#IntelCon2020

IntelCon
by Ginseg

Matrioshka SIGINT: Análisis de señales “ocultas”

David Marugán
@RadioHacking

Congreso Online de Ciberinteligencia
Julio 2020

- Manager en **ANADAT**
- Instructor EC-Council CEH.
- Mundo Hacker Team.
- “Radiotranstornado”, desde edad muy temprana.
- Miembro de la Emergency Response Unit (ERU) IT & Telecom Cruz Roja.
- “Aprendiz constante” de técnicas SIGINT caseras.
- **Experto en absolutamente… nada**.
- **No me dan alergia las “ondas”, ni llevo en la cabeza papel de aluminio**, ni remedios homeopáticos contra emisiones “nocivas” y… ¡Todavía estoy vivo! ☺
- **Odio los efectos y transiciones en los PowerPoint**.

IntelCon
by Ginseg

¿Qué tienen en común los submarinos nucleares, las tarifas eléctricas, la BBC de UK y los brokers de Wall **Street**...?

Congreso Online de Ciberinteligencia | Julio 2020

¿Qué veremos en esta charla?

- ¿Qué es **SIGINT** y qué trabajo realiza un analista de señales? ¿qué **herramientas** utiliza?
- La señal del **"Buzzer" ruso** y algunas novedades.
- Análisis de las **señales CIS 36-50**, BEE-36, T600.
- ¿Qué esconden los programas de **la BBC4** que transmite desde UK?
- ¿Por qué le interesa la transmisión en Onda Corta a Wall Street?: **HF y los "brokers" de Bolsa.**
- **Inteligencia Acústica ACINT**, los IDS del mar…

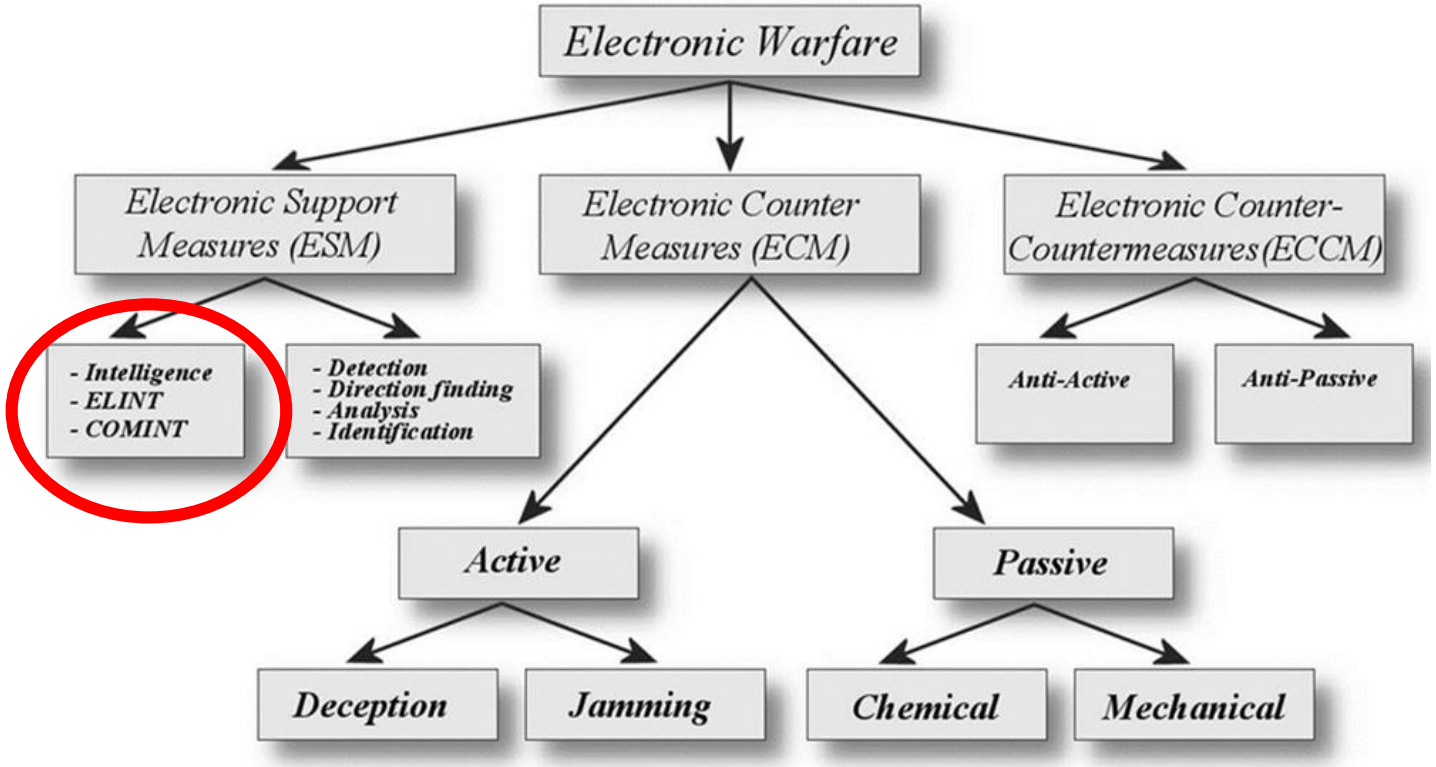
¿Qué NO veremos en esta charla?:

"¡¡Cómo escuchar a la POLICÍA…!!"

DEFINICIÓN SIGINT

SIGINT(Inteligencia de Señales):

- **Inteligencia de comunicaciones (COMINT)**: supone la utilización de toda clase de comunicaciones conocidas, como GSM, la radio, Internet, etc.
- **Inteligencia electromagnética (ELINT)**: NO Comunicaciones. Supone la utilización de campos eléctricos y campos magnéticos: radares, jammers, etc.
- **Inteligencia telemétrica (TELINT):** su función es la detección de imágenes, medidas y radiaciones mediante imágenes ópticas.
- Etc



SINGINT, COMINT...BLA BLA

lo que imaginamos: NSA style...

"Made in Spain" SIGINT!

¿QUÉ HACE UN ANALISTA DE SEÑALES?

El analista de señales **intenta extraer el máximo de información de una señal**, realizándose preguntas como:

- ¿Qué tipo de señal es? ¿**está catalogada** ya?
- ¿Está **cifrada**? ¿Qué **modulación y parámetros** podemos observar?
- ¿Cuál es su **procedencia**? ¿Quién la opera? ¿desde dónde?
- ¿Cuál es su **destinatario final**?
- ¿Qué **objetivo** tiene?
- ¿Se puede relacionar con algún **evento específico en el tiempo**?
- El producto o **informe SIGINT**.

Algunos **FALSOS MITOS** entorno al analista de señales:

- **El analista analiza la señal a nivel técnico** con la intención de **transformar su análisis en un producto SIGINT** válido a otros niveles.
- **El analista de señales NO es un criptoanalista**, y la mayor parte de las veces no decodifica ni conoce la información que contiene la señal que estudia.
- En muchas **ocasiones se debe apoyar en otras disciplinas como el HUMINT, OSINT**, etc.
- Es imprescindible trabajar OFFLINE con grabaciones de calidad. **Un analista no puede realizar su trabajo con una mala grabación**.

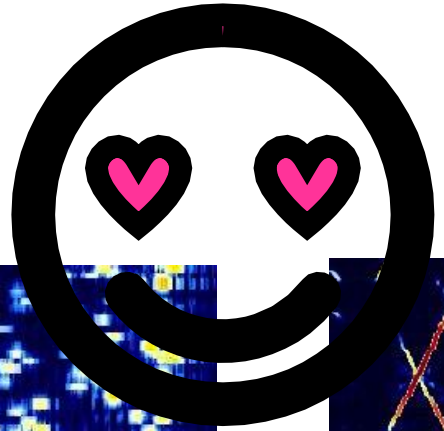
¿POR QUÉ ANALIZAR SEÑALES RF EN EL SIGLO XXI?

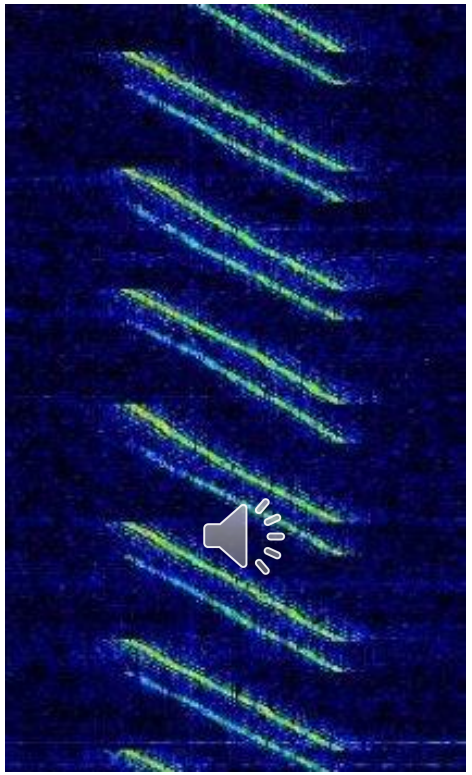
- **El espectro radioeléctrico está lleno de señales de gran interés** hoy día, no solo a nivel de SIGINT militar.
- A nivel de COMINT **podemos encontrar todo tipo de señales de radio interesantes como fuente de inteligencia,** como por ejemplo: estaciones diplomáticas, servicios de inteligencia, comunicaciones militares, emisiones clandestinas, etc.
- Aunque cada vez la tarea de análisis de señales está mas automatizada, **sigue siendo imprescindible contar con analistas** formados y especializados.
- El despliegue de las **tecnologías para IoT o el TSCM** implica también su conocimiento en el ámbito de la seguridad en “el mundo civil”.

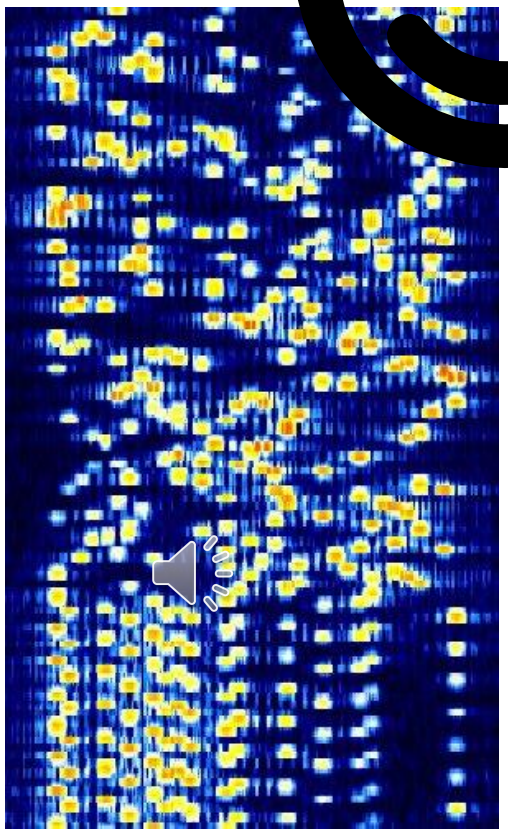
Captura video tras atentados De Paris, donde se ve a un terrorista portando un equipo de radio DMR de alta gama, posiblemente usando cifrado. + Info: https://www.securityartwork.es/2015/12/18/inseguridad-en-radiocomunicaciones/

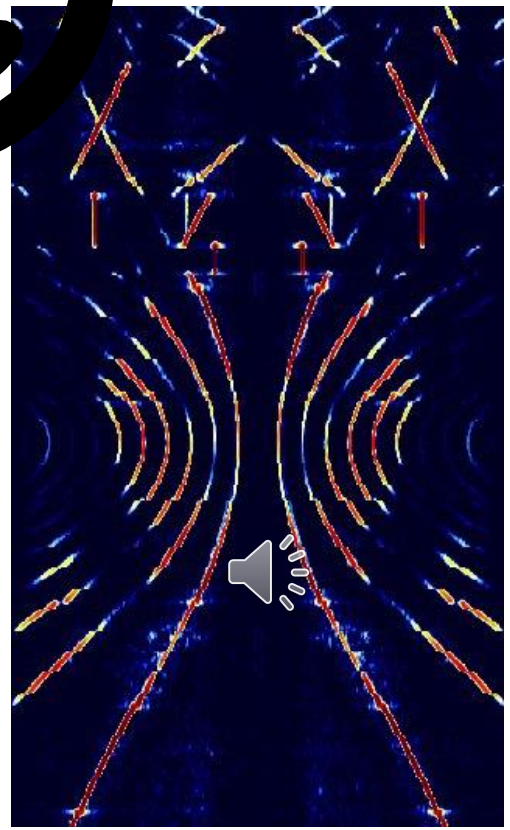
¿QUÉ HACE UN ANALISTA DE SEÑALES?

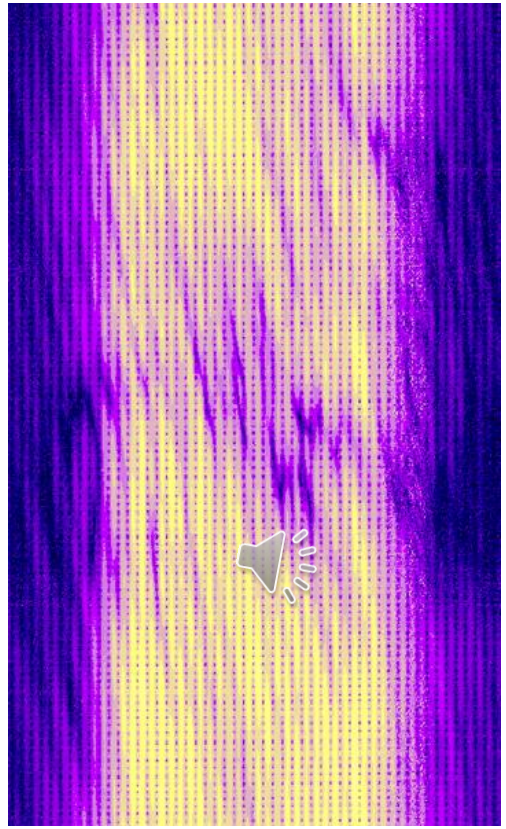
AUDIOS EJEMPLO.
Y además son bonitas LECHE!!...











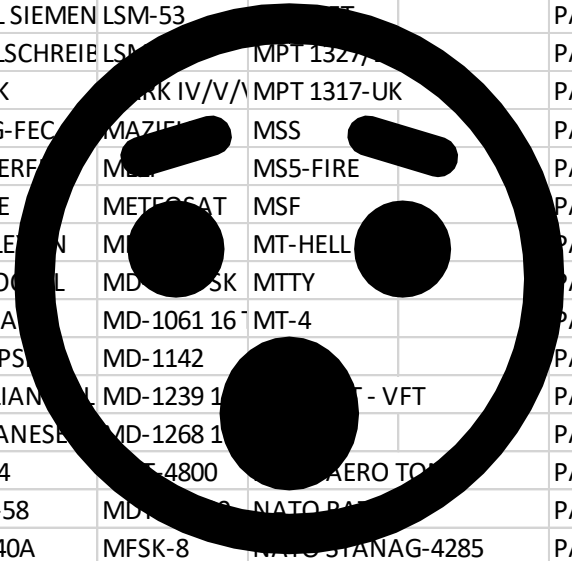
Imágenes de ejemplo de SIGIDWIKI
https://www.sigidwiki.com/

¿QUÉ HACE UN ANALISTA DE SEÑALES?

