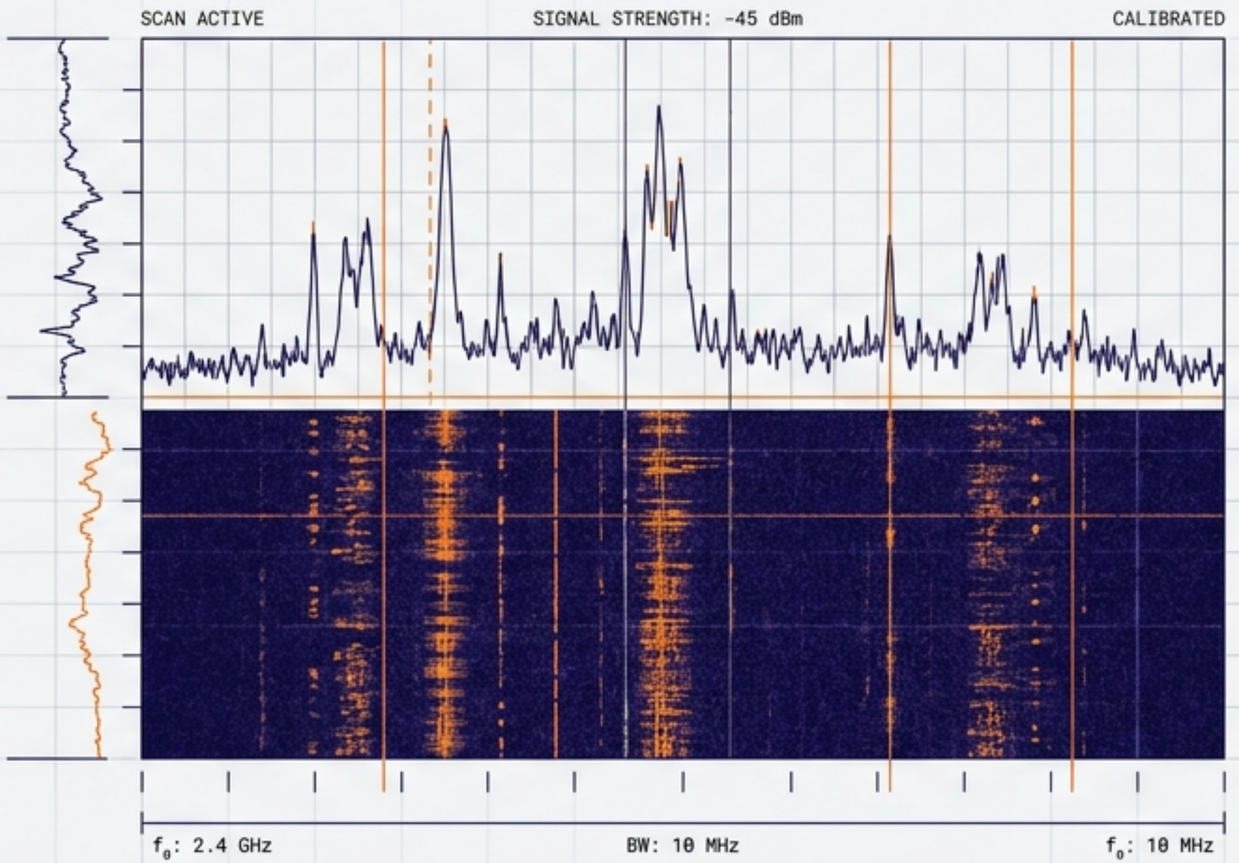
Livello: Avanzato | Protocollo: Analisi Passiva RF

