SIGINT on a Budget

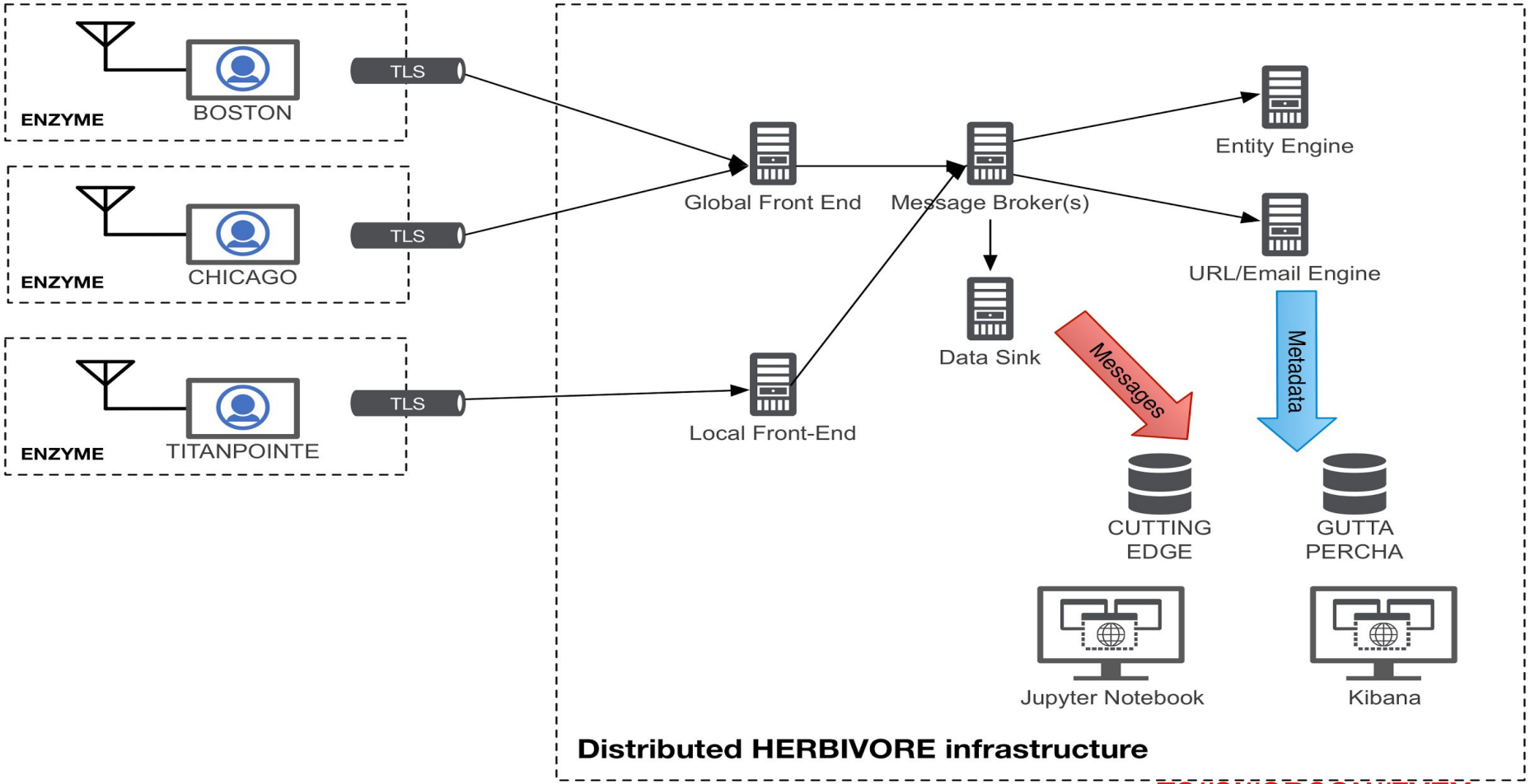
Listen In, **Gather** Data, Be **Terrified**…