IntelCon
by Ginseg

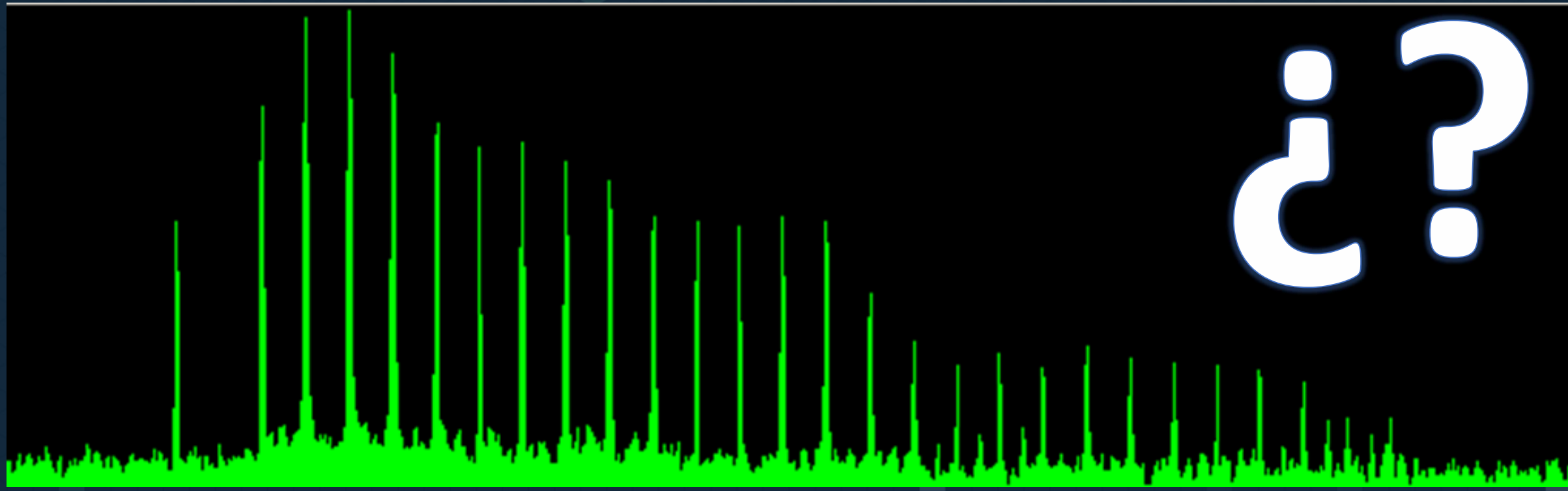
#IntelCon2020

108.86 FEC-S	ANNEX 10	AUTOSPEC II	CIS-96	CV-786 FSK	FAF SYSTEM	G-TOR	LINK-11B	MIL STD-2500		NORTH KOREAN DIPLO	POR-VFT	REFLEX	SPREAD-11	SSTV SC-2 12	YUG DIPLO
1200-FSK	APOC	BAUDOT	CIS-100	CW MORSE	FARCOS SYST	HARRIS-ALE	LINK-11 Seria	MMP-4800		NUM 13	PRESS-FAX	ROU-MOI FE	SPREAD-21	SSTV SC-2 18	YUG 20 To
1200-PSK STA	APOR-VFT	BAUDOT 1 St	CIS-150	CZECH-2400	FAX	HARRIS 39	LINK-14	MOBITEX		OTHR SYSTEM	PSK-HELL	ROCKWELL-4	SPREAD-51	SSTV SC-2 20	ZL F
1600-PSK	APRS	BAUDOT 1,5	CIS-200	DCF 77	FAX FRENCH	HAVE QUICK	LINK-16	MOTOROLA		PACKET-HF (Radioaficona	PSK-105-HEL	RS 8Tone AR	STATUSBOX	SSTV Scottie	ZETRON 6/
1800-PSK	ARAMIS R&S	BAUDOT 2 St	CIS-300,5	DDS-4800	FAX 480	HC-ARQ	LINK-22	MODAT		PACKET V/UHF (Radioafic	PSK-245-HEL	RS-ALIS v1	SSR	SUI-FEC	ZVEI-I
2400-PSK	ARES	BAUDOT F7B	CIS-1200	DGPS	FEBEKO	HCLOS	LOJACK	MOI-ROMA		PACT	PSK-MIL STA	RS-ALIS v2	SSTV Autom	SWED-ARQ	ZVEI-II
2-BPSK	ARCOTEL-ALI	BR 6028	CIS-1280	DGPS/DATA	FEC-A	HELL SIEMEN	LSM-53			PACTOR-ARQ	PSK-MIL STA	RS-2400 PSK	SSTV AVT B&	SWED-DIPLO	ZVEI-
2-DPSK	ARQ6-70	BUL-39 Tone	CIS- 3x100 VF	DCS	FEC-S	HELLSCHREIB	LSM	MPT 1327/		PACTOR-FEC	PSK-MIL STA	RUM-FEC	SSTV AVT 24	SWEDISH MBS	
36-50	ARQ6-90	BULG-ALE	CIS- 3x144 VF	DMB	FELD-HELL	HFSK	RK IV/V/	MPT 1317-UK		PACTOR-GLOBE WIRELESS	PSK-MIL STA	RUS-144 FEC	SSTV AVT 90	TADIL-C	
3-PSK	ARQ6-98	BULG-107 Ps	CIS- 3x BAUD	DTMF	FHSS	HNG-FEC	MAZIE	MSS		PACTOR-I 1	PSK-MIL STA	RUS DIPLO-2	SSTV AVT 94	TADIL-J	
4+4	ARQ-E	BULG-ASCII	CLOVER	DUP-ARQ	FLEET BROAD	HYPERF	ME	MS5-FIRE		PACTOR-I 2	PSK-MIL STA	RUS DIPLO-6	SSTV AVT 18	TADIRAN HF-DATA Mod	
4-DPSK	ARQ-E3	BULG-DIPLO	CLOVER 400	DUP-ARQ II	FLEX	IMBE	METEOSAT	MSF		PACTOR-I 3	PSK-MIL STA	RUS DIPLO-F	SSTV HQ1	TE-204 FSK	
81-29	ARQ-M2-242	CABMASTER	CLOVER 500	DUP-FEC 2	FM-HELL	INFLE	MI	MT-HELL		PACTOR-I 4	PSK-MIL STA	RUS -INTEL V	SSTV HQ2	THOMSON 8-FSK	
81-40.5	ARQ-M2-342	CCIR-7	CLOVER MAF	DUPLO-HELL	FMS-BOS	INFO	MD	MTTY		PACTOR-I 5	PSK-MIL STA	RUS- CHIRP	SSTV Martin	THROB	
81-81	ARQ-M4-242	CCIR-I	CLOVER 2000	EAS	FNL BURST	IRA-A	MD-1061 16	MT-4		PACTOR-I 6	PSK-MIL STA	RUS PARALLE	SSTV Martin	TMS 430	
ACARS-HF	ARQ-M4-342	CCITT	CLOVER II	ECHOTEL-EA	FRENCH-300	ISR-PS	MD-1142			PACTOR-I 7	PSK-MIL STA	SATCOM-MD	SSTV P3	TPLEX	
ACARS V/UH	ARQ-N	CDPD	CMT	EEA/CCIR 2	FSK-CIS	ITALIAN	MD-1239 1	T - VFT		PACTOR II	PSK-MIL STA	SATURN	SSTV P5	TRACKER	
AEGIS	ARQ-S	CHINESE 32T	COBRA	EEA/CCIR 7	FSK-HELL	JAPANESE	MD-1268 1			PACTOR II FEC	PSK-QAM ST	SAT-A-TELEX	SSTV P7	TT2300B	
ARCOTEL-18	ARS-GUARD	CHINESE MIL	CODAN 16	EFJ-LTR	FSK STANAG	JT-44	4800	AERO TO		PACTOR III	PSK-08	SAT-C-DATA	SSTV PD50	TURKISH-25 Tone	
ARCOTEL-24	ARTOR	CHINESE MIL	CODAN SELC	EIA	FSK-411	KFF-58	MD	NATO PA		PACTOR III / 16Tonos	PSK-63F	SCADA	SSTV PD90	TWINPLEX	
AES2	ASCII	CHINESE 240	CODAN 81	ELECTROCON	FSK-600	KG-40A	MFSK-8	NATO STANAG-4285		PAGER	PSK-125F	SLOW-FELD H	SSTV PD120	TWINPLEX-ARQ	
AES4	ASCII 10Bit A	CIS NAVY	CODEC	EMWIN	GAF 144 3Ch	KG-84A NAT	MFSK-16	NATO 100		PAKNET	PSK-31 BPSK	SMS	SSTV PD160	TWINPLEX BAUDOT	
ALADIN R&S	ASCII 11Bit A	CIS-11	COGNITO	EOTD	GERMAN MC	KG-84C NAT	MIL STD-110-	NATO 75		PAKTEL-CP100	PSK-31 QPSK	SINOP	SSTV PD180	UHFLOS-HDR	
ALF	ASCII-CZECH	CIS-14	COMPULERT	EPIRB	GE MARK-V	KG-87	MIL STD-188-	NATO 16 Tone		PANTHER-H	QAM	SITOR-A	SSTV PD240	UK-ARMY	
ALGERIAN-4T	ASCII-RUSSIA	CIS-27	COQUELET 8	EPLRS	GE-STAR	KG-94A	MIL STD-188-	NATO 39 Tone		PCM 30/E1	Q15x25	SITOR-B	SSTV PD290	UK-MIL 8Ch VFT	
ALGERIAN-8T	ASCII-SLOVA	CIS-36	COQUELET 13	ERMES	GL-HELL	KIV-19	MIL STD-188-	NEC/D3		PCS	RAC-ARQ	SKYFAX	SSTV Robot 2	UK-NAVY	
ALIS	ASTRO APCO	CIS-40.5	COQUELET 8	ET-1	GMDSS/DSC	KL-43	MIL STD-188-	NEXNET		PCW	RADIONICS S	SKYHOPPER	SSTV Robot 3	USC-11	
ALIS 8Bit	ATCS-SPEC20	CIS-73	COQUELET 8	ET-2	GMDSS/DSC	KRE-PSK	MIL STD-188-	NEXTEL		PICCOLO MK12	RAM Mobile	SOVIET 84	SSTV Robot 8	US INTEL	
ALIS-2	ATIS	CIS-75	COQUELET 8(	EURO	GN-150 FSK 3	KY-99	MIL STD-188-	NMT 450		PICCOLO MK6	RAMP	SP-14	SSTV SC-1 16	US INTEL FEC	
	AUM 13		COQUELET 8	F7B 195,3 4T	GNY SYSTEM	LINK-1	MIL STD-188-	NMT 900		PICCOLO VFT 2x20	RBDS	SKYPER	SSTV SC-1 24	US MIL 4Frec.	
	AUTOSPEC		CROWD 36 ISS		GOLAY	LINK-4	MIL STD-188-	NOAA-GEOSAT		PICCOTOR	RDS	SMT	SSTV SC-1 48	USAF Pseudo	



IntelCon
by Ginseg

EJEMPLO SEÑAL 1



EJEMPLO DE SEÑAL: “THE BUZZER” / MDZhB(*)

- **Apodada el “Buzzer”** o zumbador**, lleva transmitiendo desde principios de los 80** en 4.625 kHz USB. El sonido es un **Channel Marker**.
- Durante muchos años su señal ha consistido en un corto y **monótono zumbido, repetido con un promedio de 25 p.p.m durante 23 horas y 10 min. al día**.
- En ocasiones excepcionales **se han escuchado voces femeninas y masculinas de fondo**. Posiblemente varios transmisores.
- Todavía hoy se desconoce el objetivo “exacto” de las emisiones y esto genera todo tipo de especulaciones acerca de su propósito. **Todo apunta a un uso militar (Hub Distrito Occidental Rusia “Vulcan”, formato de mensajes Monolyth-Монолит).**

(*) de Mijail Dimitri Zhenia Boris

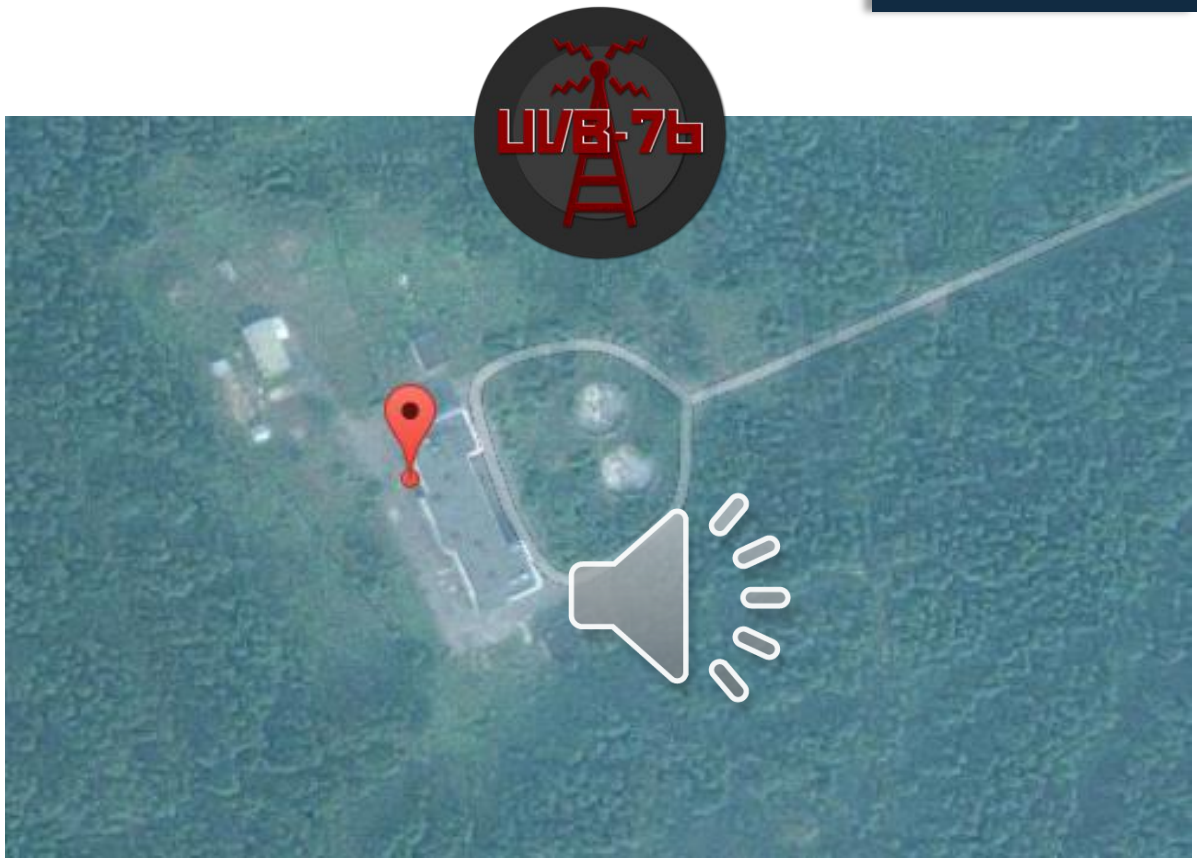
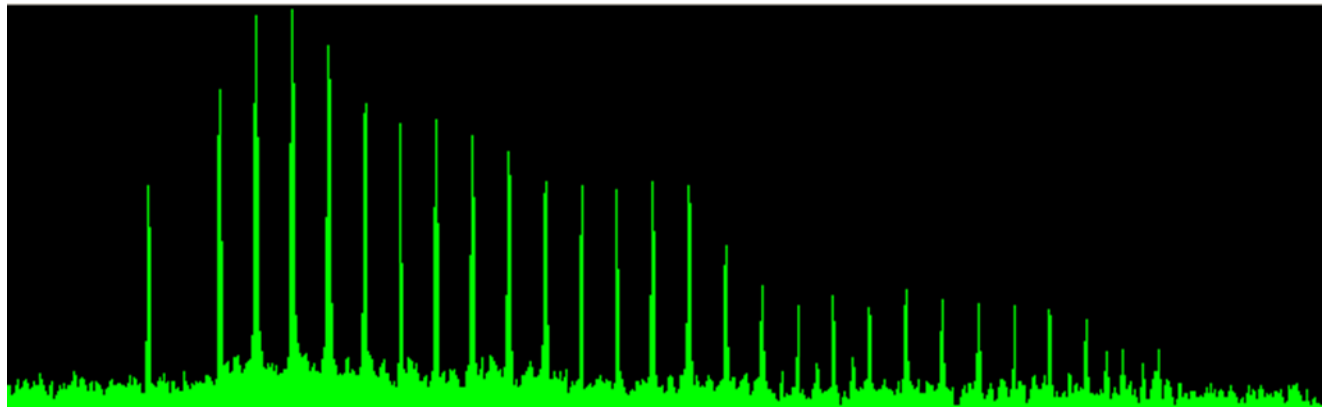