Spiare.com

Guida Operativa all'Analisi di Spettro TSCM

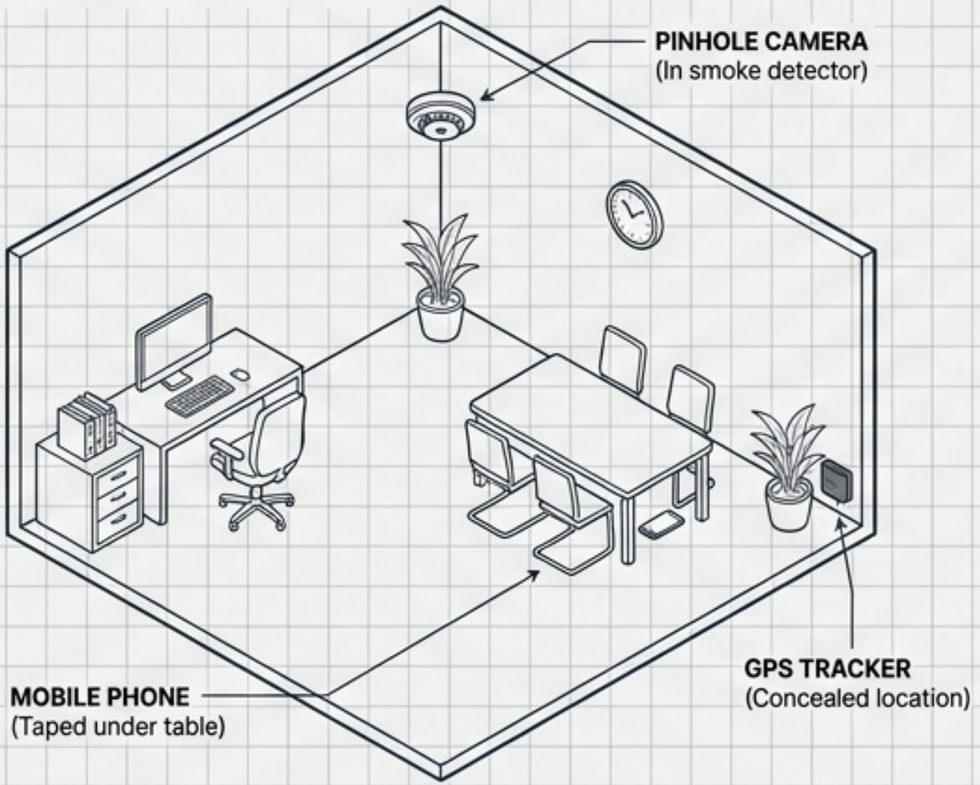
Dal segnale grezzo all'identificazione della minaccia: manuale tattico per bonifiche ambientali e controspionaggio.