All For Under $100

Derived From	MILK/CSSM 1-52
Dated	20180121
Declassify On	20480121

TS//SI//ORCON//FVEY

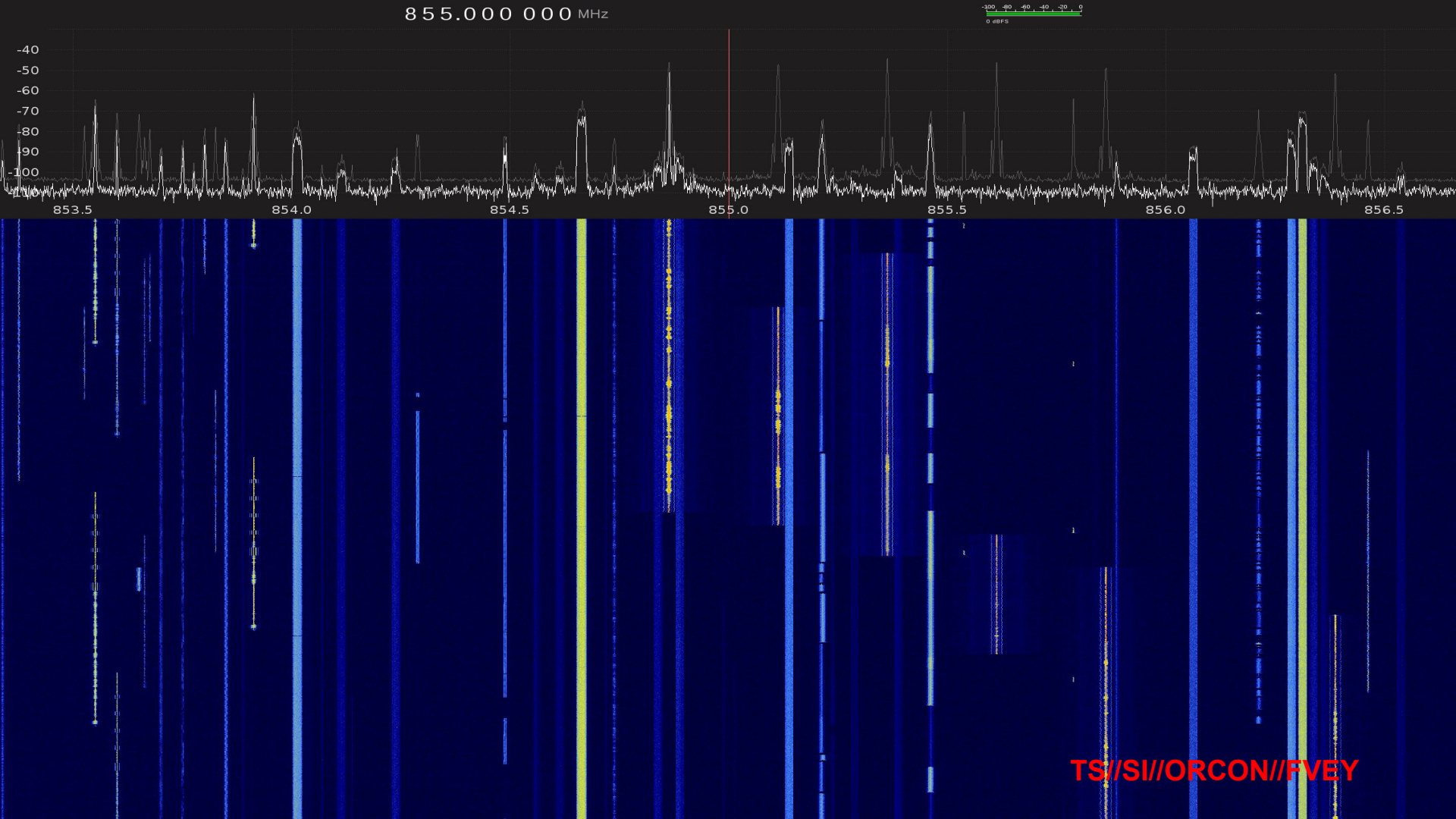

TS//SI//ORCON//FVEY

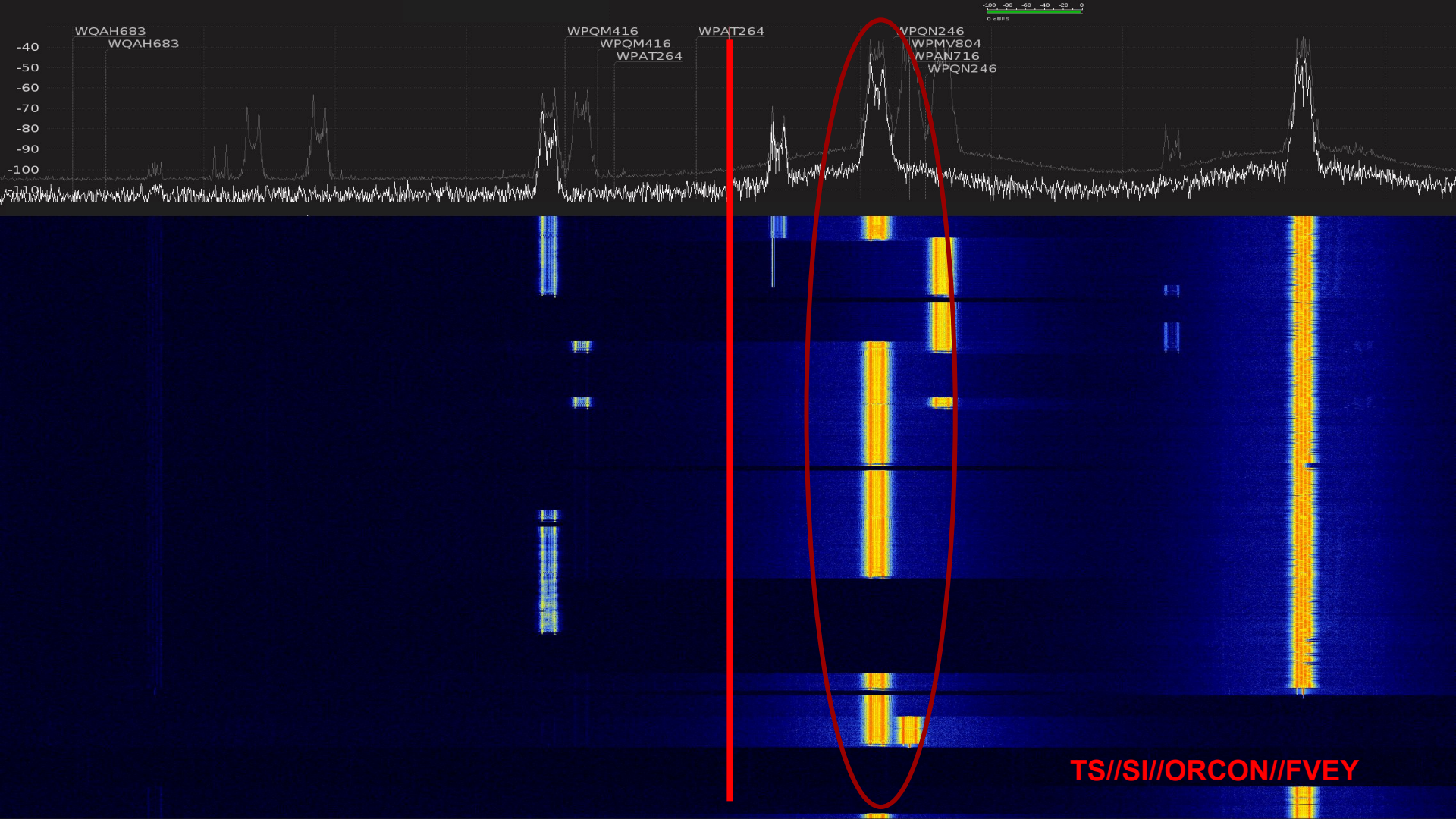


TS//SI//ORCON//FVEY


CONFIGURATION
NAME:
COMBAT
Enemies feeble, never attack first.
0 1 2 3
MISSION
Simplified plot and gameplay.
0 1 2 3
PUZZLE
Most puzzles are more difficult.
0 1 2 3
CYBER
Cyberspace is normal.
0 1 2 3
START


USRP B210
70 MHz – 6 GHz
ESD SENSITIVE
Ettus Research
A National Instruments Company
RF A
TX/RX
RX2
RF B
TX/RX
RX2


855.000 000 MHz
-100 -80 -60 -40 -20 0
0 dBFS
-40
-50
-60
-70
-80
-90
-100
853.5
854.0
854.5
855.0
855.5
856.0
856.5
TS//SI//ORCON//FVEY


WQAH683
WQAH683
WPQM416
WPQM416
WPAT264
WPAT264
WPQN246
WPMV804
WPAN716
WPQN246
-40
-50
-60
-70
-80
-90
-100
-110
TS//SI//ORCON//FVEY