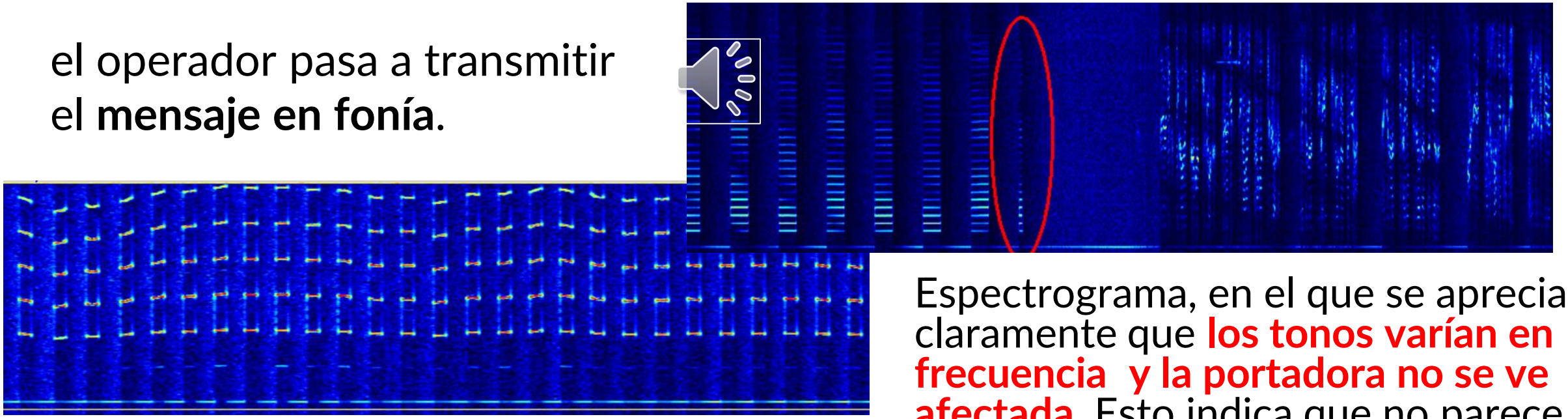
Imagen satélite Google de la antigua ubicación de la UVB-76 en un bosque de Povarovo, a unos 40 Km de Moscú. Actualmente se podría ubicar en el Oblast de Pskov y otros.

EJEMPLO DE SEÑAL: “THE BUZZER”



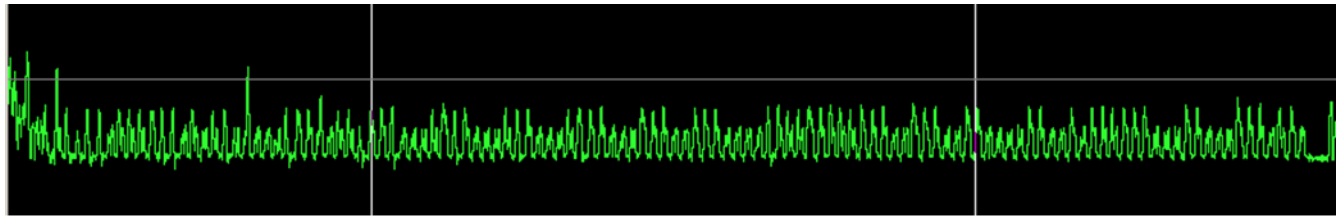
Este es el espectro típico de la señal. La portadora y unos **25 tonos separados unos 118,5 hz**.En este espectro se aprecian tonos simples y equidistantes

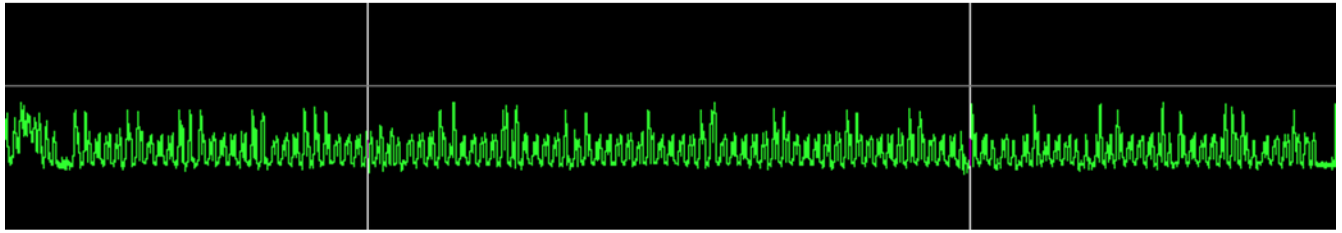
el operador pasa a transmitir el **mensaje en fonía**.

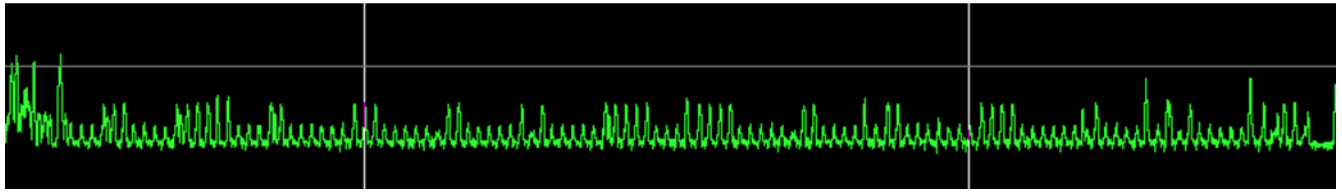


Espectrograma, en el que se aprecia claramente que **los tonos varían en frecuencia y la portadora no se ve afectada**. Esto indica que no parece que sea un efecto de la ionosfera.

EJEMPLO DE SEÑAL: “THE BUZZER”



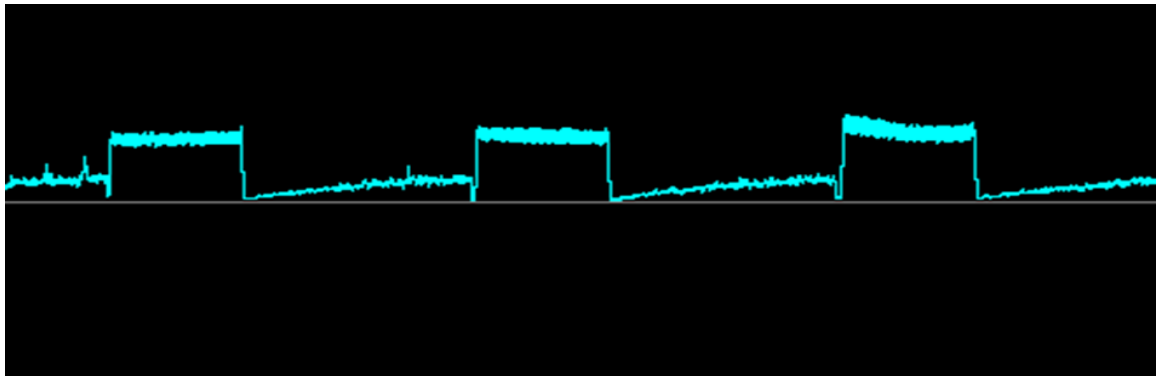


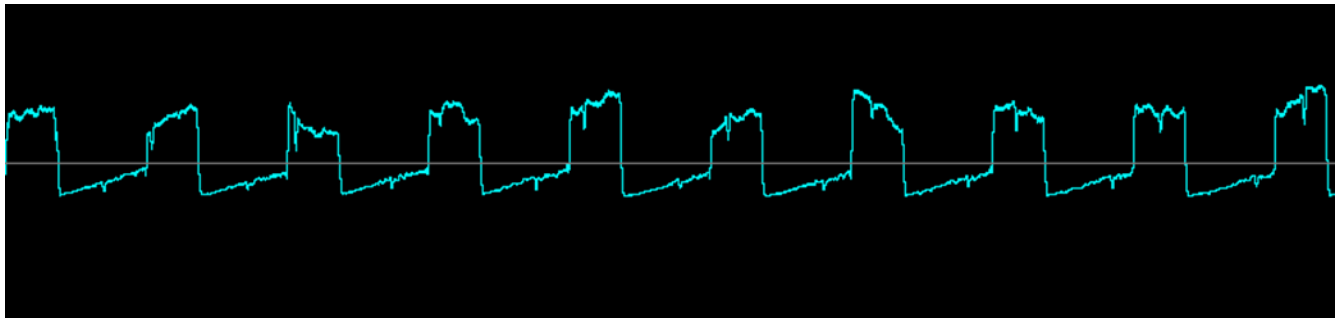


Demodulación de diferentes segmentos de la señal como ejemplo.

Envolvente típica y… ¿**Modulación en amplitud**? ¿Algún tipo de **PAM (Pulse-Amplitude Modulation)**? ¿Un “defecto” en el hardware?