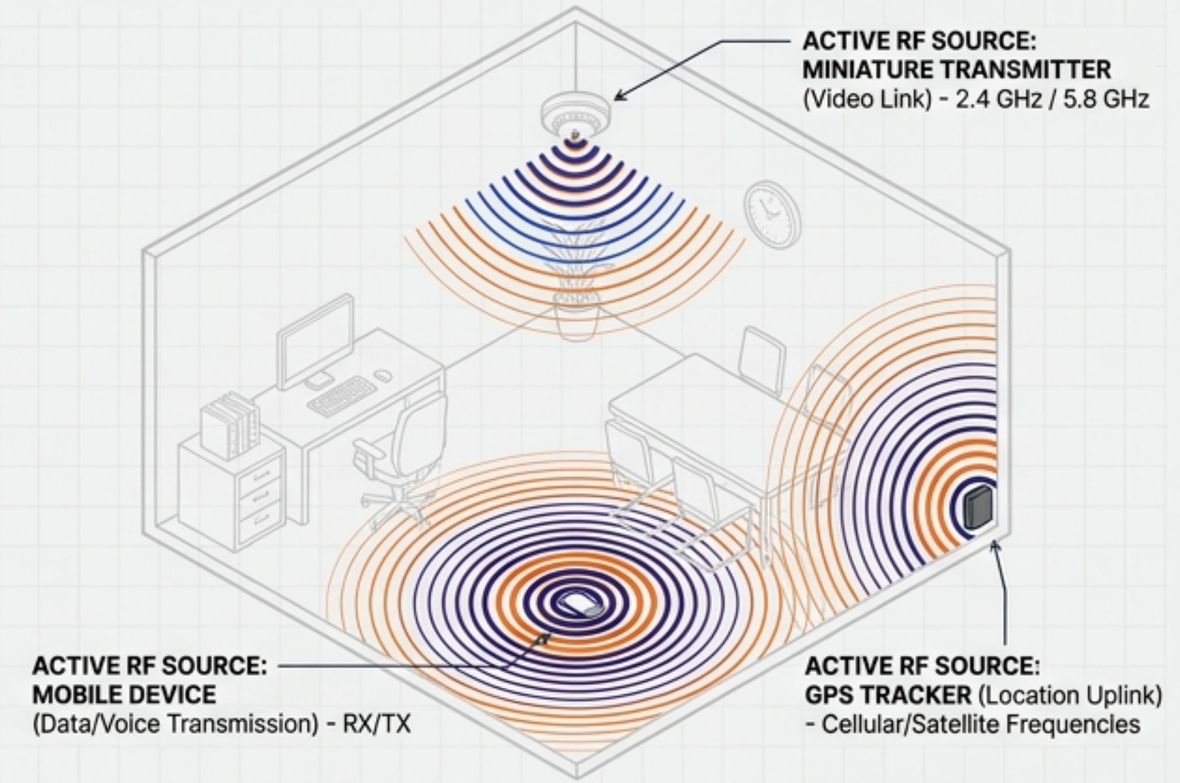
Rendere Visibile l'Invisibile

L'analisi spettrale è il primo livello di scansione in una bonifica TSCM (Technical Surveillance Countermeasures). Ogni dispositivo attivo emette energia elettromagnetica. L'analizzatore cattura questa traccia invisibile prima ancora di sapere cosa sia.

PANORAMICA FISICA DEGLI OGGETTI



MAPPA ENERGETICA RF



KEY INSIGHT

- **L'Obiettivo:** Distinguere il traffico legittimo dalle anomalie RF.
- **Il Vantaggio:** Rilevamento in tempo reale, totale flessibiiltà, analisi non intrusiva.

L'Arsenale: Matrice delle Capacità Hardware

Spiare.com

Entry-Level	RTL-SDR v3	500 kHz–1.75 GHz	~50 dB Dynamic Range	€30-50 Uso: Formazione.
Prosumer	Airspy R2	24–1800 MHz	~80 dB Dynamic Range	€169 Uso: TSCM base.
Avanzato	**HackRF One / SDRplay**	Fino a 6 GHz	50–100 dB	€200-320 Uso: Ricerca, TX/RX.
Professionale	**R&S PR100 / HSA-Q1**	DC–13.44 GHz	**>100 dB Dynamic Range**	€15.000+ Uso: TSCM certificabile.

COMPONENTI DELL'ANALIZZATORE HSA-Q1

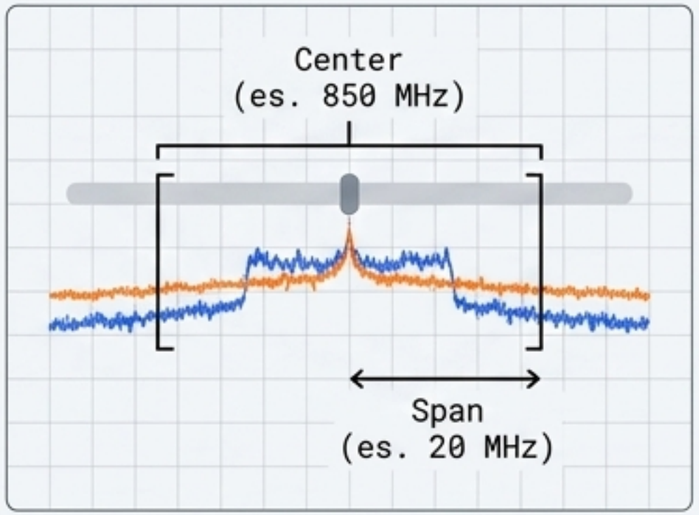
CONTENUTO KIT

CARATTERISCHITÀ PRINCIPALE

ATTENZIONE: LIMITI DEI SISTEMI SDR.
Il limite dei sistemi economici SDR è la saturazione in ambienti RF dense nf densi e il ridotto dynamic range.
Per indagini probatorie, la strumentazione professionale è insostituibile.