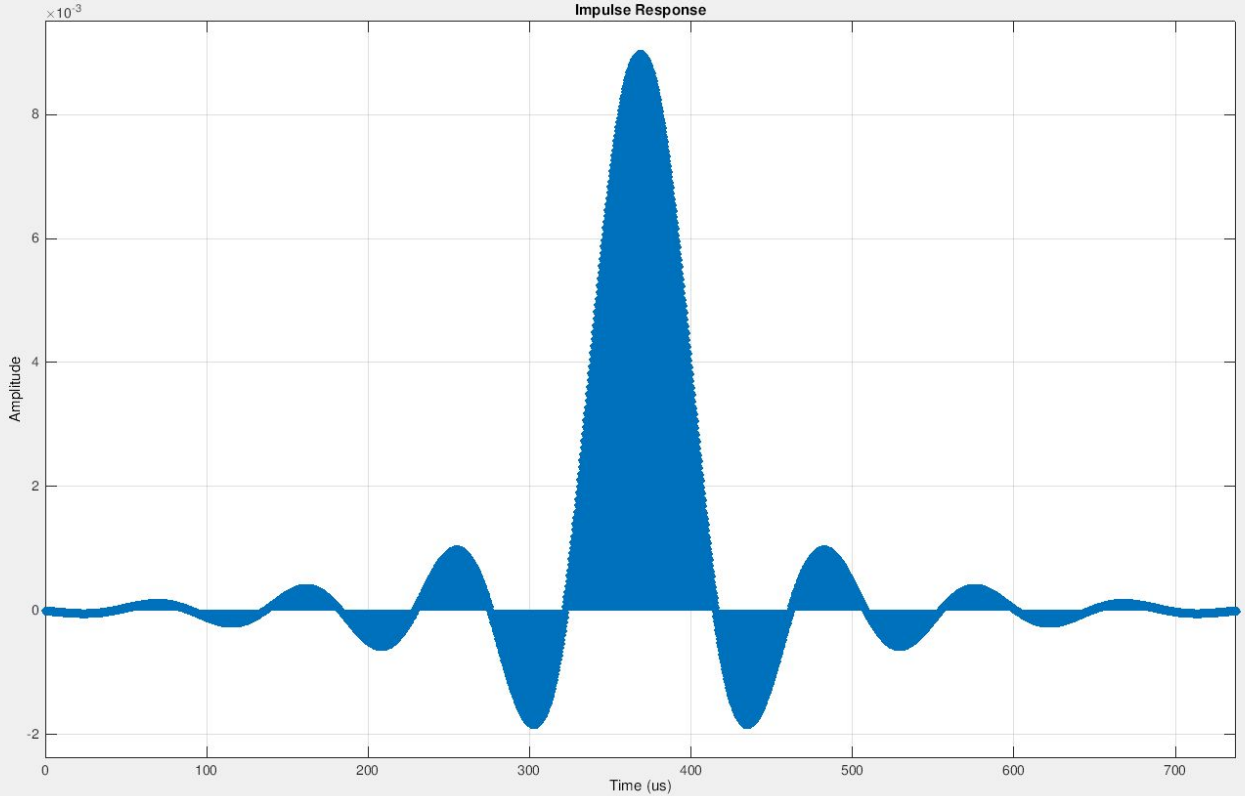
TS//SI//ORCON//FVEY

Filter Visualization Tool - Figure 2: Impulse Response

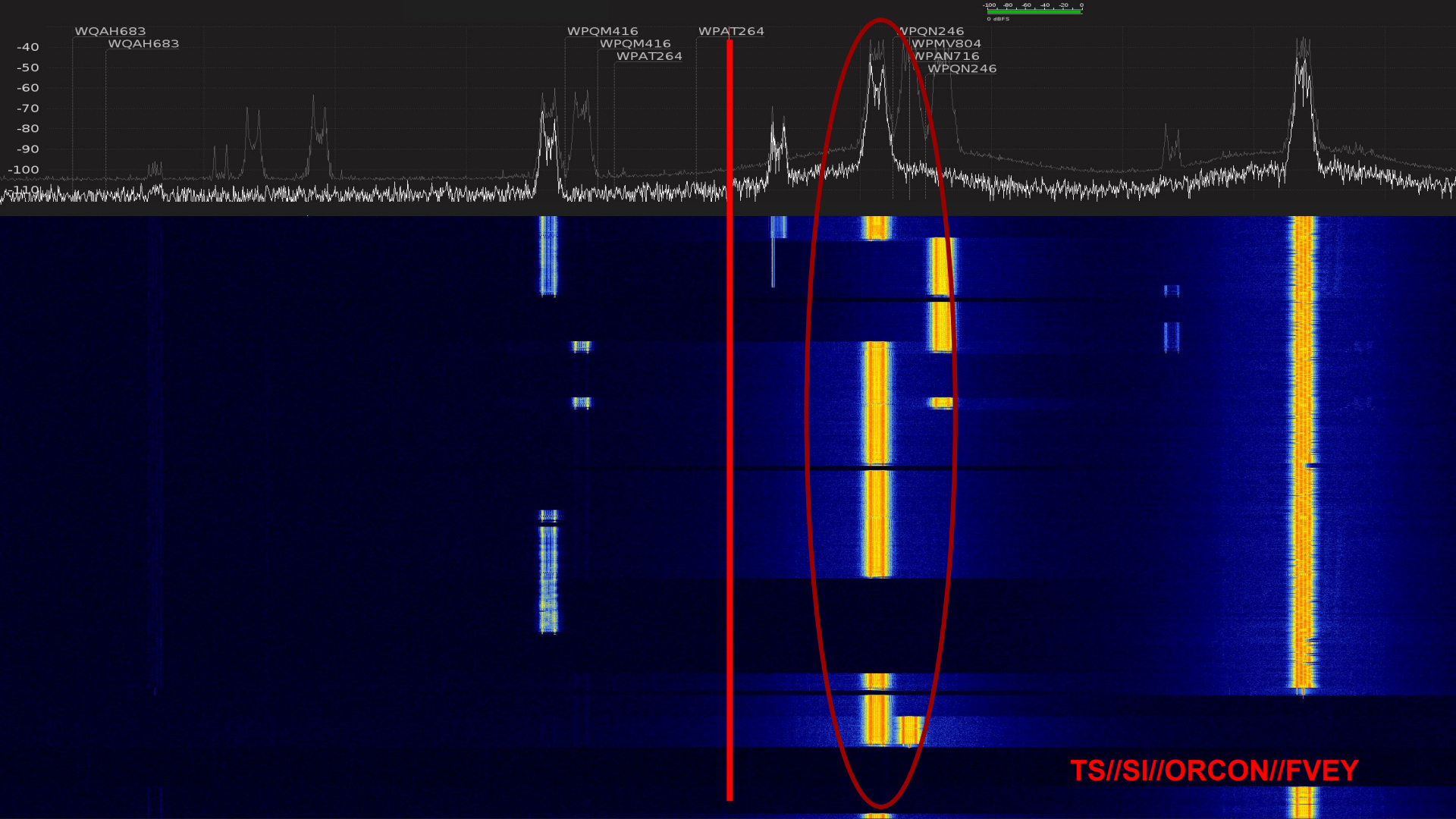
File Edit Analysis Insert View

Impulse Response

Figure 2: Impulse Response



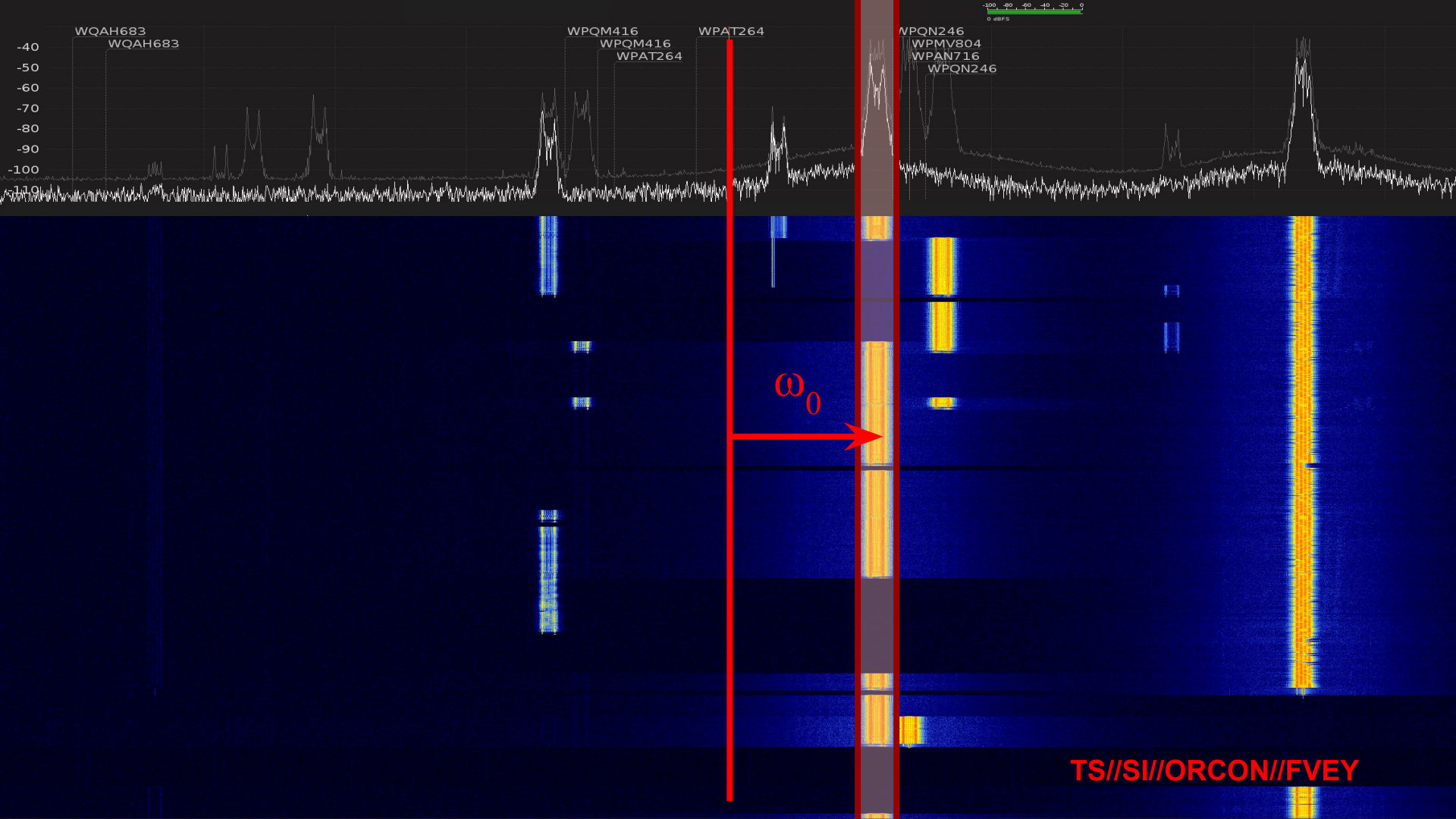
EY


WQAH683
WQAH683
WPQM416
WPQM416
WPAT264
WPAT264
WPQN246
WPMV804
WPAN716
WPQN246
-40
-50
-60
-70
-80
-90
-100
-110
TS//SI//ORCON//FVEY

$$\mathrm{rect}(\omega) \rightarrow \frac{\sin(\pi t)}{\pi t}$$

If we had infinite time and space, life would be easy...

$$\frac{\sin(\pi t)}{\pi t} e^{j\omega_0 t} \rightarrow \mathrm{rect}(\omega - \omega_0)$$

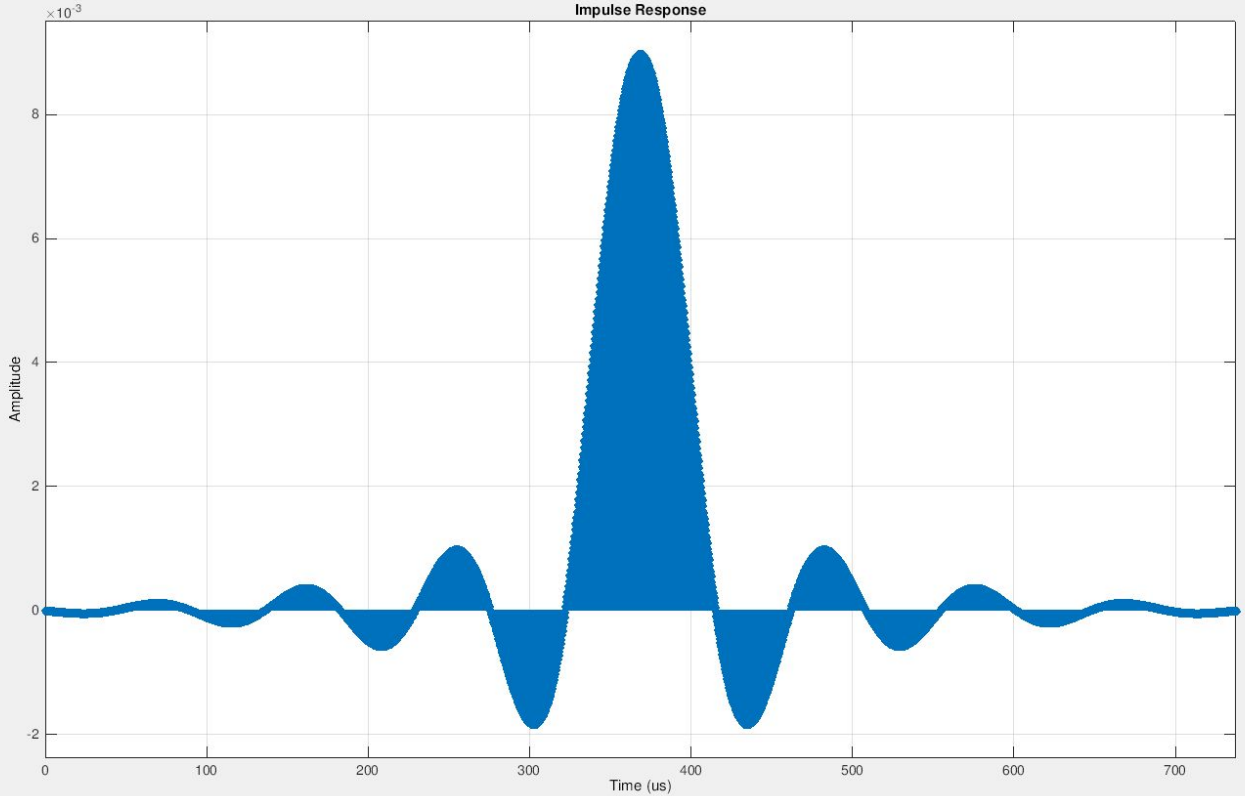

WQAH683
WQAH683
WPQM416
WPQM416
WPAT264
WPAT264
WPQN246
WPMV804
WPAN716
WPQN246
-40
-50
-60
-70
-80
-90
-100
-110
ω_0
TS//SI//ORCON//FVEY