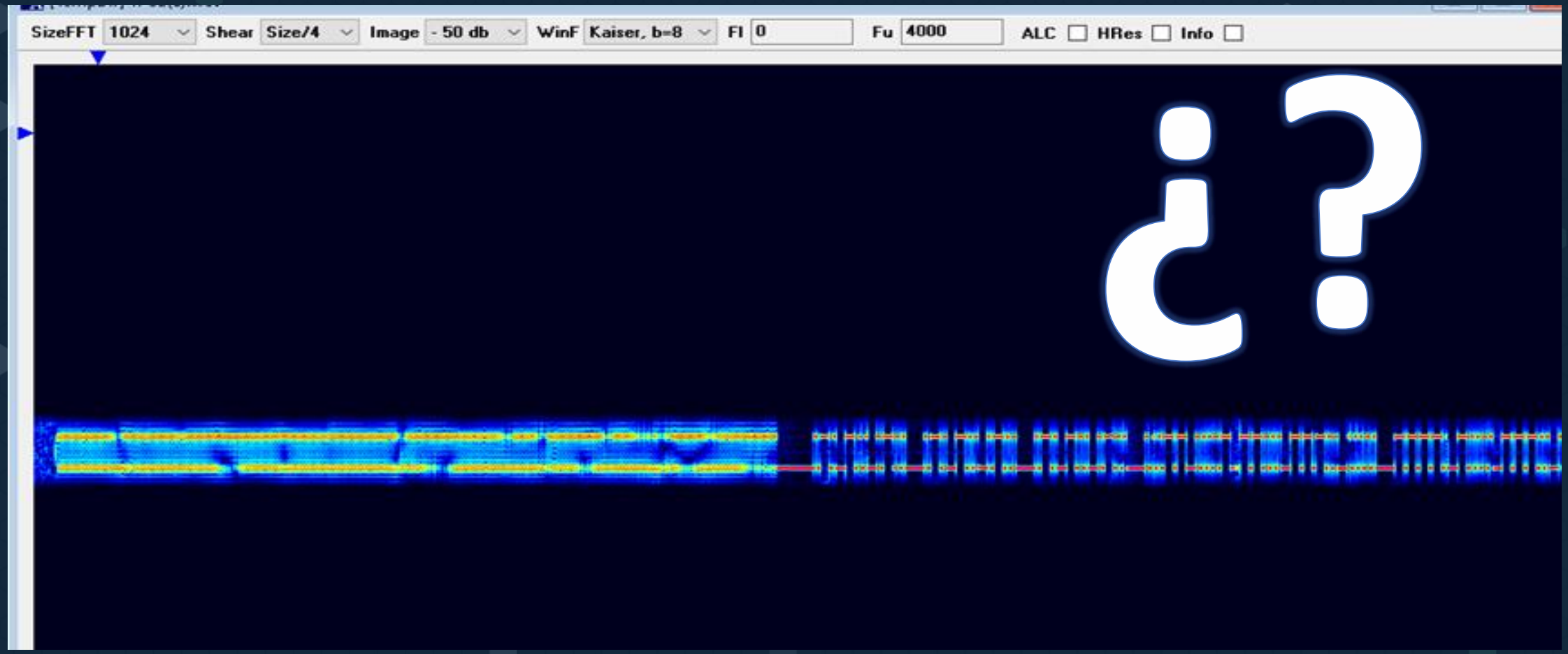
No está nada claro…





IntelCon
by Ginseg

EJEMPLO SEÑAL 2



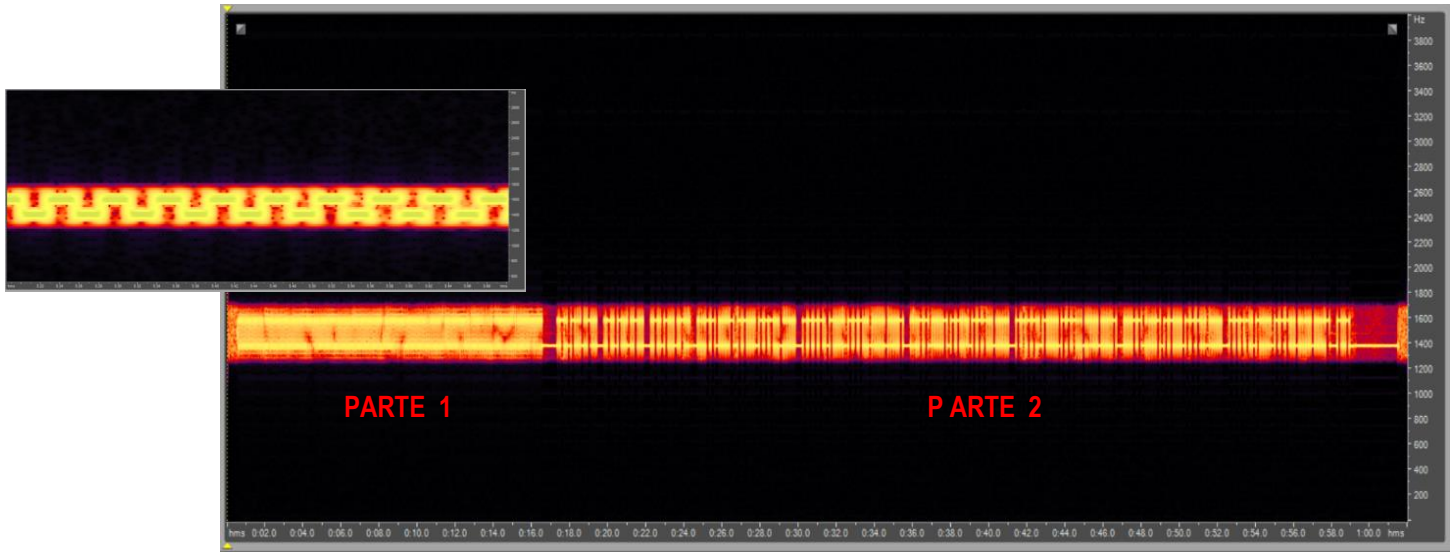
EJEMPLO DE SEÑAL: CIS 36-50 / T-600

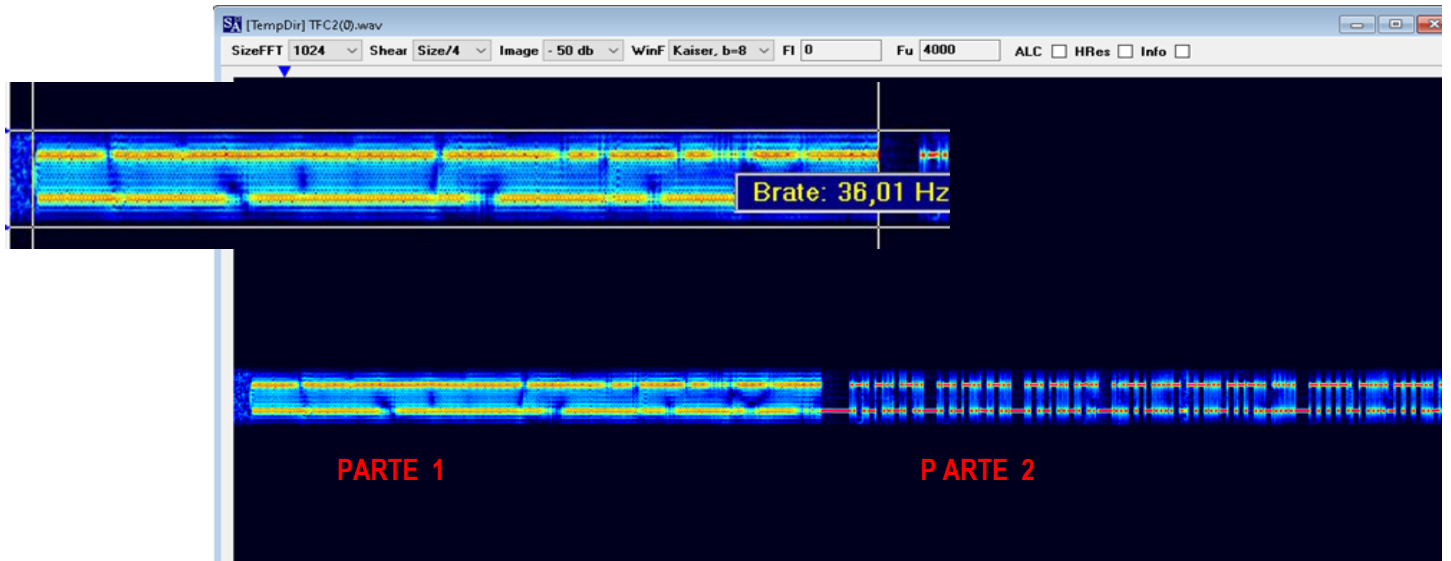
IntelCon by Ginseg

#IntelCon2020

Señal rusa denominada “CIS 36-50”

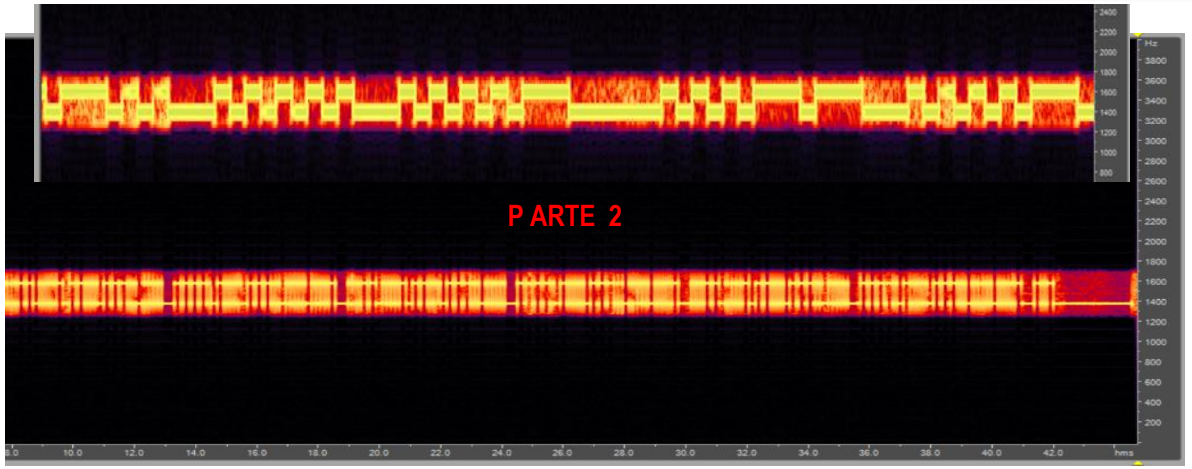
- **Modulación** 2FSK, 200Hz ancho de banda
- **Velocidad** 36 Bd / **28,56** Bd
- **Portadora** 1528,69 Hz
- **Velocidad de preámbulo** 36 Bd
- **PARTE 1**: Ocupación o IDLE a 36 Bd
- **PARTE 2**: TX datos **supuestamente a 50 Bd**

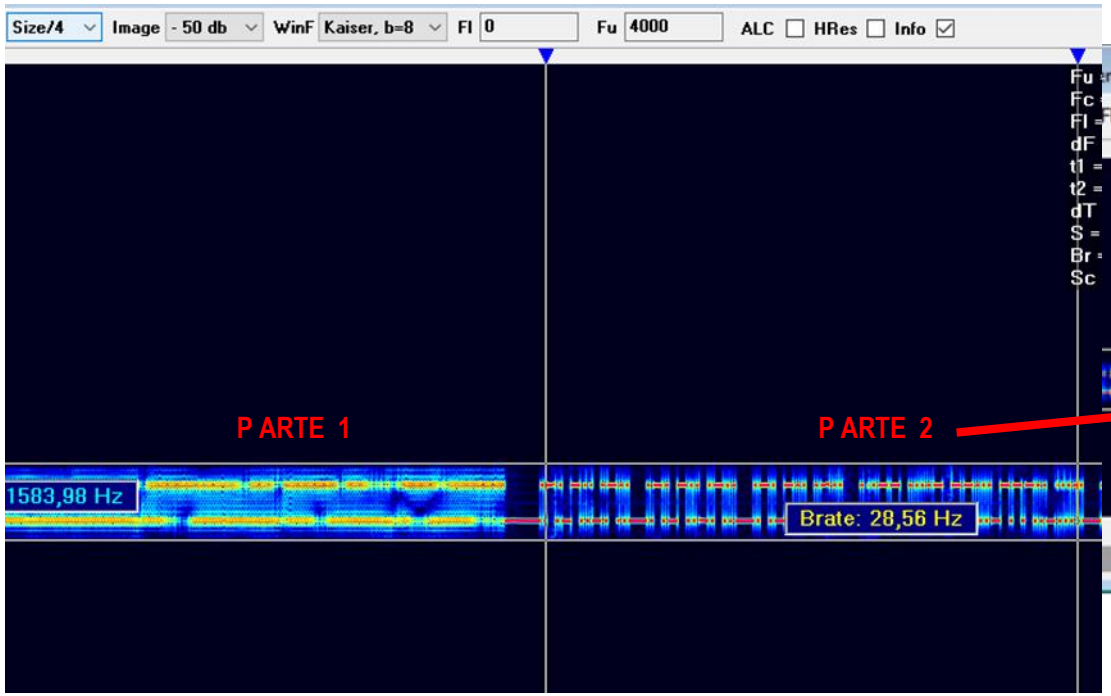


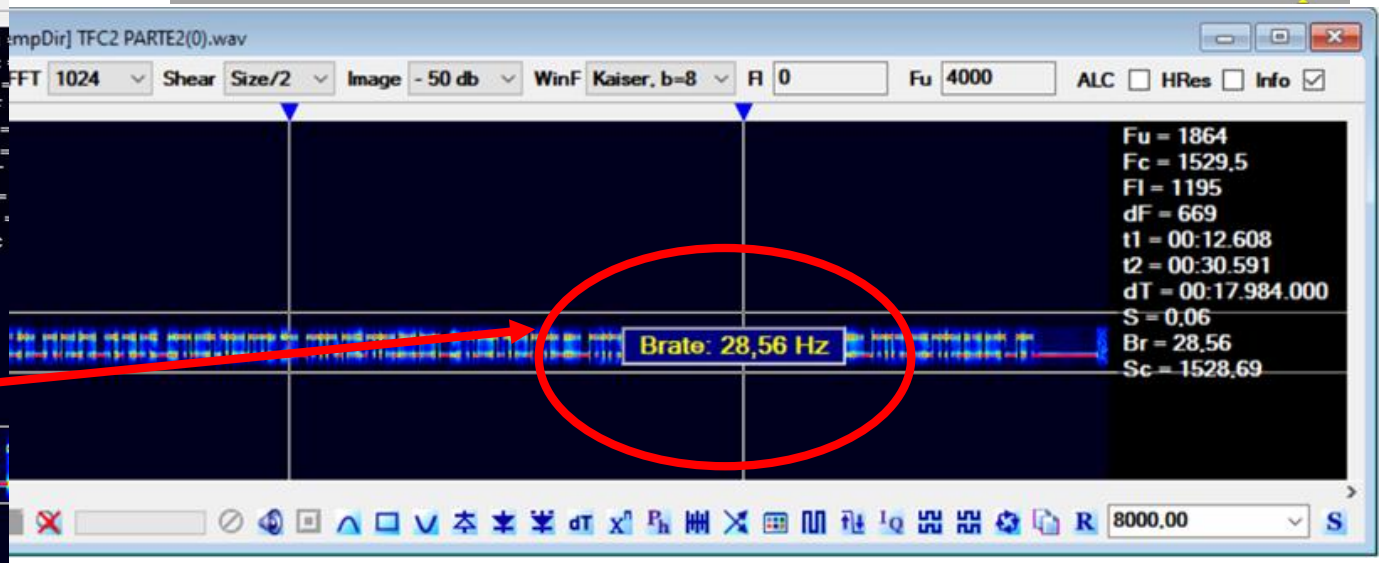


EJEMPLO DE SEÑAL: CIS 36-50 / T-600

- **Procesamiento de la PARTE 2, con duración diferente al IDLE.**
- Se supone que se trata de la **transmisión de datos.**
- Se observa que **la velocidad de la PARTE 2 no corresponde con los 50 Bd esperados**, siendo esta muy inferior: **28,56 Bd**.