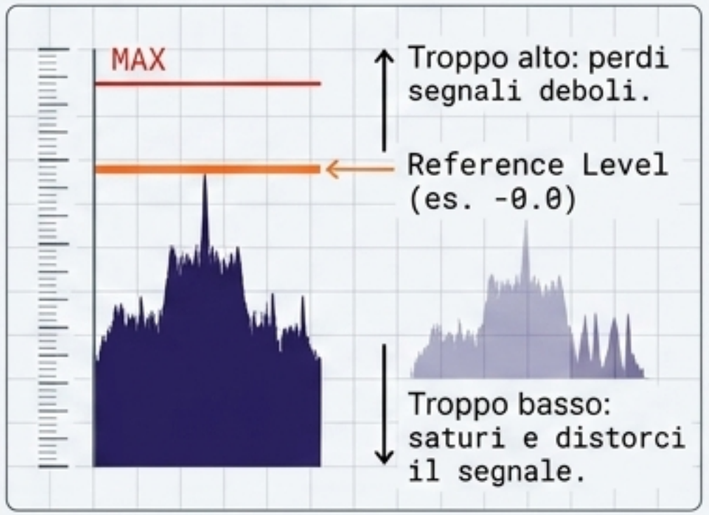
Il Cruscotto dell'Operatore: Parametri Fondamentali

Frequenza Centrale e Span



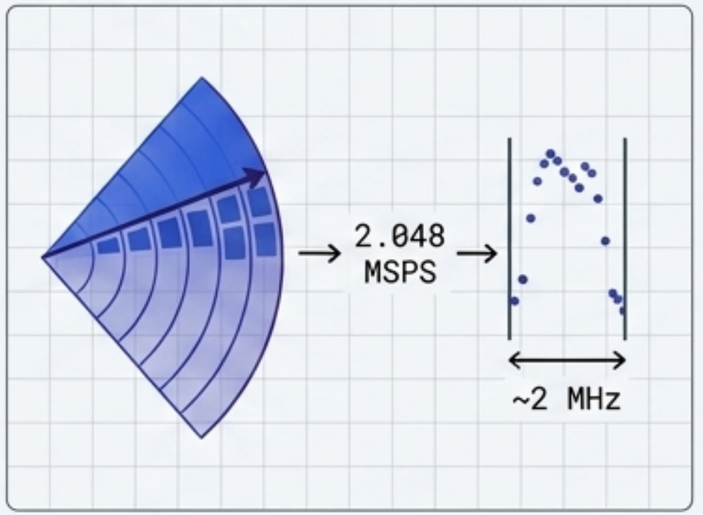
Definiscono la finestra di osservazione. Center è il punto mediano dello schermo (es. 850 MHz), Span è l'ampiezza totale visualizzata (es. 20 MHz).

Livello di Riferimento (Reference Level)



Il limite superiore del display, basato sulla potenza massima prevista. Troppo alto: perdi segnali deboli. Troppo basso: saturi e distorci il segnale.

Sample Rate (Campionamento)

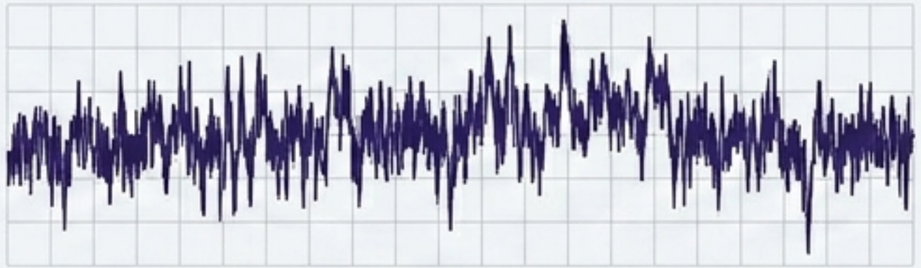


Determina la larghezza di banda visibile simultaneamente. 2.048 MSPS = ~2 MHz di finestra spettrale.