Filter Visualization Tool - Figure 2: Impulse Response

File Edit Analysis Insert View

Impulse Response

Figure 2: Impulse Response



EY

Filter Visualization Tool - Figure 1: Magnitude Response (dB)

File Edit Analysis Insert View Debug Desktop Window Help

Figure 1: Magnitude Response (dB)

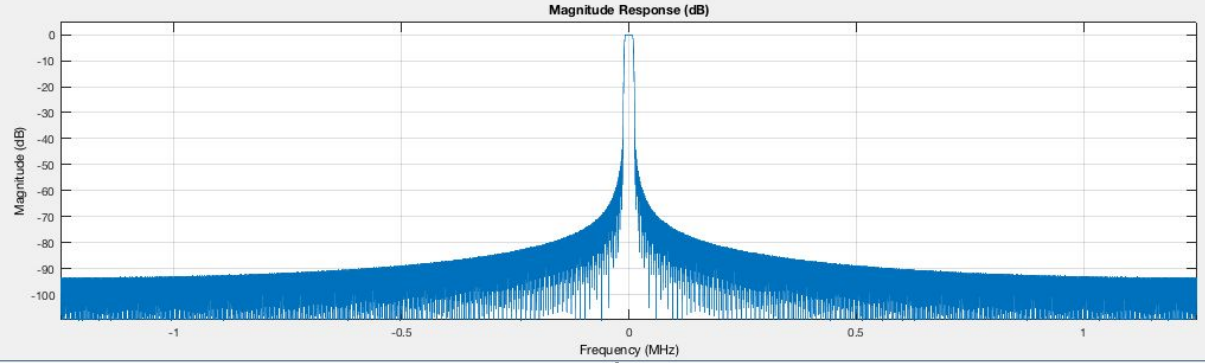
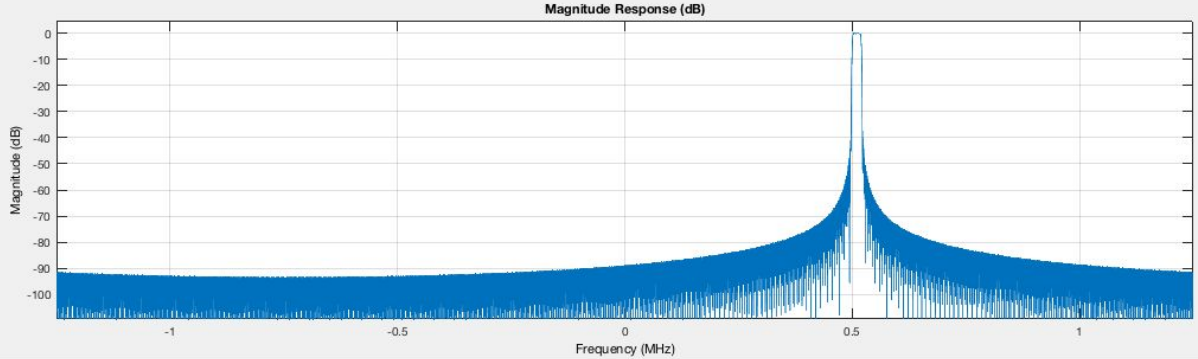
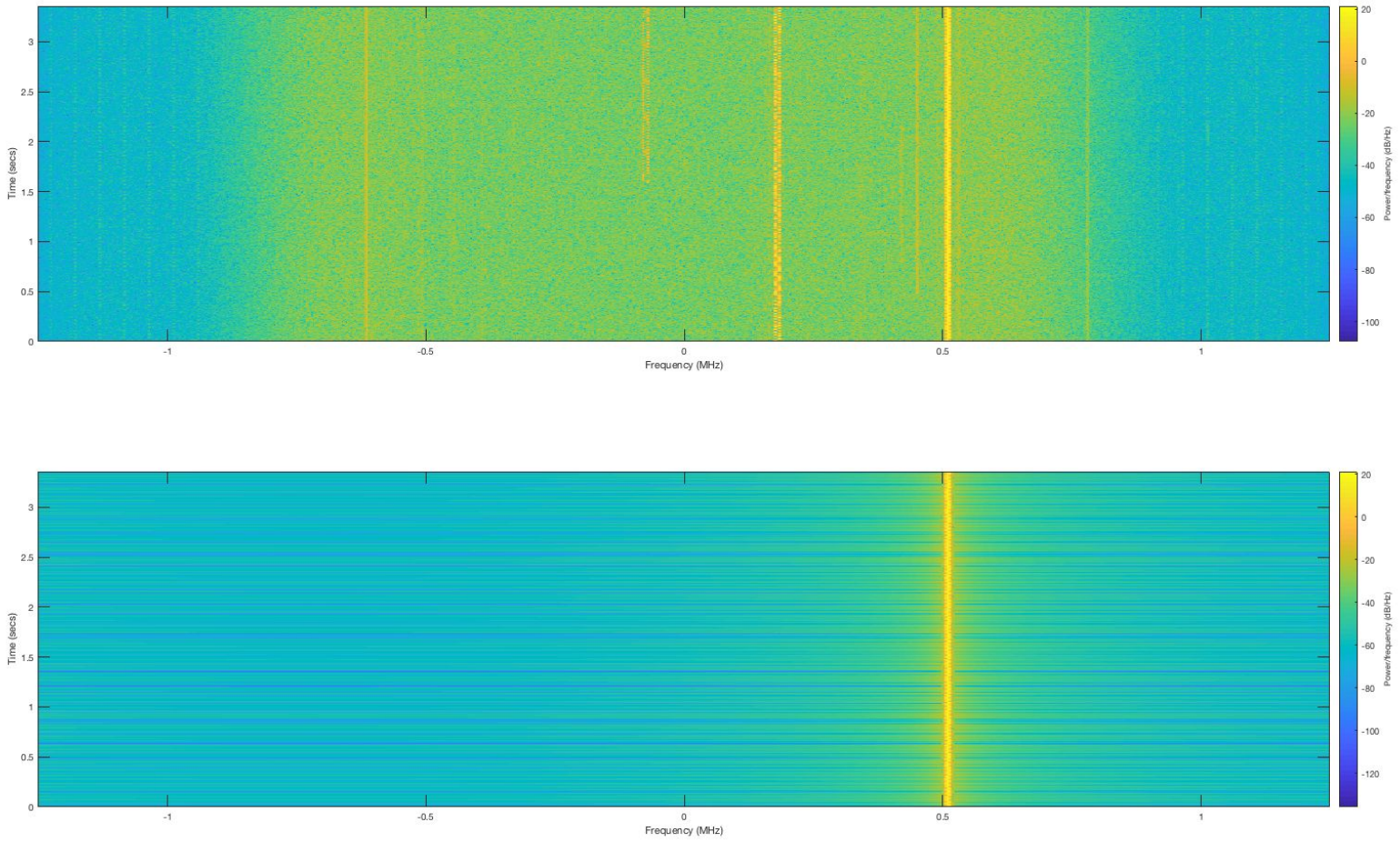
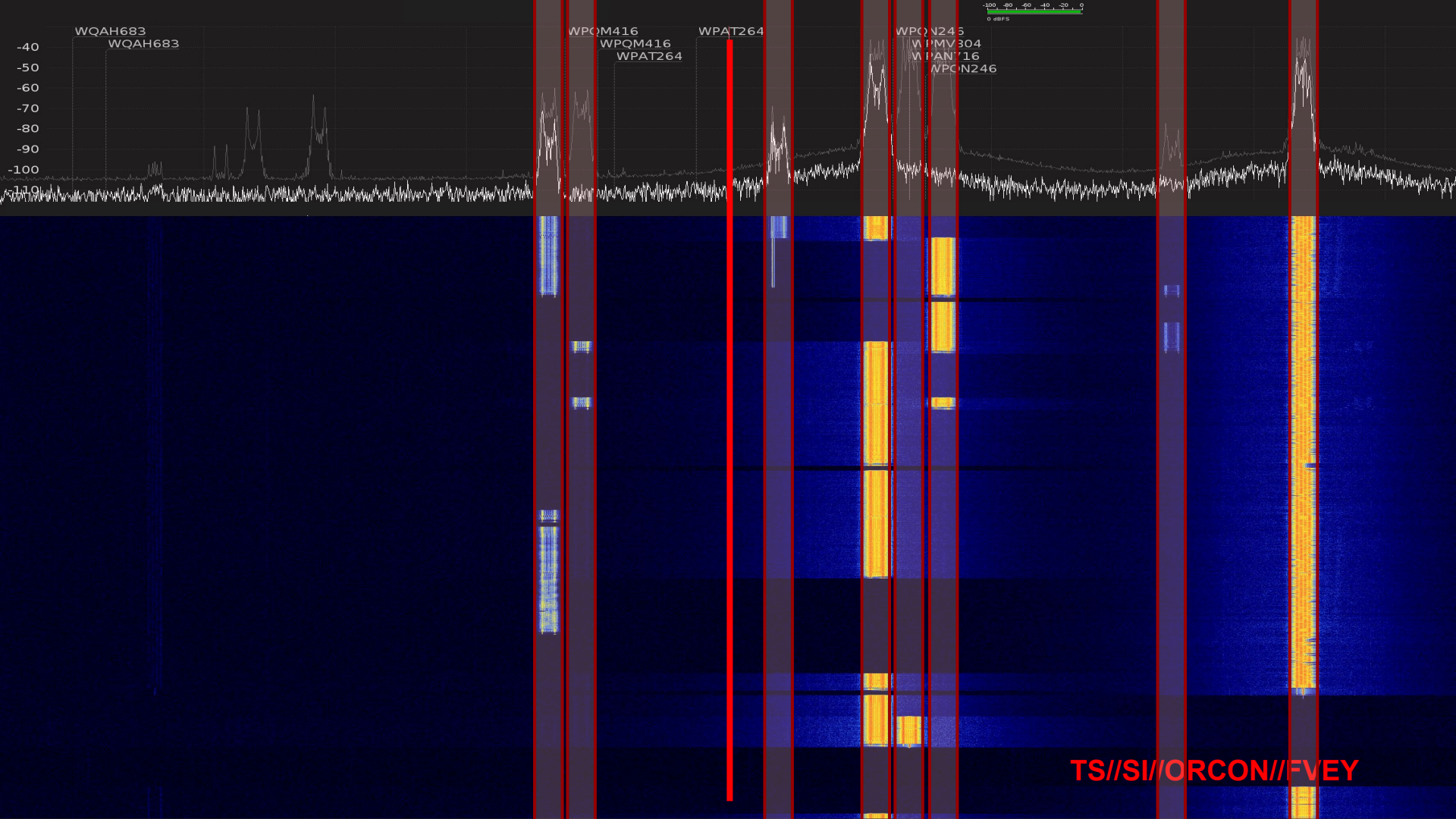
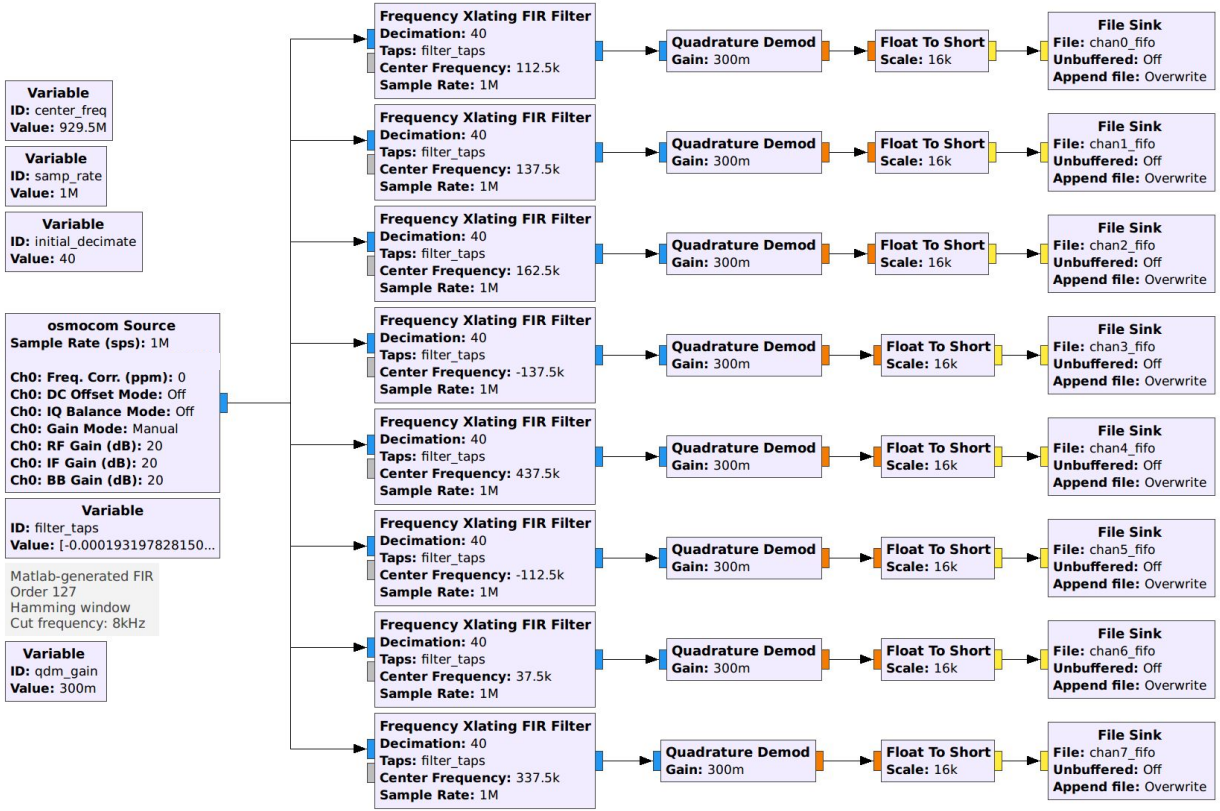