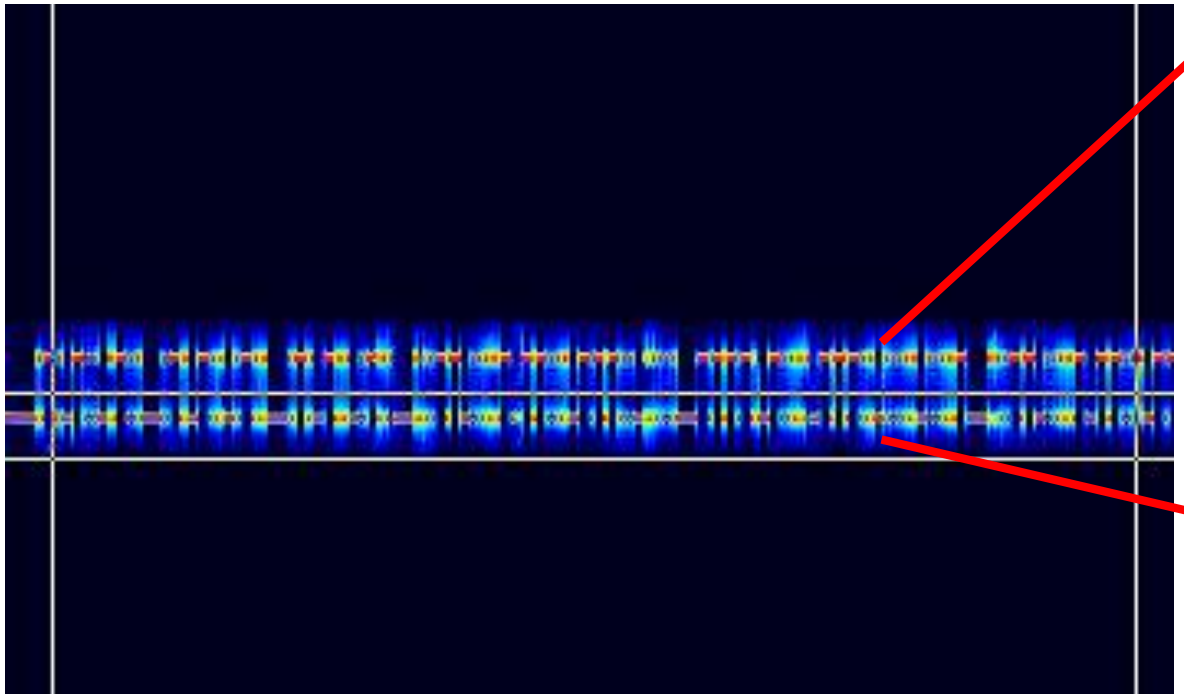


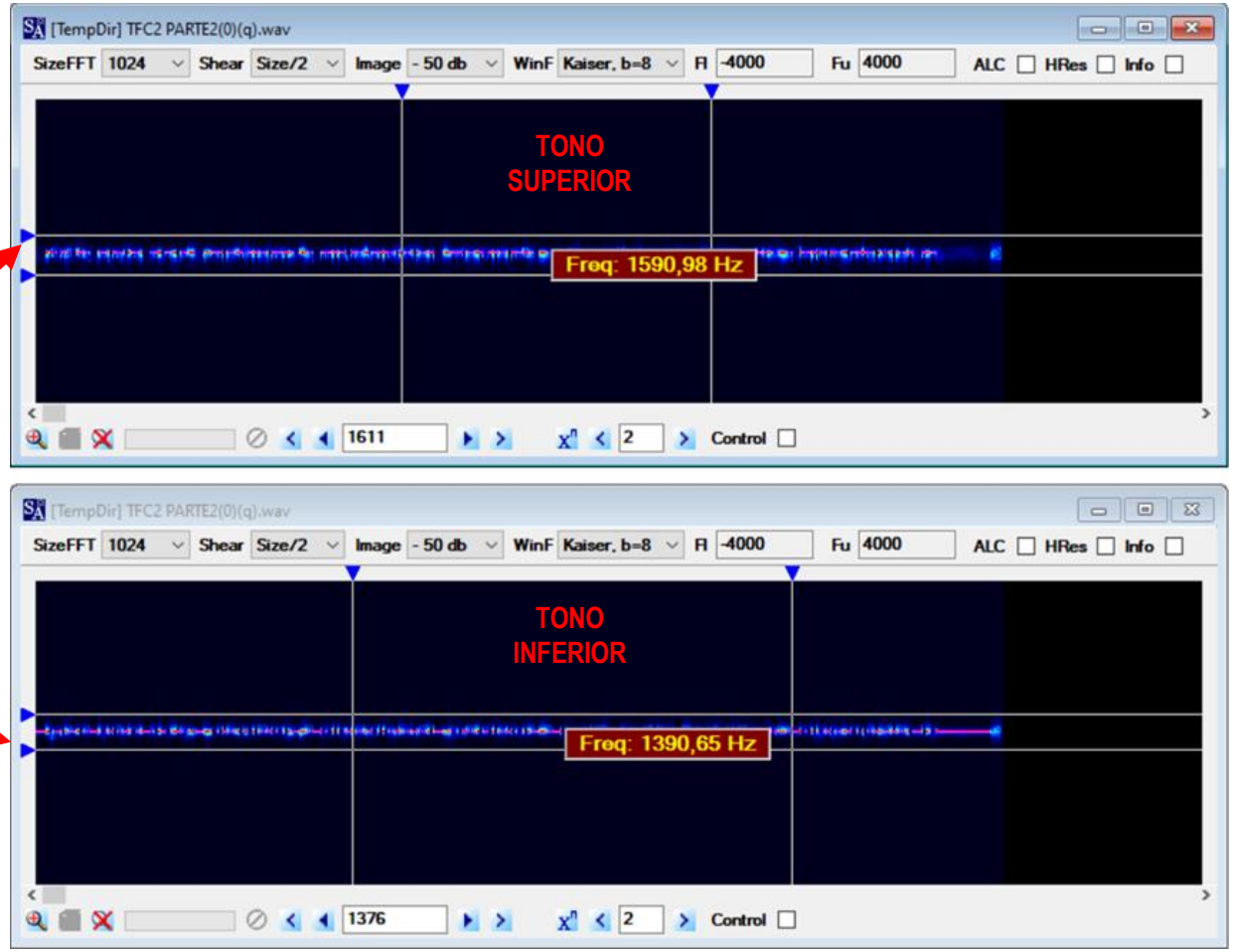
EJEMPLO DE SEÑAL: CIS 36-50 / T-600

IntelCon by Ginseg

#IntelCon2020

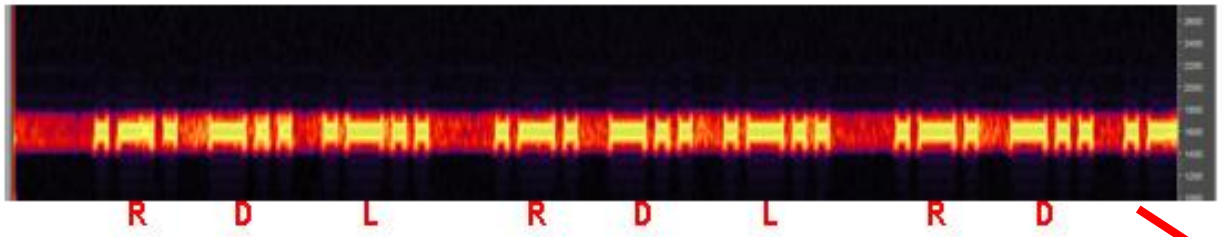
- Dada las discrepancias encontradas, el analista debe **analizar cada tono por separado para llegar a alguna conclusión**.

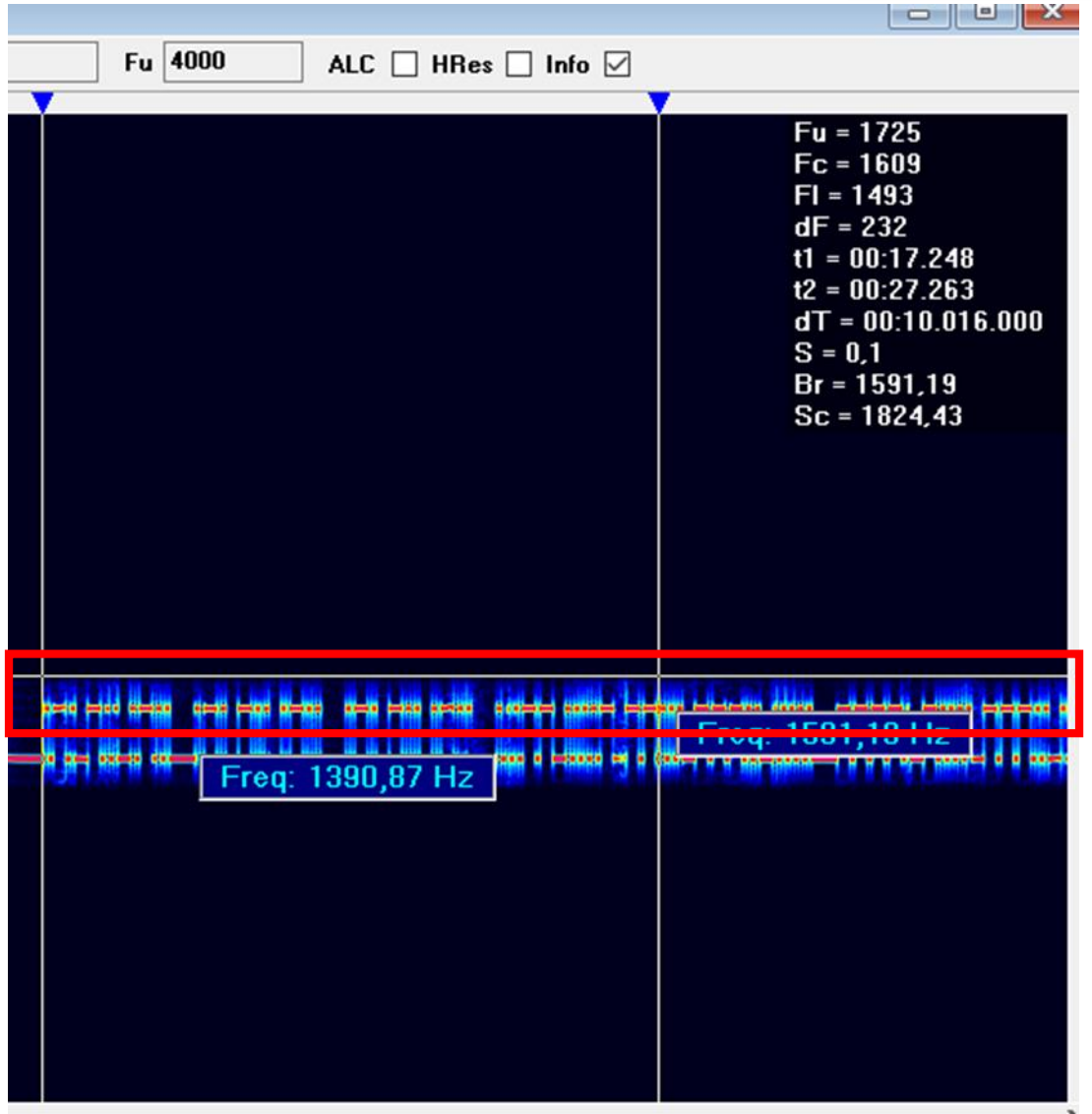




EJEMPLO DE SEÑAL: CIS 36-50 / T-600

- Si aislamos el tono superior **podemos observar sorprendentemente que en realidad se trata de una transmisión de datos en Código Morse** con el texto **"RDL... RDL.. RDL..."**





- **¿Qué quiere decir este mensaje?**

En este punto el analista, conociendo los datos recopilados en el análisis y el resultado, podrá **recurrir al OSINT para obtener más información sobre los datos "camuflados"** en esta señal.

EJEMPLO DE SEÑAL: CIS 36-50 / T-600 / BEE

- Tenemos un **sistema CIS 36-50 habitualmente empleado por la Armada rusa pero que NO cumple el estándar.**
- **T**iene “ofuscado” un mensaje en Morse que comienza por **RDL seguido de grupos de 5 números** (el mensaje está cifrado), finalizando con la letra “K” (cambio). Probablemente se trata de **comunicaciones de submarino en altura de periscopio.**
- Este sistema es **similar a los denominados BEE y T600**, aunque pueden usar diferentes parámetros de shift y velocidad, por lo que se debe analizar cada muestra por separado.

Russian Navy
Voyenno-Morskoy
Flot Rossii

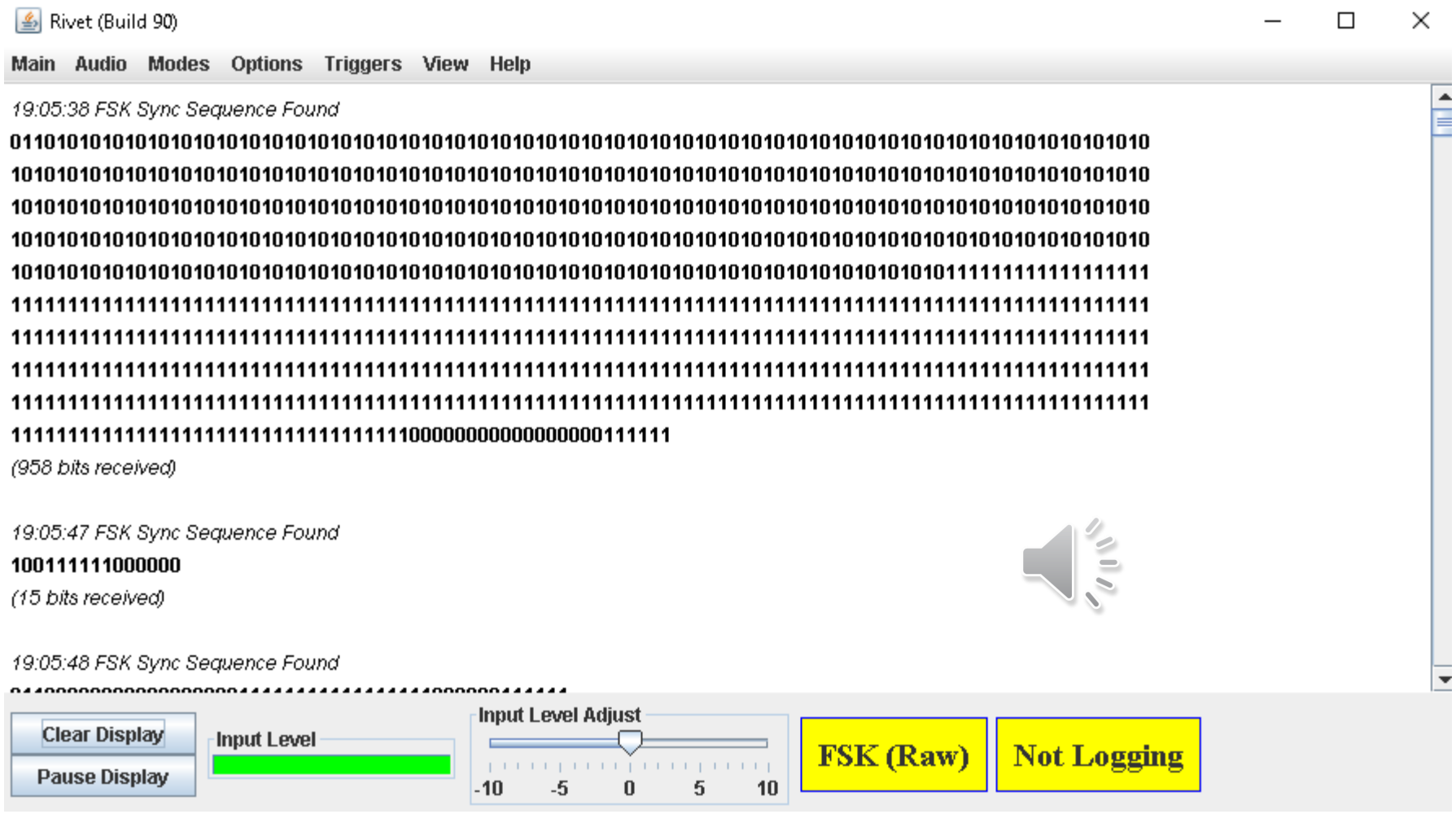
Frigate Neukrotimy © Ary Boender

By Fritz Nusser
Last update: June 2013
www.udxf.nl

Publishing results about military and secret service matters is, by nature, a continuous process of trial and error. If you, who might know it better, note any inaccuracies or mistakes, please send your comments to UDXF.

Fuente: Boletín monográfico de la comunidad UDXF sobre las comunicaciones de la Armada Rusa http://www.udxf.nl/Russian%20navy.pdf

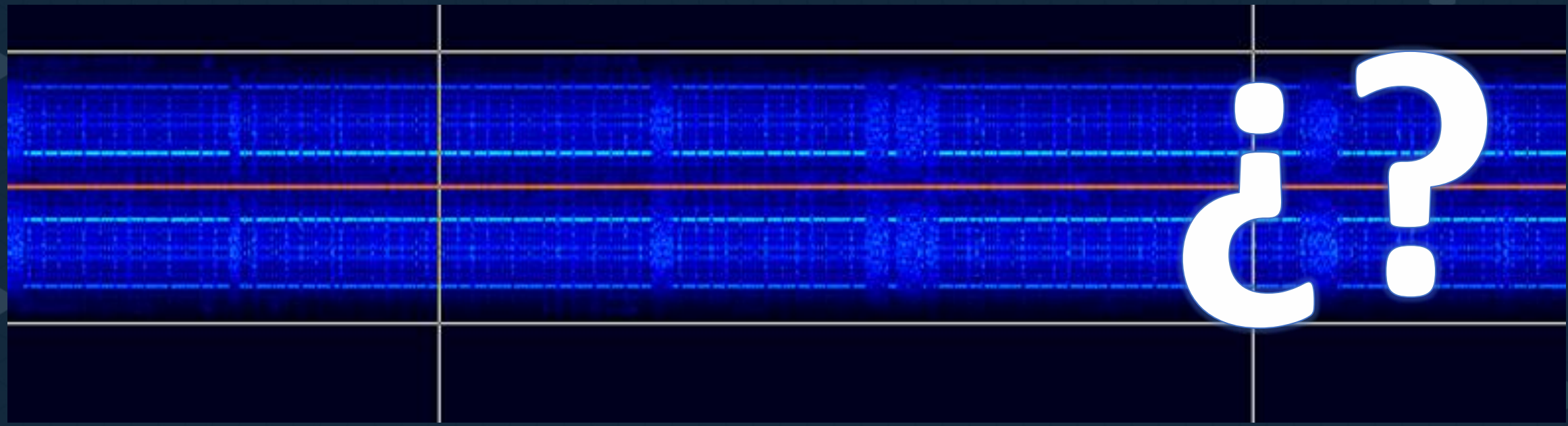
EJEMPLO DE SEÑAL: CIS 36-50 / T-600 / BEE



Captura de la decodificación del radiomodem T600 FSK , SHIFT 250 , 100 Bd con el software Rivet v90 de Ian Wraith en Modo RAW FSK.