Spiare.com

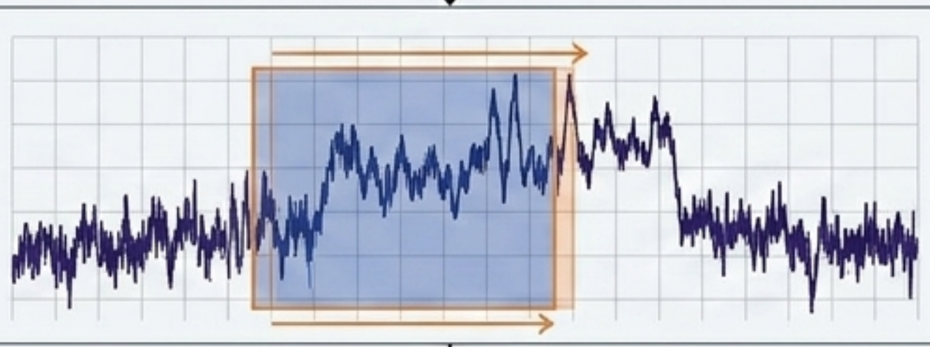
Filtrare il Rumore: RBW vs VBW

Segnale Grezzo



Spiare.com

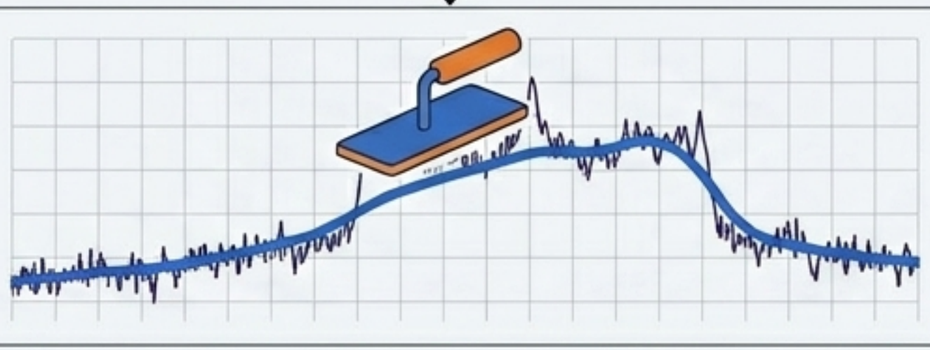
RBW - Resolution Bandwidth



Separa i segnali vicini e abbassa il rumore di fondo (noise floor), ma rallenta drasticamente il tempo di scansione.