Figure 2: Magnitude Response (dB)




Time (secs)
Frequency (MHz)
Power/frequency (dB/Hz)
Time (secs)
Frequency (MHz)
Power/frequency (dB/Hz)


WQAH683
WQAH683
WPQM416
WPQM416
WPAT264
WPAT264
-40
-50
-60
-70
-80
-90
-100
-110
TS//SI//ORCON//FVEY



The **USRP** can cost well over $1000 though...


RTL-SDR.COM
QUICKSTART SETUP GUIDE: RTL-SDR.COM/QSG
DVB-T+DAB+FM+SDR
RTL2832U R820T2 TCXO+BIAS T+HF
V.3
RTL-SDR.COM
QUICKSTART SETUP GUIDE: RTL-SDR.COM/QSG
DVB-T+DAB+FM+SDR
RTL2832U R820T2 TCXO+BIAS T+HF
V.3
RTL-SDR.COM
V.3
RTL-SDR.COM
V.3

Pulse
H1102NL
orange pi

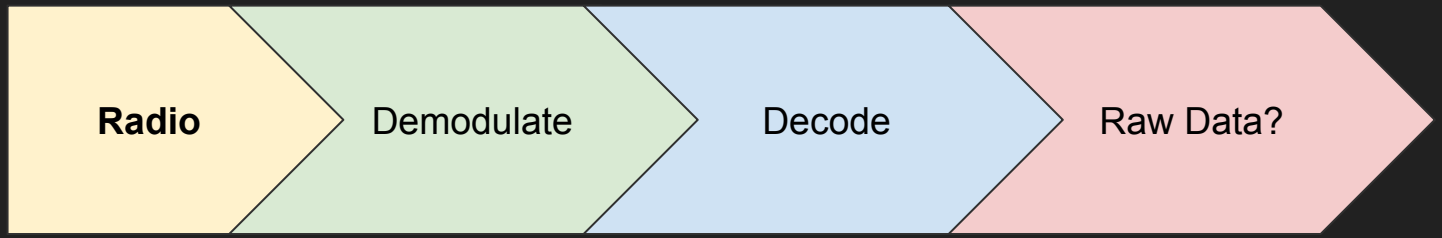
Equipment Costs

Item	Cost	Cumulative
Raspberry Pi/Orange Pi	$35.00	$35.00
Raspberry Pi/Orange Pi Case	$7.00	$42.00
CanaKIT 2.5A Power Supply	$9.99	$51.99
NESDR SMArt + Antenna Kit	$25.95	$77.94
** You might want to add an LNA to the mix, for maximum performance. Your extra $22.06 gets you this.*	**TOTAL**	**$77.94**

MultiFM

An efficient and compact channelizer for RTL-SDR, USRP and Airspy

- Split the spectrum into n even channels, centered where specified by user
- Fairly sophisticated fixed-point DSP
- Supports user-specified filters and gains per channel
- Supports sampling rates up to 6Msps on a Raspberry Pi, filtering is optimized using NEON SIMD when on ARM
- Flexible as all (maybe too flexible), uses JSON to express configuration
- Dumps 16-bit PCM samples out to a specified file, easy for other applications to pick up