IntelCon
by Ginseg

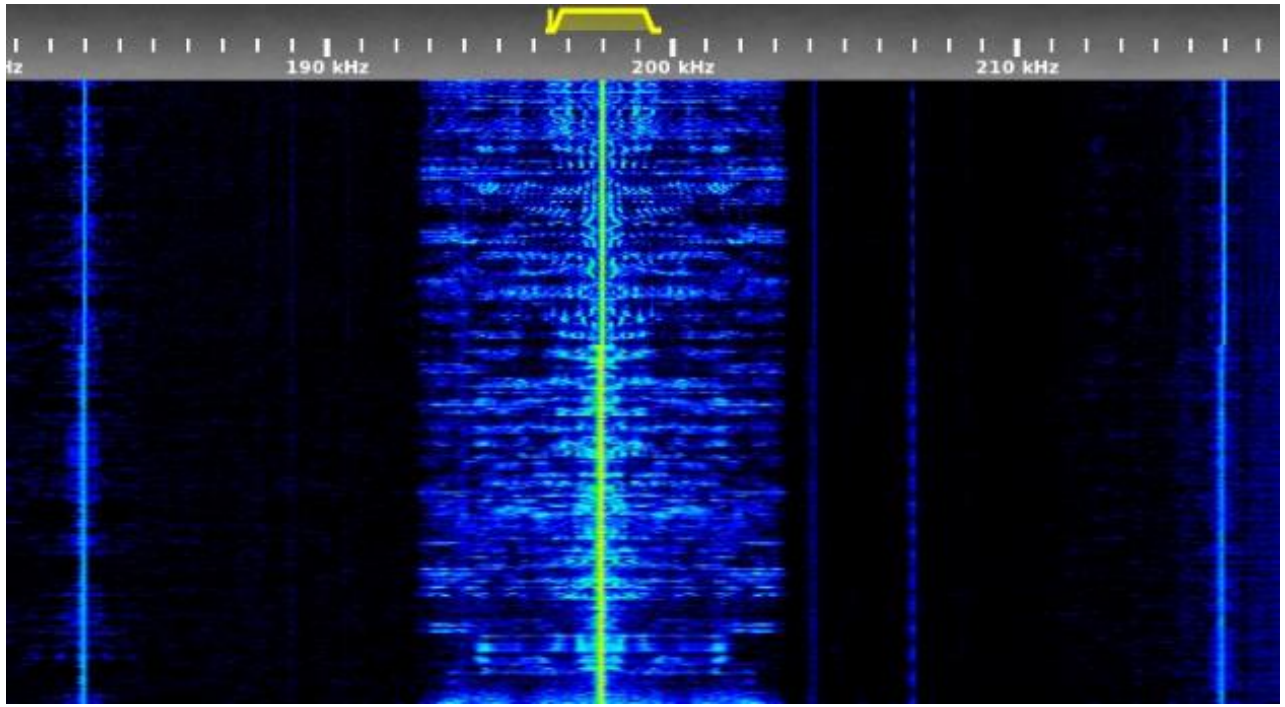
EJEMPLO SEÑAL 3

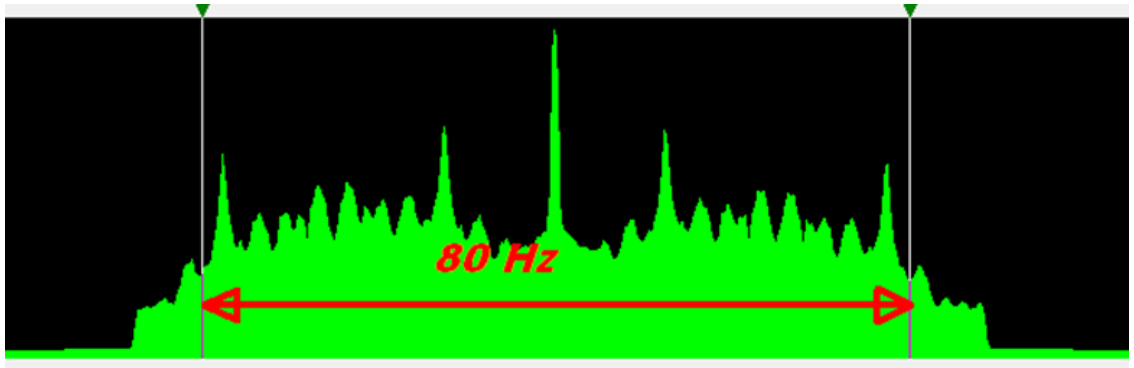


EJEMPLO DE SEÑAL: BBC 4 – UK AMDS TELESWITCH

- BW(RF):12 Khz
- BW(PSK) 80 Hz.
- Modulación: PSK (45º) sobre portadora AM
- Codificación: Manchester
- Velocidad:50 sps (25 bits/s)

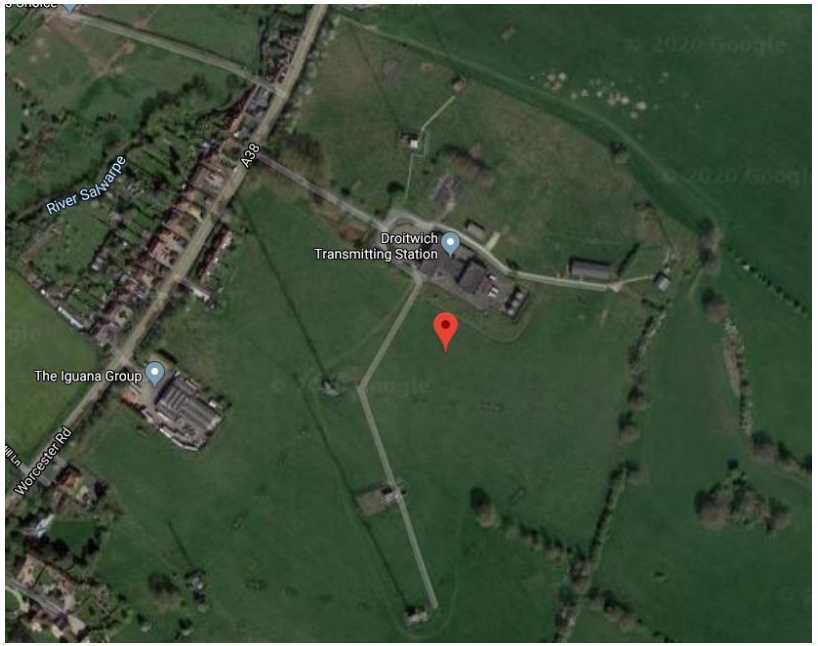
- Modo Rx:Grabación en USB sobre portadora -1Khz.
- Trama:2 s.

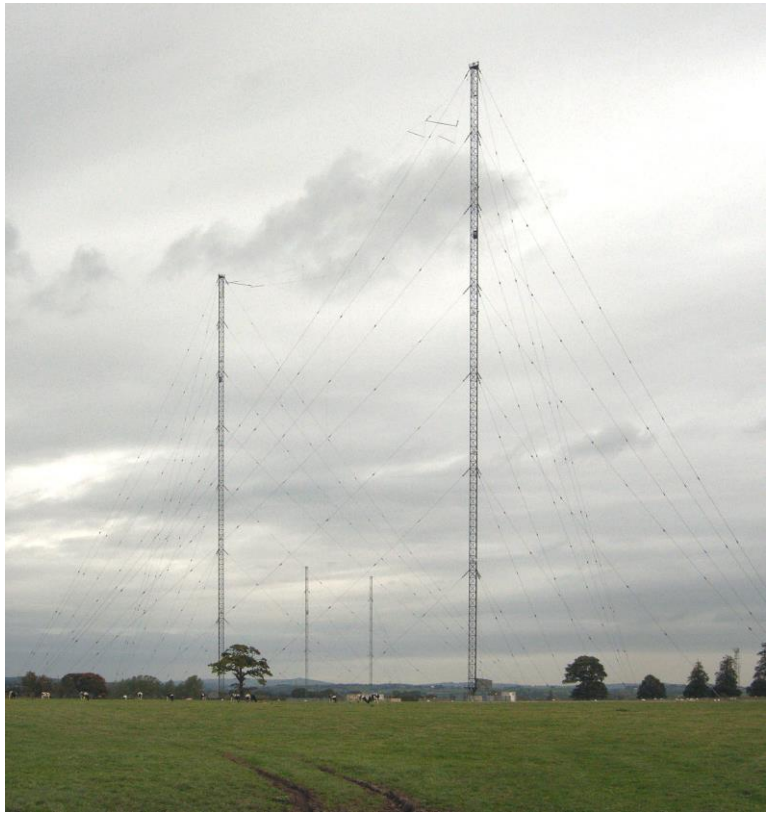




EJEMPLO DE SEÑAL: BBC 4 – UK AMDS TELESWITCH

- **El transmisor principal en Droitwich con una potencia de 500kW**, puede llegar a la mayor parte del Reino Unido y otras partes de Europa, mientras que los **dos transmisores más pequeños están ubicados en Westerglen y Burghead**.

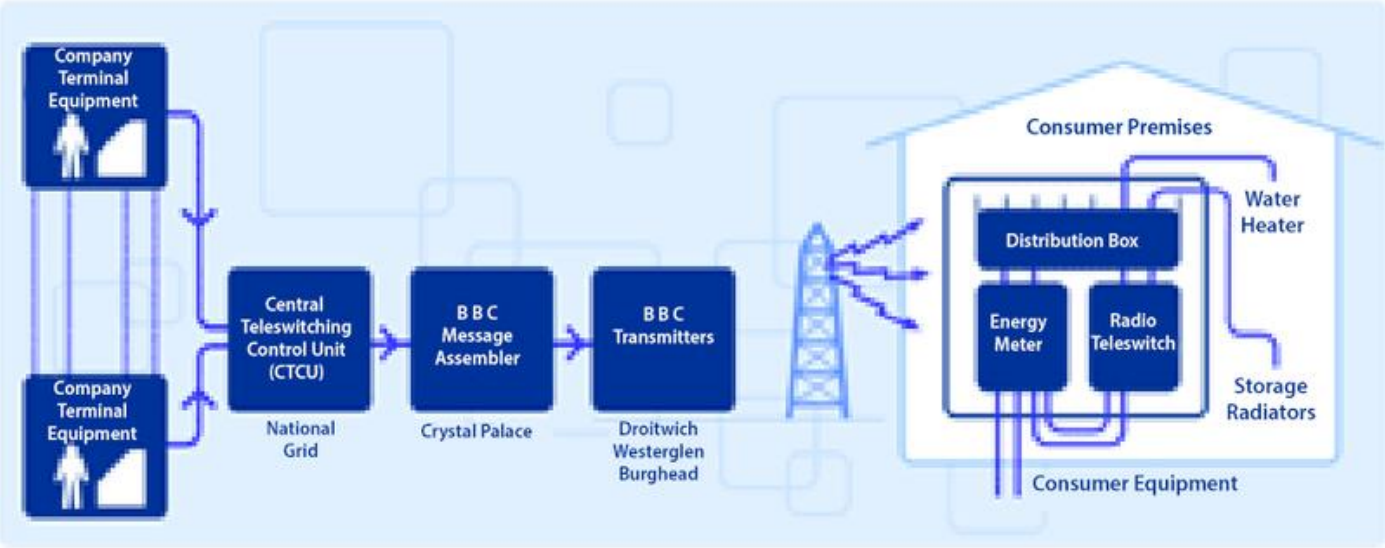




Fotos de la ubicación del transmisor de la BBC4 en Droitwich con sus mástiles de más de 200m de altura.

EJEMPLO DE SEÑAL: BBC 4 – UK AMDS TELESWITCH

- **Usada por suministradores de electricidad de UK para conmutar las tarifas eléctricas en función de diferentes parámetros: fecha, hora UTC, mensajes de usuario.**
- En su página se puede leer que uno de los usos de esta red es **avisar de inundaciones… ¿A quién?**

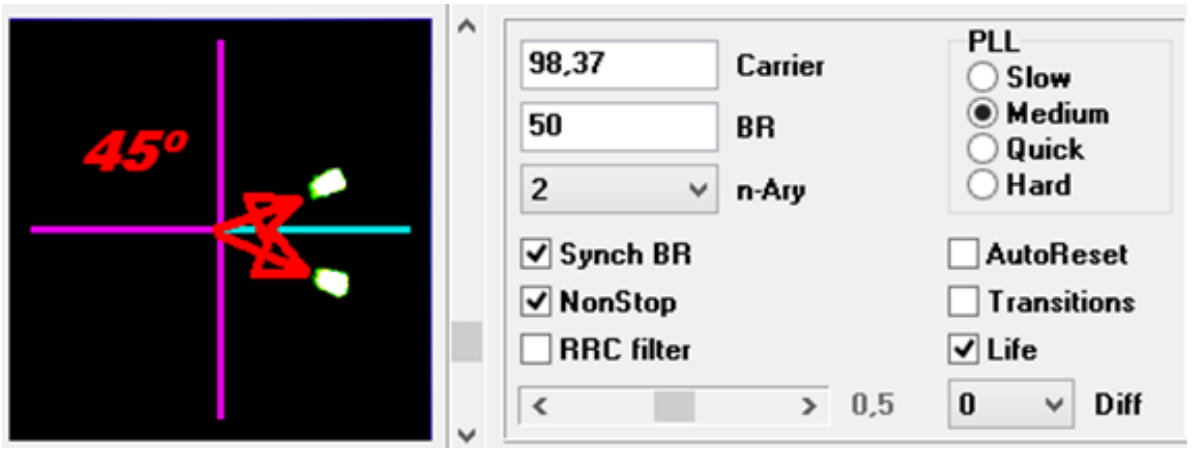


Esquema de funcionamiento de UK AMDS TELESWITCH y receptor de abonado. Web oficial UK AMDS

EJEMPLO DE SEÑAL: BBC 4 – UK AMDS TELESWITCH

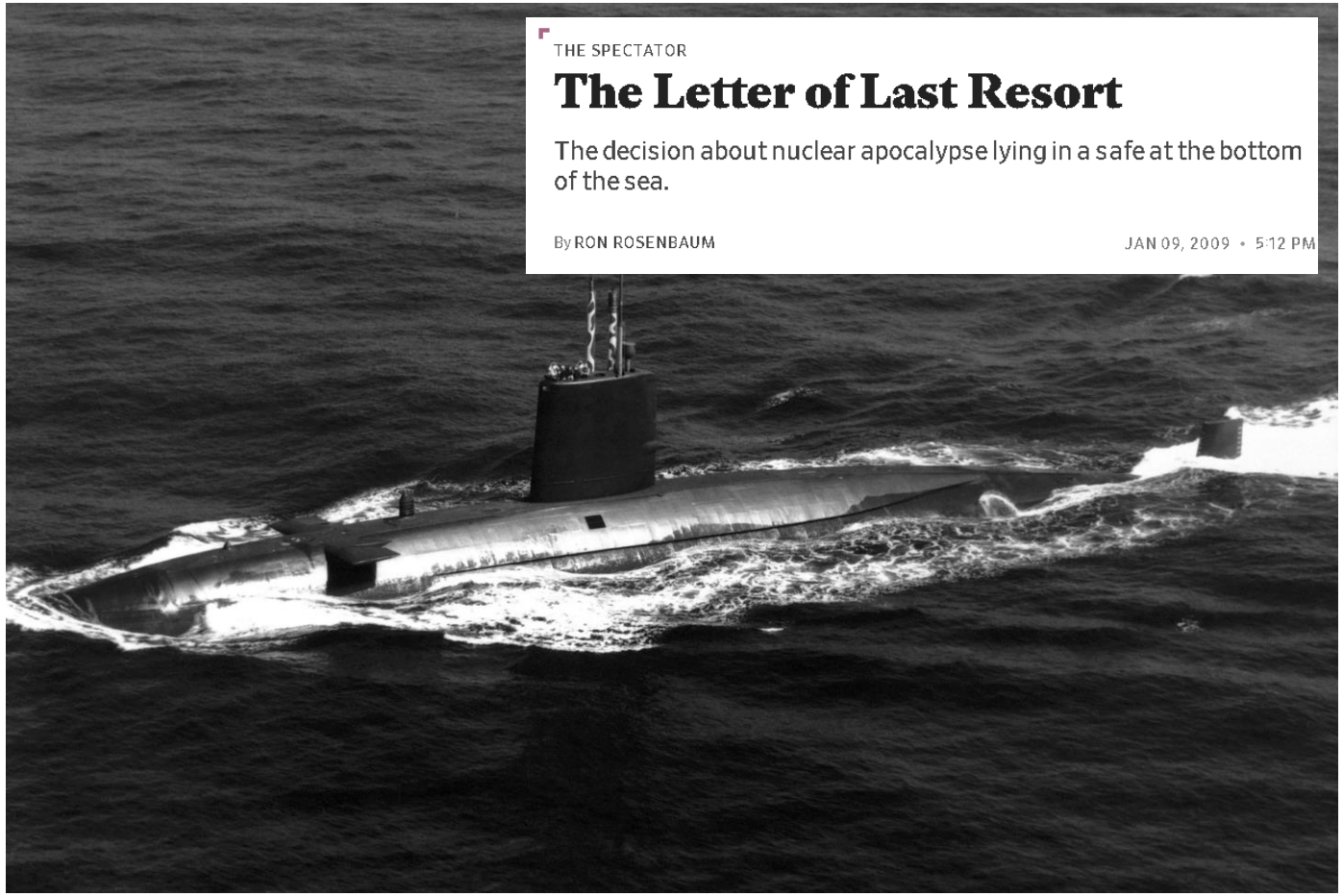
- **Se transmiten 30 mensajes por minuto**, cada mensaje tiene 50 bits de datos. 18 de estos bits están ocupados por un encabezado y una verificación de redundancia cíclica (CRC). 32 bits están disponibles para datos.
- **La constelación muestra dos estados con una diferencia entre ellos de unos 45º**. (La fase de la portadora varia ± 22,5 º) posiblemente **para evitar interferencias en la emisión comercial de BBC4** en AM.

