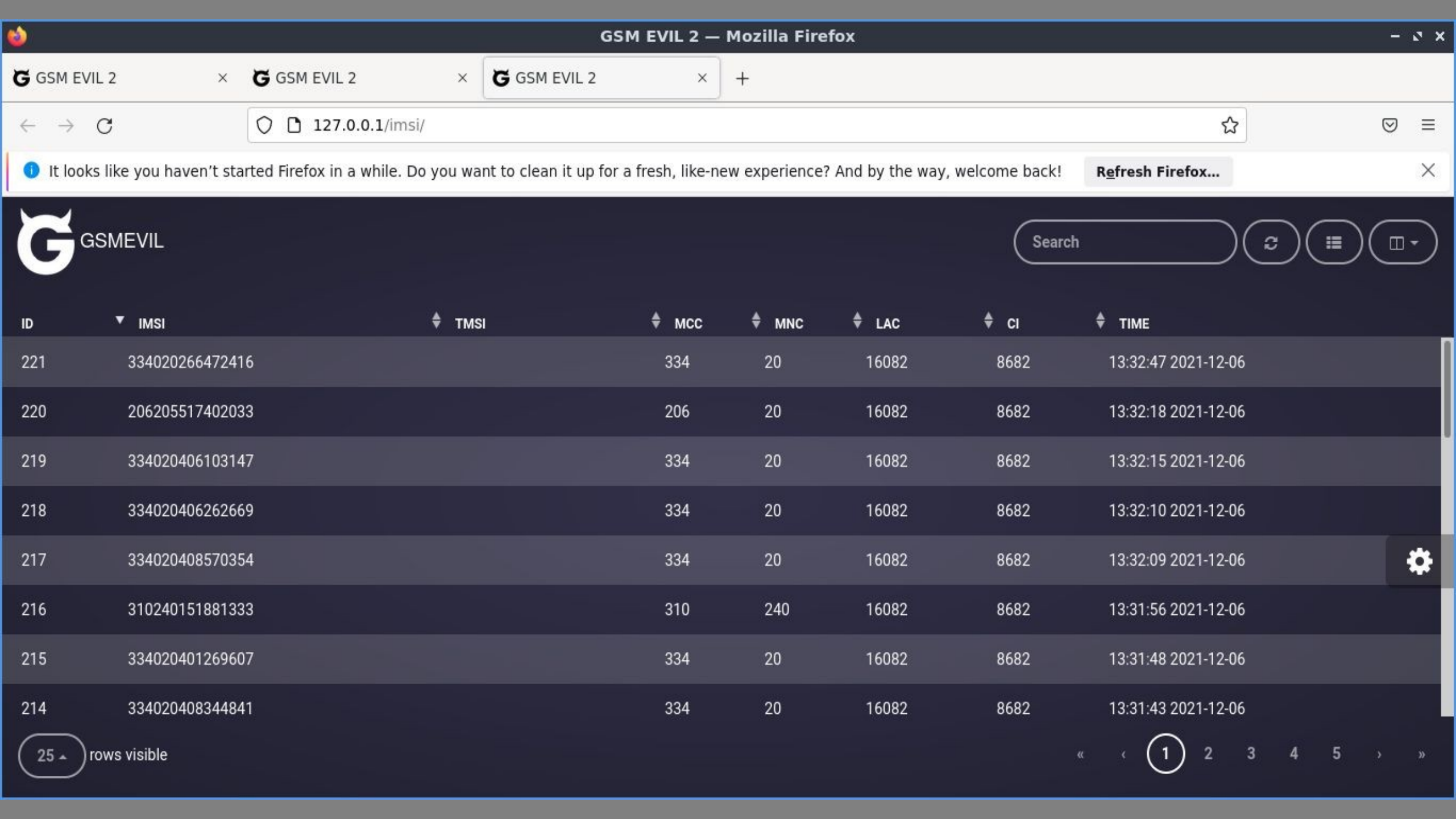
About:-
Author: sheryar (ninjhacks)
Version : 2.0.0

Disclaimer:-
This program was made to understand how GSM network works.
Not for bad hacking !
We are not responsible for any illegal activity !