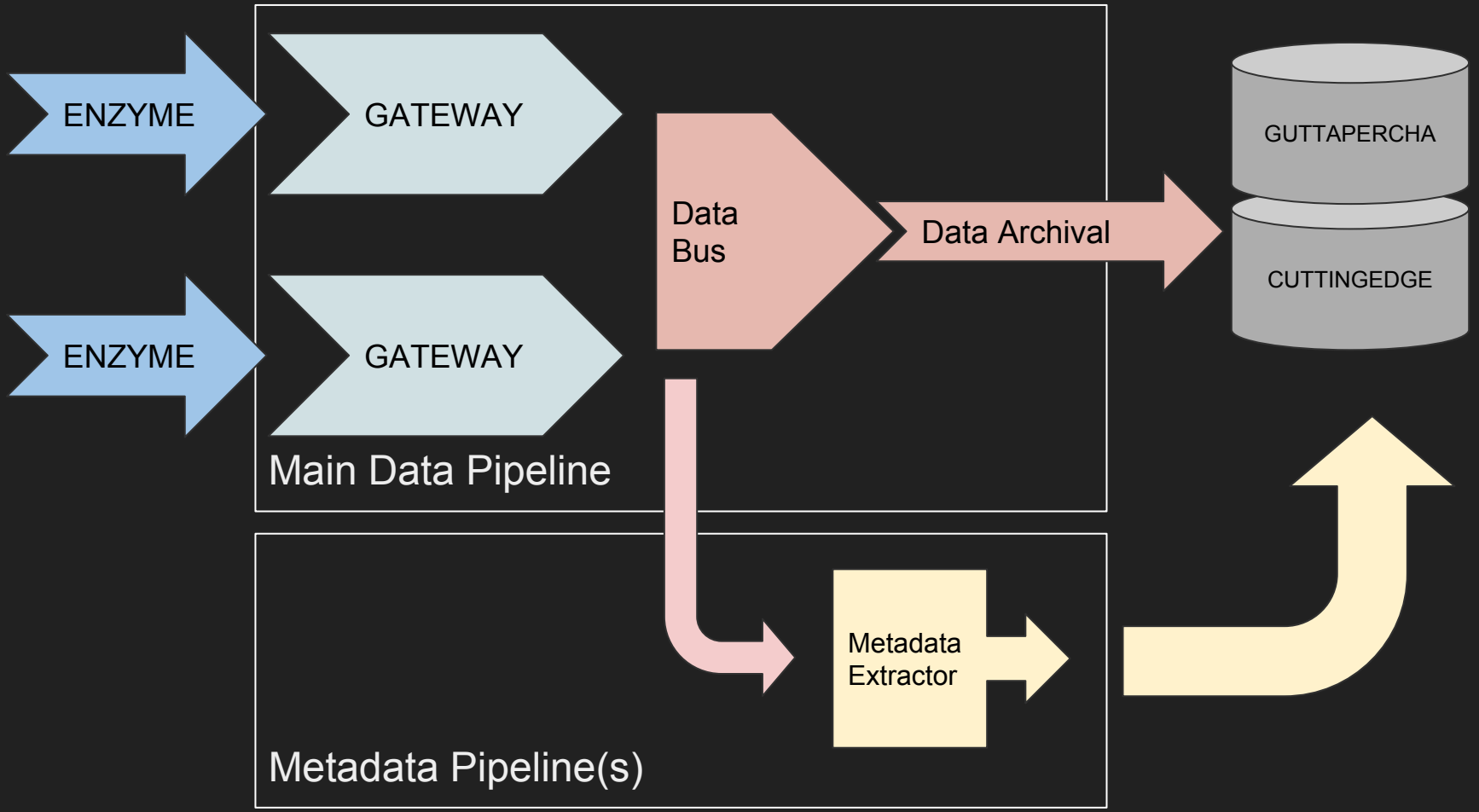


??