3 MHz RBW = Fondo a -73 dBm.
3 kHz RBW = Fondo a -104 dBm.

VBW - Video Bandwidth

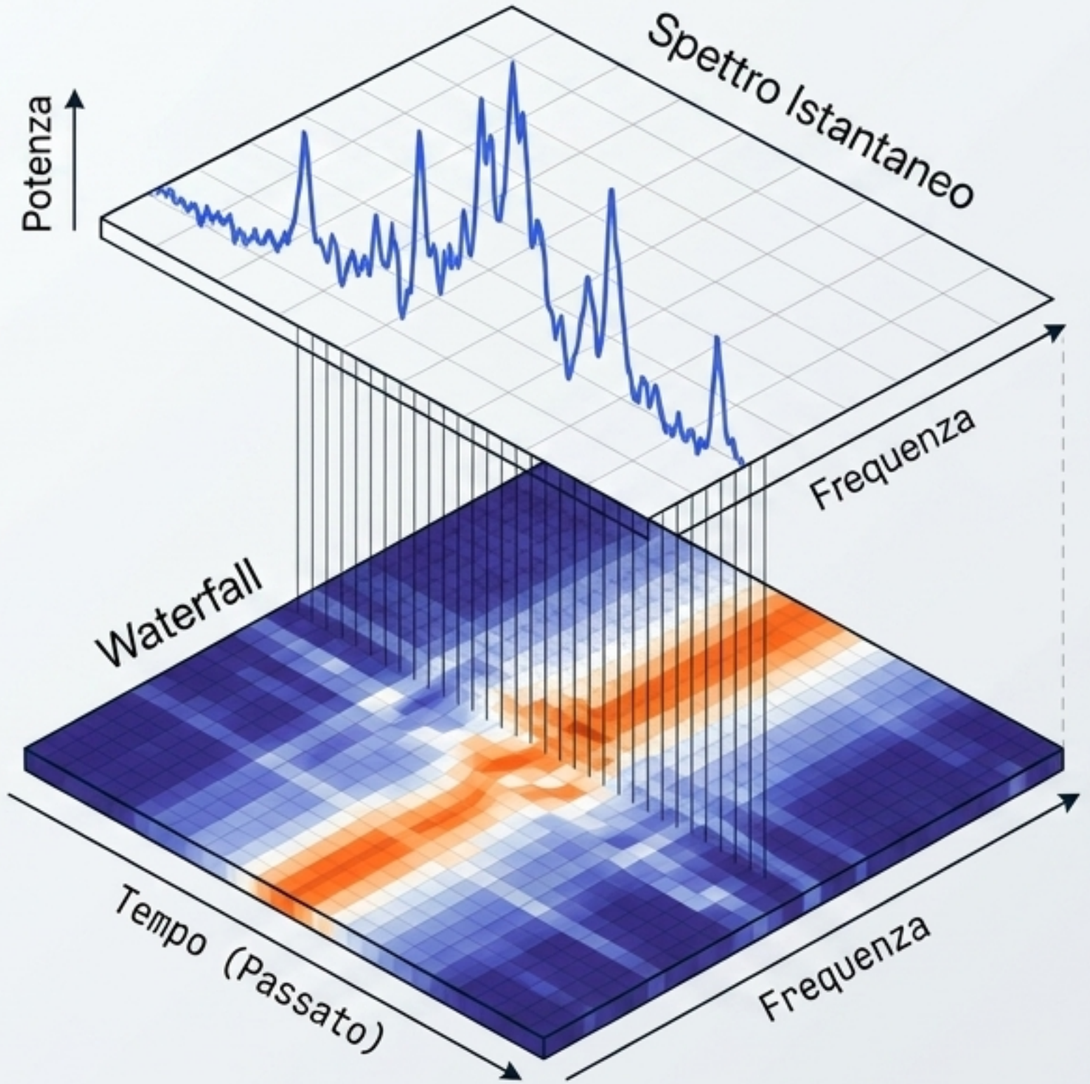


Calcola la media della traccia per pulire l'interfaccia visiva. Non abbassa il rumore reale, riduce solo il rumore sulla traccia a schermo.

Spettro vs Waterfall: Il Valore del Tempo

Spettro Istantaneo

- Ci dice cosa c'è ORA.
- Curva Frequenza/Potenza aggiornata in tempo reale.

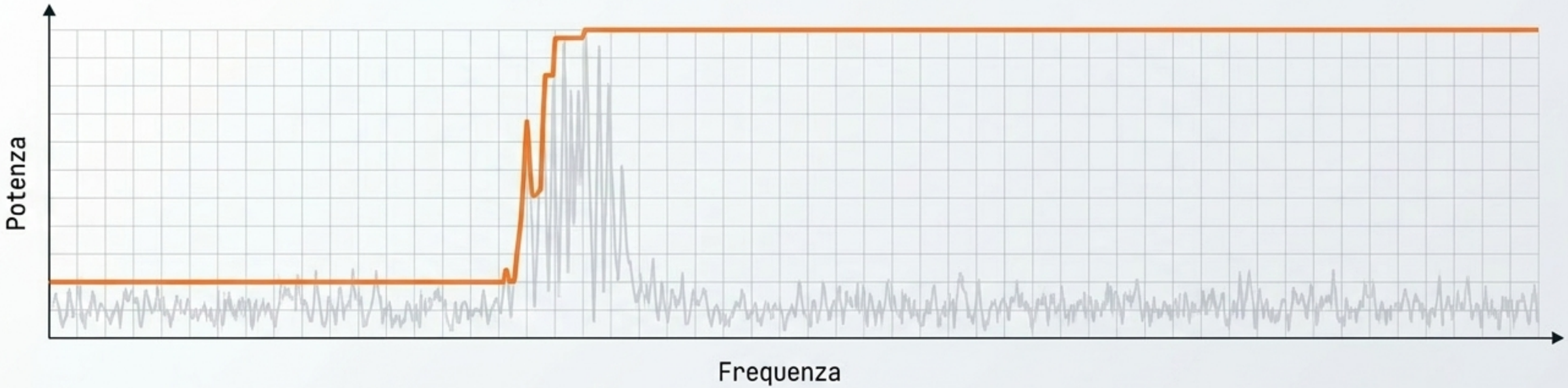


Waterfall

- Ci dice cosa sta SUCCEDENDO.
- Mappa cronologica a colori: X (Frequenza), Y (Tempo in discesa), Colore (Potenza).
- **Cruciale: Rivela pattern, durata e continuità,** impossibili da cogliere in un singolo istante.