-----

```





It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back! Refresh Firefox... X



Search [refresh] [menu] [window]

ID	IMSI	TMSI	MCC	MNC	LAC	CI	TIME
221	334020266472416		334	20	16082	8682	13:32:47 2021-12-06
220	206205517402033		206	20	16082	8682	13:32:18 2021-12-06
219	334020406103147		334	20	16082	8682	13:32:15 2021-12-06
218	334020406262669		334	20	16082	8682	13:32:10 2021-12-06
217	334020408570354		334	20	16082	8682	13:32:09 2021-12-06
216	310240151881333		310	240	16082	8682	13:31:56 2021-12-06
215	334020401269607		334	20	16082	8682	13:31:48 2021-12-06
214	334020408344841		334	20	16082	8682	13:31:43 2021-12-06

25 rows visible



Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	127.0.0.1	127.0.0.1	GSMTAP	81	(CCCH) (RR) Immediate Assignment
2	0.015984005	127.0.0.1	127.0.0.1	GSMTAP	81	(CCCH) (RR) Paging Request Type 1
3	0.036149112	127.0.0.1	127.0.0.1	GSMTAP	81	(CCCH) (RR) System Information Type 3
4	0.042030918	127.0.0.1	127.0.0.1	LAPDm	81	U, func=UI
5	0.064788841	127.0.0.1	127.0.0.1	GSMTAP	81	(CCCH) (SS)
6	0.070925188	127.0.0.1	127.0.0.1	LAPDm	81	U, func=Unknown(DTAP) (SS)
7	0.077061380	127.0.0.1	127.0.0.1	GSMTAP	81	(CCCH) (RR) Paging Request Type 1
8	0.083524147	127.0.0.1	127.0.0.1	GSMTAP	81	(CCCH) (RR) Paging Request Type 1
9	0.135767374	127.0.0.1	127.0.0.1	GSMTAP	81	(CCCH) (RR) Paging Request Type 1
10	0.144589556	127.0.0.1	127.0.0.1	GSMTAP	81	(CCCH) (RR) Paging Request Type 1
11	0.157976780	127.0.0.1	127.0.0.1	GSMTAP	81	(CCCH) (RR) Paging Request Type 1
12	0.200353240	127.0.0.1	127.0.0.1	GSMTAP	81	(CCCH) (RR) Paging Request Type 1
13	0.201008206	127.0.0.1	127.0.0.1	LAPDm	81	U, func=UI(CCCH) (RR) System Information Type 5

▶ Frame 925: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface lo, id 0  
 ▶ Ethernet II, Src: 00:00:00\_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00\_00:00:00 (00:00:00:00:00:00)  
 ▶ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1  
 ▶ User Datagram Protocol, Src Port: 58421, Dst Port: 4729  
 ▶ GSM TAP Header, ARFCN: 685 (Downlink), TS: 0, Channel: CCCH (8)  
 ▶ GSM CCCH - Paging Request Type 1

```

0000 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00  .....E.
0010 00 43 9d 4b 40 00 40 11 9f 5c 7f 00 00 01 7f 00  .C.K@.@. \.....
0020 00 01 e4 35 12 79 00 2f fe 42 02 04 01 00 82 ad  ...5.y / .B.....
0030 c3 00 00 11 5d 8c 02 22 08 b8 15 06 21 00 01 f0  ....]..". ....!.
0040 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b  ++++++++ ++++++++
0050 2b  +
  
```



# System Bus Radio

---

This program transmits radio on computers / phones without radio transmitting hardware.

## Why?

---

Some computers are intentionally disconnected from the rest of the world. This includes having their internet, wireless, bluetooth, USB, external file storage and audio capabilities removed. This is called "air gapping". Even in such a situation, this program can transmit radio.

Publicly available documents already discuss exfiltration from secured systems using various electromagnetic radiations. This is documented in the TEMPEST guidelines published by the US National Security Agency and the US Department of Defense. This project simply adds to that discussion.

## How to use it

---

**NEW:** Try it in your browser, click here: <http://fulldecent.github.io/system-bus-radio/>

Enter the `Using _mm_stream_si128` folder and compile using `make`. (There are also other flavors you can `make` and try in different folders!)



**RSOISS**

серия 1

1/12



**80 лет со дня рождения  
первого космонавта планеты Земли  
- Ю.А.Гагарина**




# Contact

Help

mail.aec.org.sy

هيئة الطاقة الذرية السورية  
Atomic Energy Commission of Syria

**SquirrelMail**



**Atomic Energy Commission Of Syria Webmail  
Login**

Name:

Password:

Login

- @H4unt3dH
- <https://www.linkedin.com/in/mikejonesnotanalias/>
- [hauntedhacker2121@gmail.com](mailto:hauntedhacker2121@gmail.com)
- TheHauntedHacker.com
- <https://teespring.com/en-GB/stores/the-h4unt3d-h4ck3r>
- <https://www.youtube.com/channel/UCMTI8uupT2orU0WeLDiqZ-g>
- On all major streaming platforms Spotify, iTunes, Pandora etc.