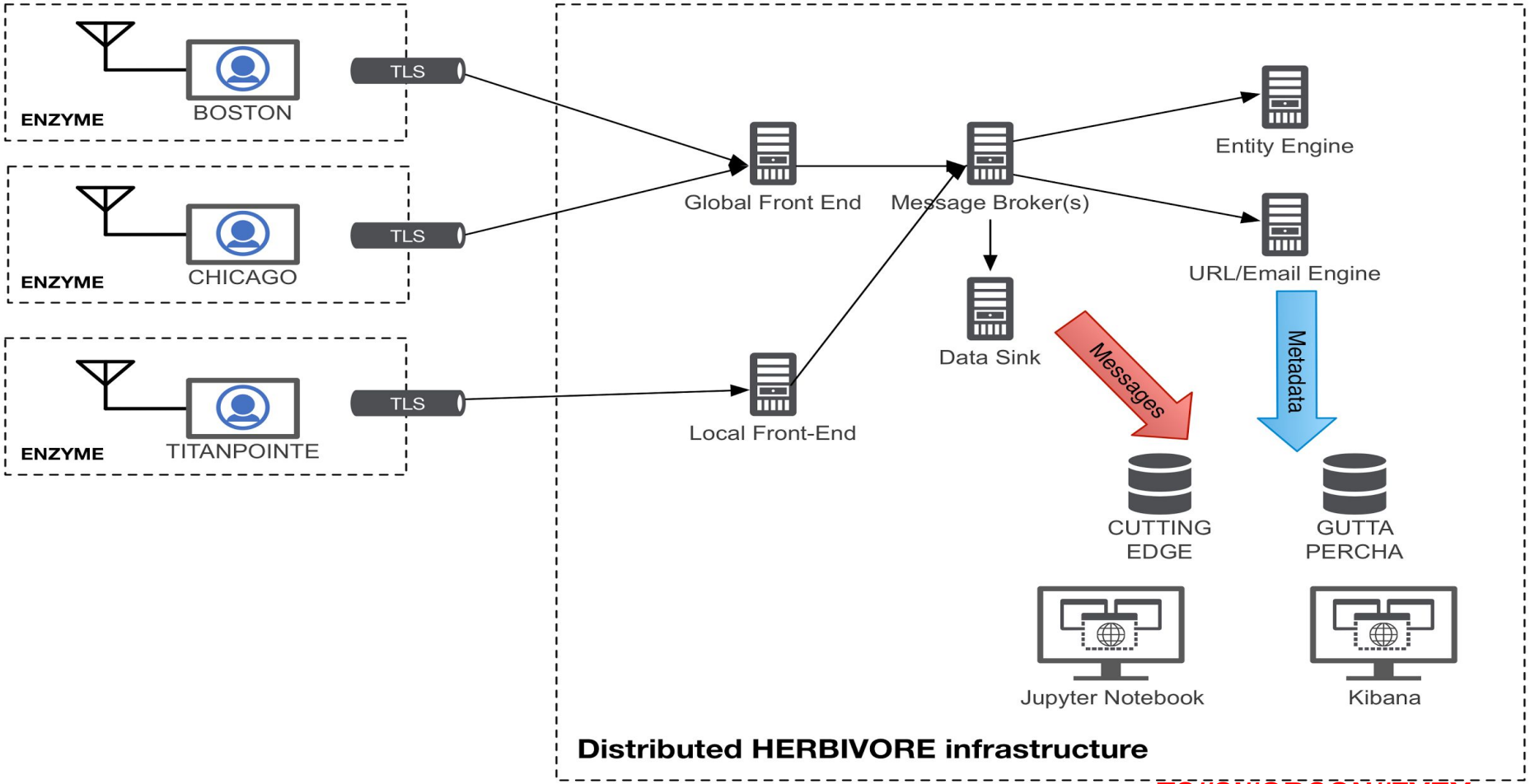
HERBIVORE

HERBIVORE infrastructure

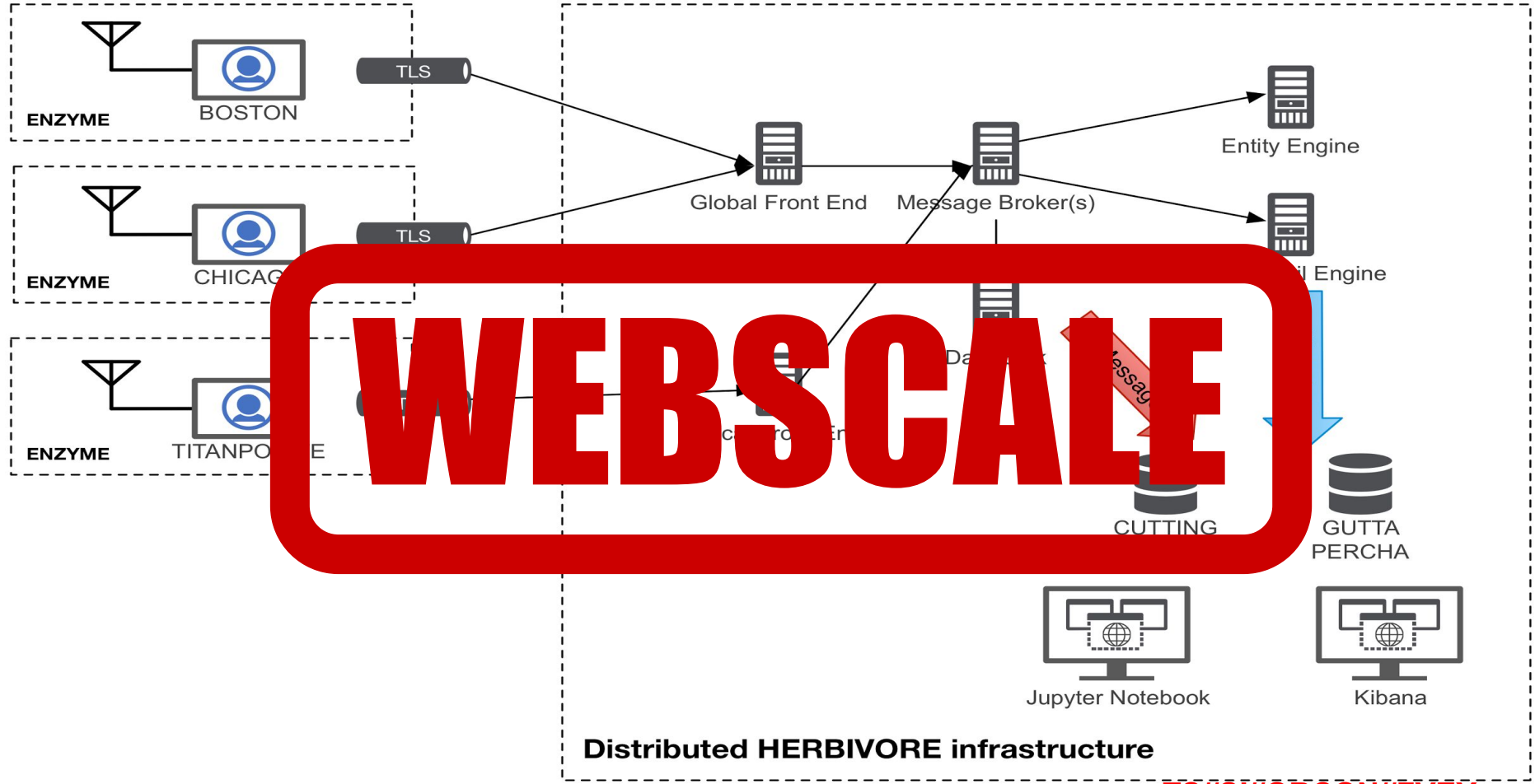
- **ENZYMEs** which converts decoded messages from a variety of sources into messages to be consumed
  - Many Sources: AIS, LRIT/HRIT are original sources. Also can collect from online sources (Twitter, Facebook, Instagram, etc.).
- **HERBIVORE** which ENZYMEs are configured to connect to, delivering messages to the infrastructure
  - Consists of message gateways that feed messages to brokers, that deliver messages to various metadata analysis pipelines
  - Messages eventually are delivered to the final sinks.
- **GUTTAPERCHA** and **CUTTINGEDGE**, two data stores that will archive received messages and make them accessible for analysis.
  - **GUTTAPERCHA** uses Elasticsearch
  - **CUTTINGEDGE** is a specialized Postgres schema



TS//SI//ORCON//FVEY



TS//SI//ORCON//FVEY



Common message schema

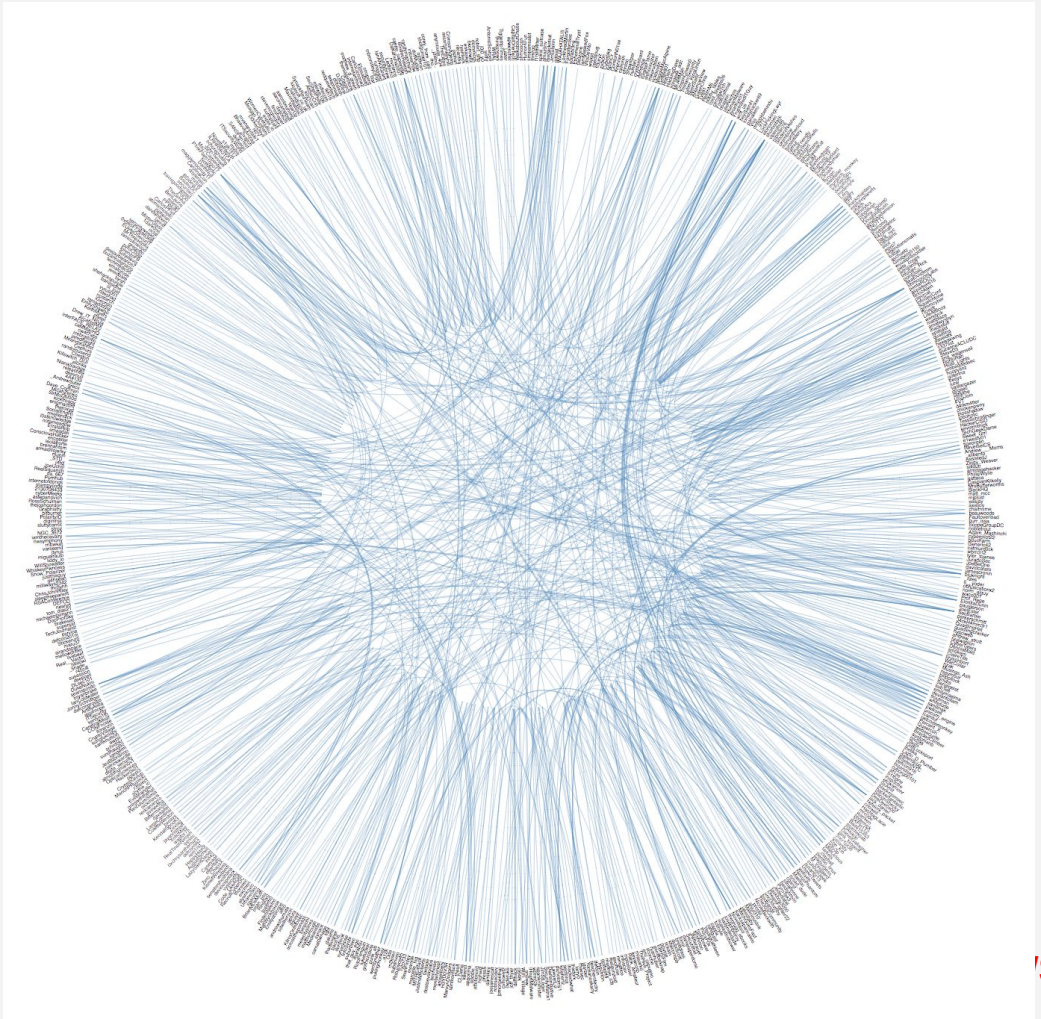

```
"version":0,
"msg":"Hi #shmoocon here\'s the repo if you want to mess with SPACECRAB https:\\/\\/t.co\\/S9jWNUZ1W7 - thanks :)",
"proto":"twitter",
"id":954829976263712770,
"metadata":{
        "urls":["https:\\/\\/bitbucket.org\\/asecurityteam\\/spacecrab"],
        "reply_to_status_id":954799311392473090,
        "hashtags":["shmoocon"],
        "user":{
                "id":39981605,
                "screen_name":"danoot"
        },
        "reply_to_user_id":39981605,
        "reply_to_screen_name":"danoot"
},
"timestamp":"2018-01-20 21:36:20 UTC"
```