Demodulación de la señal donde se aprecia la codifiación Manchester en su estructura.



EJEMPLO DE SEÑAL: BBC 4 – UK AMDS TELESWITCH

- **Existe la teoría de que puede ser usada por la flota de submarinos del Reino Unido como sistema de "hombre muerto"** al dejar de recibir la señal a determinada profundidad ante un "Armagedon".
- **¿Qué sentido tiene hoy esta señal en el aire…?** Su licencia está renovada hasta marzo de 2021 en contra de lo que se pensaba.
- **Debemos tener en cuenta la dificultad de penetración de las ondas de radio en el agua**, y la importancia de sistemas que permitan a los submarinos recibir y enviar información sin delatar su presencia al enemigo.



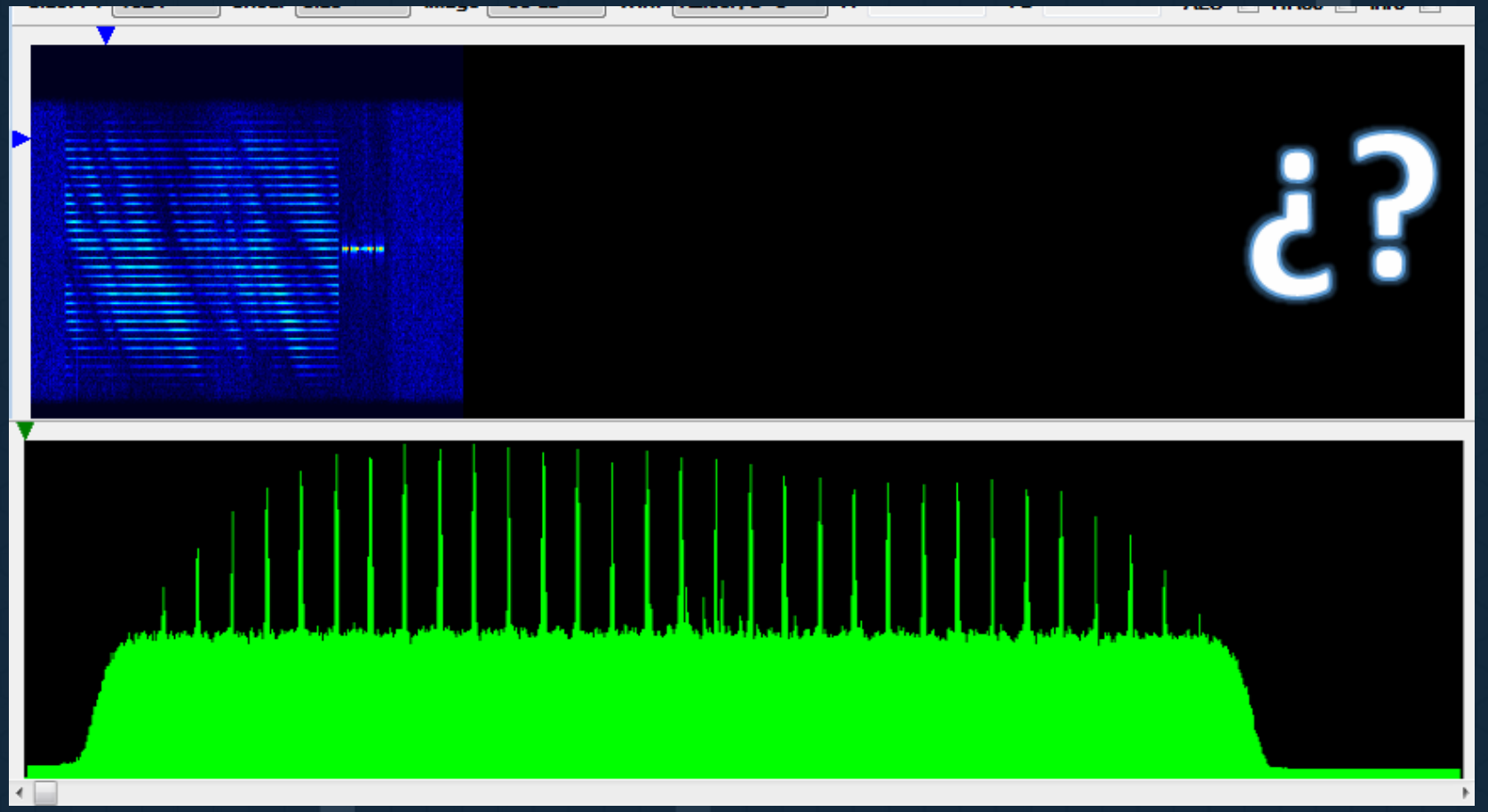
British Valiant-class nuclear-powered attack submarine underway on 14 May 1986 (Wikipedia)

EJEMPLO DE SEÑAL: BBC 4 – UK AMDS TELESWITCH

- En España tenemos un ejemplo de comunicaciones navales submarinas en la denominada **“Torre de los Americanos” o “Torreta de Guardamar”**, situada en la Guardamar del Segura.
- Está considerada **como la estructura más alta de la península ibérica, con 380m de altitud**.
- Fue instalada por la Armada de los EE.UU en 1962. Hoy depende de la Armada Española y es **usada para enviar órdenes a los submarinos**.

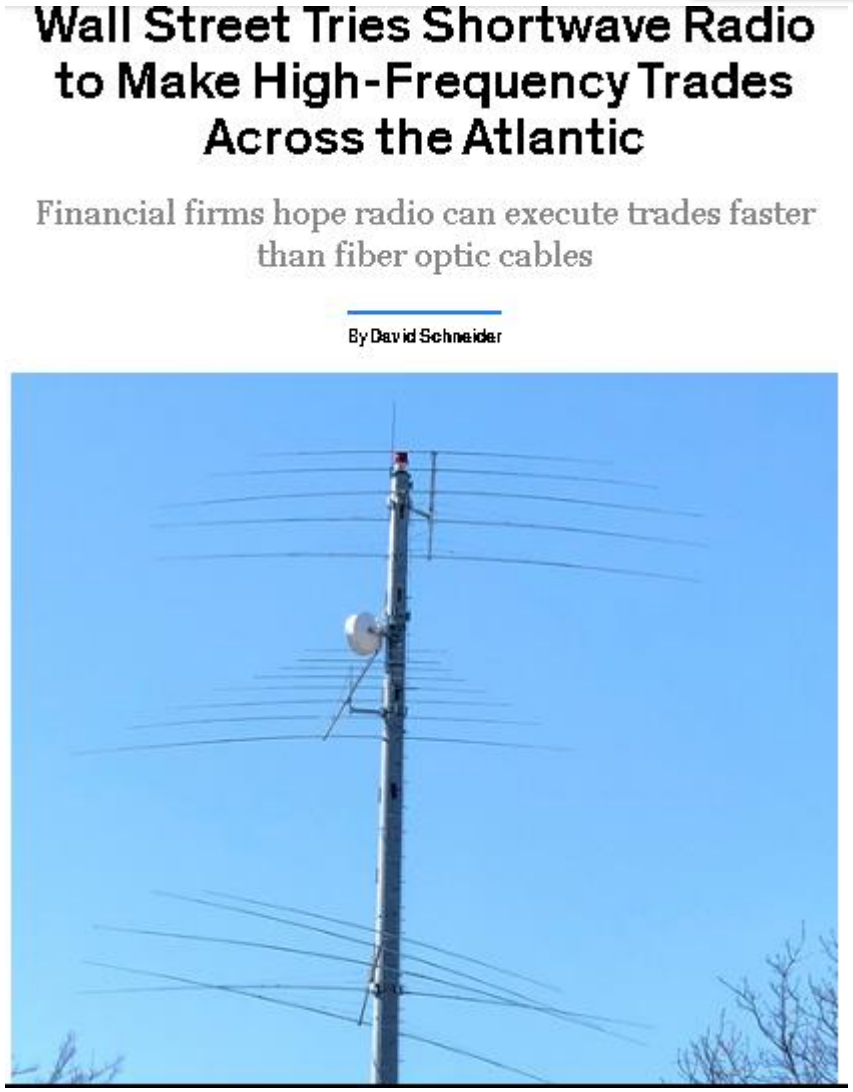
“La Torre de los Americanos” en la localidad Española de Guardamar del Segura. Fuente Wikipedia De Joanbanjo - Trabajo propio, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=36549860

EJEMPLO SEÑAL 4



EJEMPLO DE SEÑAL: LA MSK DE CHICAGO Y LOS “BROKERS”

- Hace algún tiempo diversos interesados en la radio, han investigado en **una serie de transmisores registrados en EE.UU a nombre de una compañía vinculada a las transacciones de bolsa**.
- En 2015, Hibernia Networks (que luego fue adquirida por GTT), junto con TE Subcom, completó un cable de fibra óptica que siguió una **ruta directa entre Nueva York y Londres para ofrecer el menor retraso, lo que requiere solo 59 milisegundos** para una señal para hacer el viaje de ida y vuelta.



Wall Street Tries Shortwave Radio to Make High-Frequency Trades Across the Atlantic

Financial firms hope radio can execute trades faster than fiber optic cables

By David Schneider

EJEMPLO DE SEÑAL: LA MSK DE CHICAGO Y LOS "BROKERS"

- **Bob Van Valzah, un ingeniero de software, radioaficionado y especialista en redes se encontró en West Chicago, Illinois con una extraña torre de antenas** y después de una detallada investigación lanzó la hipótesis de que transmitían datos a los centros de la Bolsa Europea a través de Onda Corta.
- **Reflejó su investigación en un blog** en 2018: https://sniperinmahwah.wordpress.com/2018/05/07/shortwave-trading-part-i-the-west-chicago-tower-mystery/
- **En la basura de la estación de antenas observo cajas de un USRP X300**… obviamente no se trataba de un equipo de una BTS comercial de GSM.

SNIPER IN MAHWAH & FRIENDS

It's all about market structure. "Pretium iustum mathematicum licet soli Deo notum"

SHORTWAVE TRADING | PART I | THE WEST CHICAGO TOWER MYSTERY

7 May 2018 — 83 Comments

Since 2014 this blog has extensively covered the wireless networks built by high-frequency trading (HFT) firms or network providers to reduce latencies between the different exchanges around the world (market makers need fast connectivity to manage risk, news traders also need to be fast, etc.). This epic investigation on microwave, which started with *HFT in my backyard*, will be fully reported in a book I'm currently writing (in French for now). As I'm quite busy with this writing (and

EJEMPLO DE SEÑAL: LA MSK DE CHICAGO Y LOS “BROKERS”

- A través de OSINT/IMINT y se averigua las ubicaciones **de 2 transmisores experimentales a nombre de SkyCast LLC**.
- **Farmingville NY** WUSB-FM de la universidad Stony Brook y a 34 km en línea recta **Riverhead**.
- **Riverhead NY** tiene unas 20 torres en 10,5 hectáreas de terreno (aprox 105000 m2).
- **En 1922 ya se recibían operaciones comerciales desde Europa en una cabaña de madera** por Onda Corta en código Morse y se retransmitía hacia Manhattan por líneas terrestres.

EJEMPLO DE SEÑAL: LA MSK DE CHICAGO Y LOS "BROKERS"

IntelCon by Ginseg

#IntelCon2020

- **¿La carrera por la latencia…?**

Nathan Wright, 80 S.W. 8th Street, Suite 2000, Miami, FL 33130,

United States of America
FEDERAL COMMUNICATIONS COMMISSION
EXPERIMENTAL
RADIO STATION CONSTRUCTION PERMIT
AND LICENSE

EXPERIMENTAL	WI2XER
(Nature of Service)	(Call Sign)
XT FX	0809-EX-PL-2015
(Class of Station)	(File Number)

NAME Skycast Services LLC

Subject to the provisions of the Communications Act of 1934, subsequent acts, and treaties, and all regulations heretofore or hereafter made by this Commission, and further subject to the conditions and requirements set forth in this license, the licensee hereof is hereby authorized to use and operate the radio transmitting facilities hereinafter described for radio communications in accordance with the program of experimentation described by the licensee in its application for license.

Operation: In accordance with Sec. 5.3(a, e & j) of the Commission's Rules

REDACTED FOR PUBLIC INSPECTION

Skycast Services LLC
FCC Form 442—Exhibit 1

NARRATIVE STATEMENT

Pursuant to Section 5.3 and Section 5.63 of the Commission's rules, 47 C.F.R. §§ 5.3, 5.63, Skycast Services LLC ("Skycast") respectfully requests that the Commission grant Skycast experimental authority using high-frequency ("HF") spectrum [redacted].