Pipeline Configuration

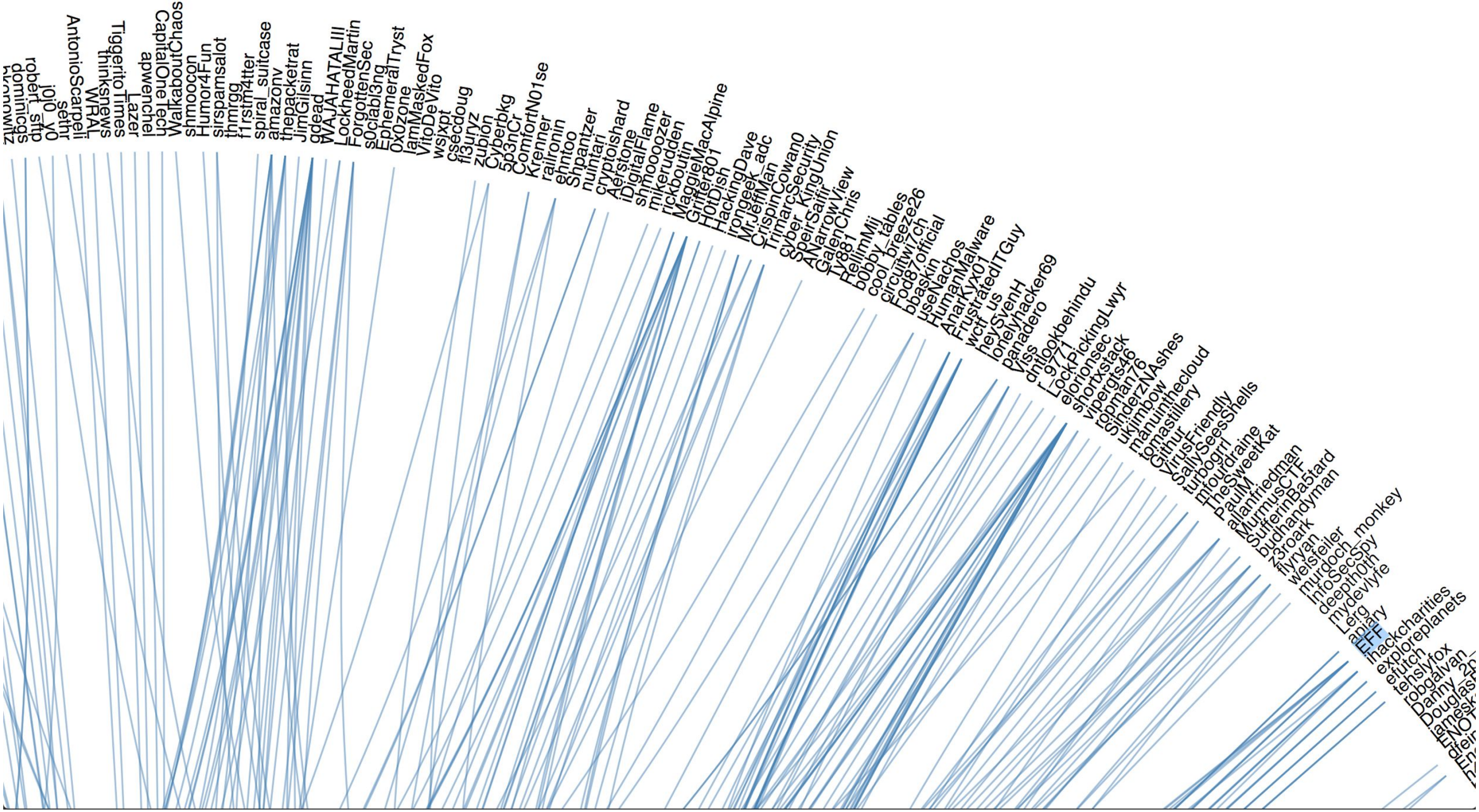
- Syntax JSON
- Stages are numbered
- Independent configs, independent processes
- Built to encourage experimentation

```
{
  "name" : "TwitterSource",
  "msgHandler" : {
    "handlerName" : "TwitterMsgHandler",
    "token" : "YOUR_SPICY_TOKEN_HERE",
    "token_secret" : "YOUR_SPICY_TOKEN_SECRET_HERE",
    "consumer_key" : "YOUR_SPICY_CONSUMER_KEY_HERE",
    "consumer_secret" : "YOUR_SPICY_CONSUMER_SECRET_HERE",
    "data_version" : 1,
    "twitter_tags" : "34C3,shmoocon,nsstorm,zuma,spacex",
    "twitter_ids" : "",
    "twitter_lru_size" : 1663,
    "twitter_ignore_rt": true
  },
  "pipeline" : [
    {
      "stageId" : 1,
      "stageName" : "ConsoleSink"
    }
  ]
}
```

What do I use all of this for?!



SI//ORCON//FVEY


dominicgs
robert_sftp
j0j0_y0
sethr
AntonioScarpeli
WRAL
thinksnews
TiggeritoTimes
Lazer
apwenchel
CapitalOneTech
WalkaboutChaos
shmoocon
Humor4Fun
sirspamsalot
thmrgg
f1rstm4tter
spiral_suitcase
amazonv
thepacketrat
JimGilsinn
gdead
WAJAHATALIII
LockheedMartin
ForgottenSec
s0ciabl3ng
EphemeralTryst
0x0zone
IamMaskedFox
VitoDeVito
wsjxpt
csecdoug
fl3uryz
zubion
Cyberbkg
5p3nCr
ComfortN01se
Krenner
railronin
ehntoo
Shpantzer
nuintari
cryptoishard
Aerstone
iDigitalFlame
shmooooozer
mikerudden
rickboutin
MaggieMacAlpine
Grifter801
H0tDish
HackingDave
irongeek_adc
MrJeffMan
CrispinCowan0
TrimarcSecurity
cyber_KingUnion
SpeirSaffir
ANarrowView
GalenChris
Ty881
RellimMij
b0bby_tables
cool_breeze26
circuitwi7ch
Fod87official
bbaskin
useNachos
HumanMalware
AnarKyx01
FrustratedITGuy
wctf_us
heySvenH
lonelyhacker69
panadero
Viss
dnilookbehindu
r_9771
LockPickingLwyr
elorionsec
shortxstack
vipergts46
ropman76
sinderzNAshes
ukjimbow
manuinthecloud
tomastillery
Githur
VirusFriendly
SallySeesShells
turbogrrl
mfourdraine
TheSweetKat
PaulM
allanfriedman
MurmusCTF
SufferinBa5tard
budhandyman
z3roark
flyryan
welsfeiler
murdoch_monkey
InfoSecSpy
deepth0th
mydevlyfe
Lerg
apiary
EFF
ihackcharities
exploreplanets
efutch
tehslyfox
robgalvan_

All AIS Ship Sightings - Chromium

All AIS Ship Sightings

localhost:8080/jupyter/notebooks/All%20AIS%20Ship%20Sightings.ipynb

jupyter All AIS Ship Sightings Last Checkpoint: Last Sunday at 9:51 PM (autosaved)

Logout

File Edit View Insert Cell Kernel Help

Trusted Python 3

Run Code

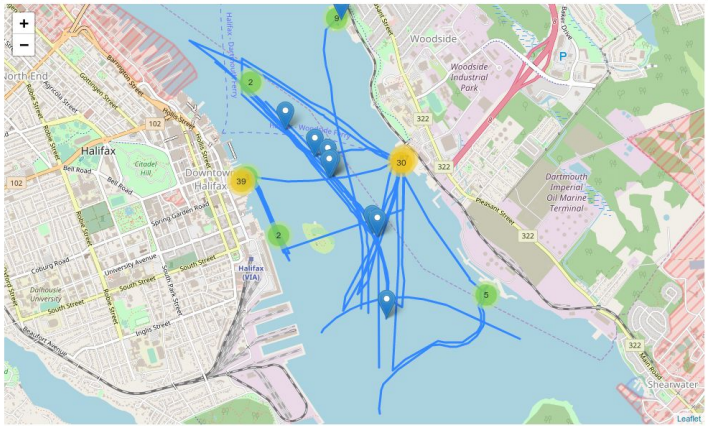
Out[122]:

	callsign	mmsi	name	nrMsg5	shipType
0	Unknown/No Msg5	316278000	Unknown/No Msg5	0	Unknown/No Msg5
1	CFH8958	316009640	ATLANTIC FIR	32	52
2	CFK9798	316013940	ATLANTIC CONDOR	1	70
3	C6ZJ7	311057100	CSL TACOMA	1	70
4	SVAX9	240991000	FOURNI	2	80
5	CFH8937	316002800	ATLANTIC WILLOW	89	52
6	CGDN	316133000	CORIOLIS II	1	99
7	CFA2372	316003090	RV LEEWAY ODYSSEY	9	90
8	2JHW9	235116052	ATLANTIC SEA	2	71
9	Unknown/No Msg5	316024142	Unknown/No Msg5	0	Unknown/No Msg5
10	VAAP	316009560	ALGOSCOTIA	5	82
11		316035161	NOVA PILOT	39	53
12	88	316035162	SCOTIA PILOT	5	53

In [123]:

```
1 bounds = info_layer.get_bounds()
2 location = [(bounds[0][0]+bounds[1][0])/2, (bounds[0][1] + bounds[1][1])/2]
3 m = folium.Map(location=location)
4 m.add_child(info_layer)
```

Out[123]:



In [ ]:

TS//SI//ORCON//FVEY

Who does this?

1. Red Teams


2. Nation States
ССВ-175

Wiretapping Laws in the US

- Receive only messages that you're authorized to:
  - Messages that are destined for you, or
  - Messages relating to tracking airplanes and boats (i.e. ADS-B and AIS), or
  - Messages that the recipient(s) have authorized you to receive, or
  - Messages that are intended for the public (i.e. broadcast)
- Do not use this software for evil!
- Consult a lawyer if you're unsure you're authorized.

TS//SI//ORCON//FVEY

Shoutouts

- **Postgres, Elastic, Jupyter** - you all are amazing
- **4F** - you all know who you are
- **Joey** - someday you'll get a handle, bruh
- **The Five Eyes**
- **GNURadio** - awesome tool

Find Us

github.com/pvachon

Phil: keybase.io/hoobdwarp

Andrew: keybase.io/nop


Can’t stop the signal, Mal
Questions?
TS//SI//ORCON//FVEY