1. Applicant's Name, Address, and FCC Registration Number ("FRN").

Skycast Services LLC
80 S.W. 8th Street, Suite 2000
Miami, FL 33130

FRN: 0025141839

2. Description of Operations and Purpose of Requested Authority.

[redacted]

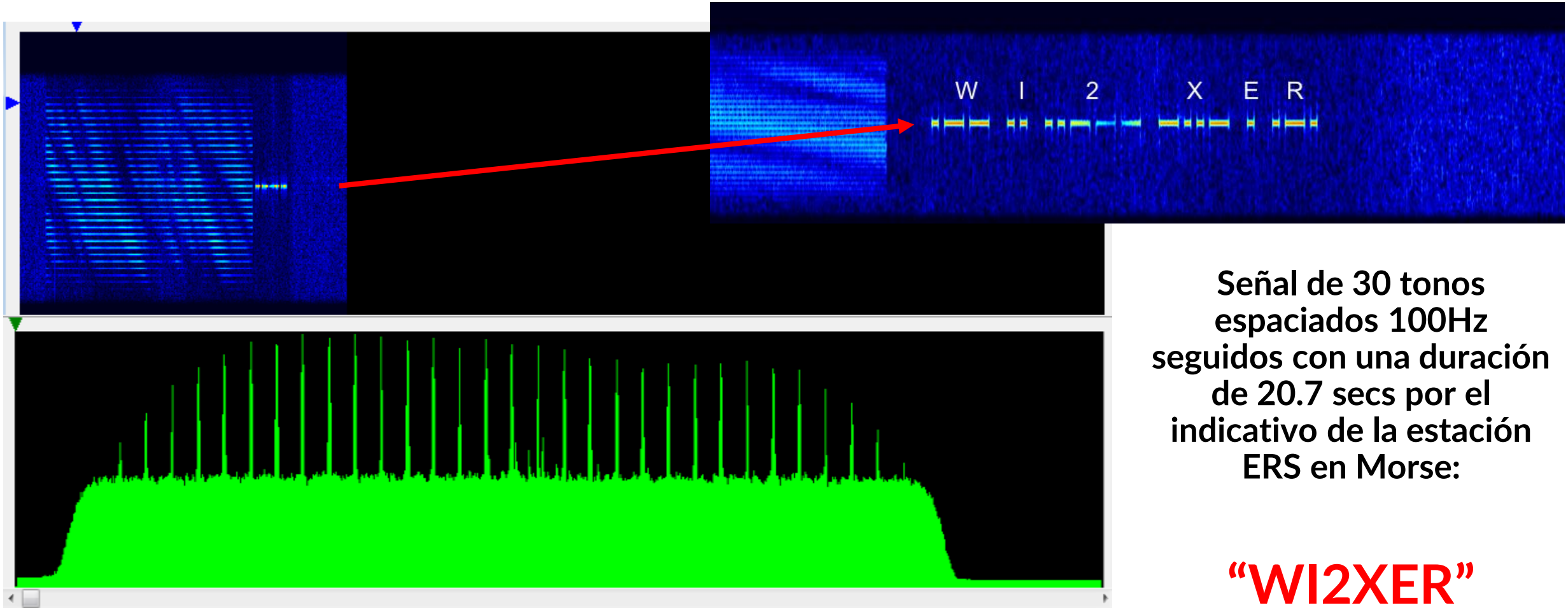
Documentación pública de la FCC americana donde se concede licencia experimental a la estación WI2XER. La información sobre patentes y tecnología empleada figura censurada por la FCC en su BB.DD.

EJEMPLO DE SEÑAL: LA MSK DE CHICAGO Y LOS “BROKERS”

IntelCon by Ginseg

#IntelCon2020

Estación ERS de HFT (Trading de alta frecuencia)??



Señal de 30 tonos espaciados 100Hz seguidos con una duración de 20.7 secs por el indicativo de la estación ERS en Morse:

“WI2XER”

***Señal capturada por Tony Anselmi**: http://i56578-swl.blogspot.com/*

EJEMPLO DE SEÑAL: LA MSK DE CHICAGO Y LOS “BROKERS”

- Los sistemas con licencia experimental utilizan una variedad de modos de modulación por desplazamiento de frecuencia, incluidos **FSK, AFSK, QPSK y 8-PSK, en frecuencias que van desde aproximadamente 6 MHz a 24 MHz** y niveles de potencia de 20 kW ERP a casi 50 kW ERP.
- De EE.UU a Europa, **la ventaja de la O.C está sobre 10 ms**. una CPU moderna puede ejecutar miles de instrucciones en 1 µs.
- **Ojo en onda corta con la latencia de serialización**. Se deberían emplear algoritmos de codificación muy eficientes para mitigar esta desventaja.
- Onda Corta **también tiene otras desventajas…**

Business

HFT Traders Dust Off Century-Old Tool in Search of Market Edge

By Brian Louis, Nick Baker, and John McCormick
18 de junio de 2018 12:00 CEST

- Jump Trading, Virtu appear to be testing shortwave for trading
- Sites are located just miles away from CME’s futures exchanges

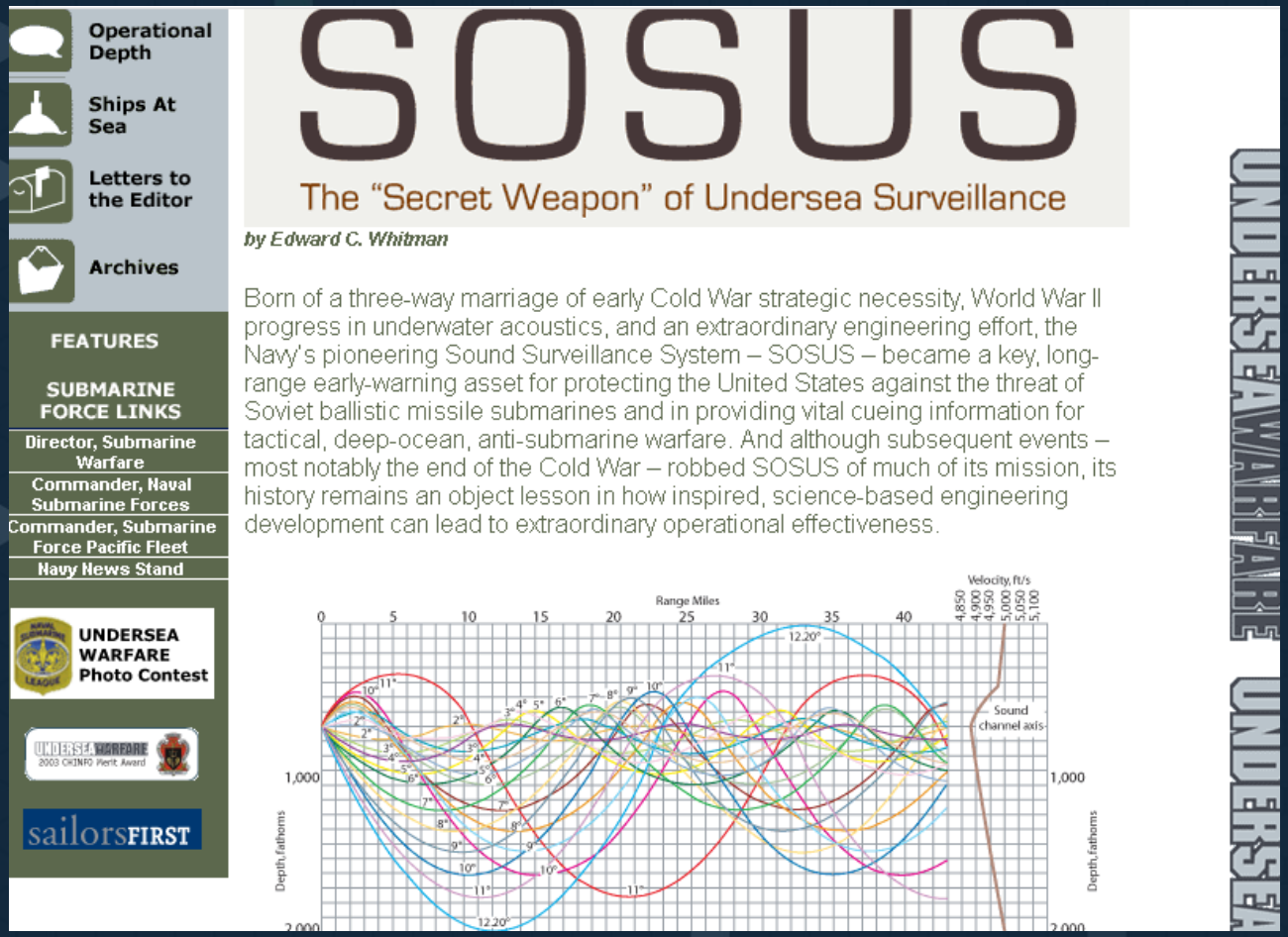
LIVE ON BLOOMBERG
Watch Live TV >
Listen to Live Radio >

Bloomberg Businessweek

The Gazillion-Dollar Standoff Over Two High-Frequency Trading Towers

The hunt for a millionth-of-a-second advantage in the town best known for *Wayne’s World* is getting heated.

“BONUS TRACK”… ACINT



Operational Depth
Ships At Sea
Letters to the Editor
Archives

FEATURES

SUBMARINE FORCE LINKS

Director, Submarine Warfare
Commander, Naval Submarine Forces
Commander, Submarine Force Pacific Fleet
Navy News Stand

UNDERSEA WARFARE Photo Contest

sailorsFIRST

SOSUS

The “Secret Weapon” of Undersea Surveillance

by Edward C. Whitman

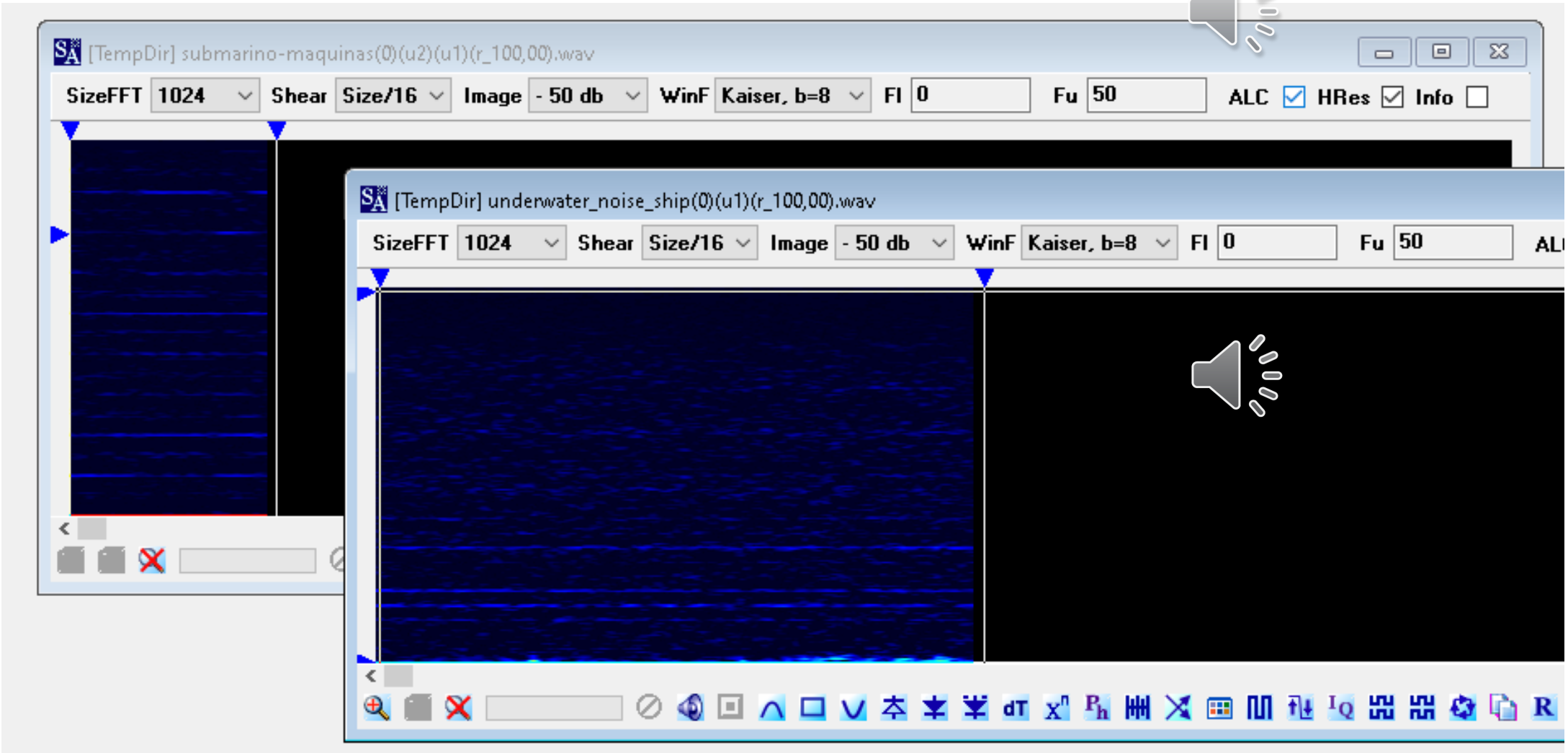
Born of a three-way marriage of early Cold War strategic necessity, World War II progress in underwater acoustics, and an extraordinary engineering effort, the Navy's pioneering Sound Surveillance System – SOSUS – became a key, long-range early-warning asset for protecting the United States against the threat of Soviet ballistic missile submarines and in providing vital cueing information for tactical, deep-ocean, anti-submarine warfare. And although subsequent events – most notably the end of the Cold War – robbed SOSUS of much of its mission, its history remains an object lesson in how inspired, science-based engineering development can lead to extraordinary operational effectiveness.

UNDERSEA WARFARE UNDERSEA

Redes de vigilancia submarina formadas con dispositivos de captación acústicos como hidrófonos…

Imagen Wikipedia.

Un poco de ACINT (Acoustical Intelligence)...



ALGUNAS HERRAMIENTAS DEL ANALISTA SIGINT

- **SDR hardware**, SDR On-line, analizadores de espectro, etc.
- **Software de tratamiento de señales** como Adobe Audition, Audacity, Cool Edit, etc.
- **Software de análisis de señales** como S.A (Signal Analyzer), Hoka Code, etc.
- **Decodificadores y/o clasificadores** como Sorcerer, Rivet, Krypto500, Decodio, Hoka Code, Sigmira, WaveCom, Go2 etc.
- **Softare de SDR** como SDR# Sharp, HDSDR, GQRX (Linux), GNU Radio, etc.
- **Documentación técnica** como libros sobre análisis, BB.DD de señales conocidas, etc.
- **“Audioteca” de señales de fabricantes**, foros especializados en análisis, etc.
- **Formación MUY ESPECIALIZADA.**
- **MUCHA PRÁCTICA… PACIENCIA.**

Fotografía de equipos RF del autor @RadioHacking

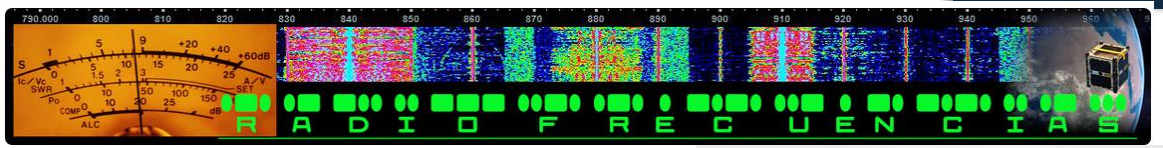
Y LO MÁS IMPORTANTE: AGRADECIMIENTOS

IntelCon by Ginseg

#IntelCon2020

- **A mis amigos "Angazu" y "Rapidbit"**, por compartir sus enormes conocimientos y análisis de señales de forma desinteresada con este **aprendiz**.
- A toda la comunidad de **RADIOFRECUENCIAS.ES**
- A **Priyom, UDXF, SIGIDWIKI** y a todos los **"radiofrikis"** que colaboran en mis locuras de forma anónima.
- A **Tony Anselmi y su fantástico blog**: http://i56578-swl.blogspot.com/
- **A Sergey Makarov**, aka "SergUA6", creador del software de análisis S.A Signals Analyzer (D.E.P).

GRACIAS A TODOS, PORQUE SIN VOSOTROS NUNCA HUBIERA SIDO POSIBLE…



SIGIDWIKI.COM
SIGNAL IDENTIFICATION GUIDE

PRIYOM.ORG
WORLD RADIO NUMBERS RESEARCH

diario SWL I5-56578 Antonio

HF utility/milcomm and signals
tony.anselmi@gmail.com

#IntelCon2020

IntelCon
by Ginseg

Gracias por la atención

Congreso Online de Ciberinteligencia | Julio 2020