Catturare l'Effimero: La Funzione Peak Hold

Spiare.com



Come Funziona

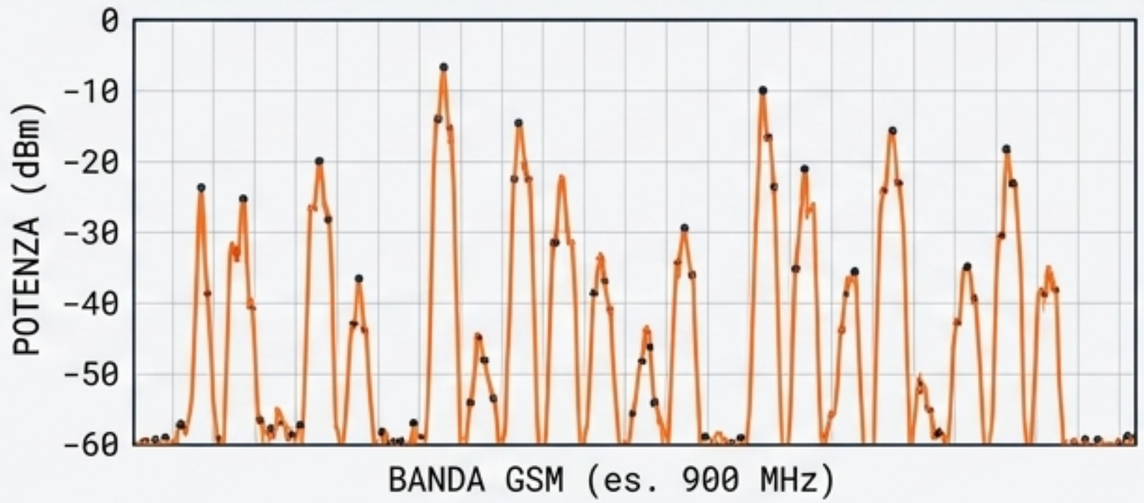
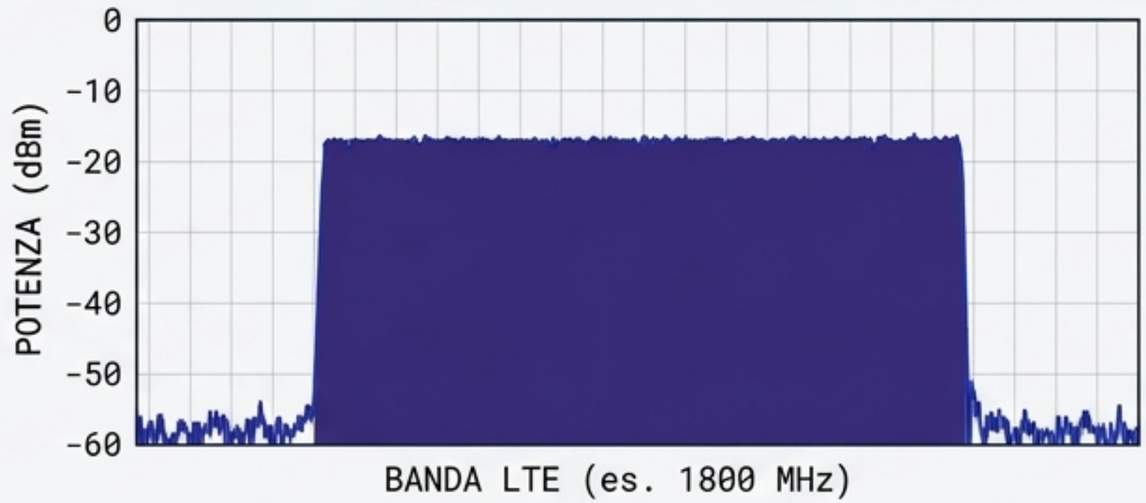
Trattiene il valore massimo registrato per ogni frequenza nelle ultime N acquisizioni.

Perché è Vitale in TSCM

- I segnali più pericolosi sono brevi o intermittenti (es. burst GSM, microfoni ad attivazione vocale).
- Minaccia Specifica: I moderni jammer GPS generano emissioni caratteristiche sulla banda L1 (1575 MHz), rilevabili come spike energetici anomali catturabili solo mantenendo il Peak Hold attivo per svariati minuti.

Firma Spettrale: Anatomia dei Segnali

Spiare.com

SEGNALE GSM (2G/3G)	SEGNALE LTE (4G)
	

GSM (2G/3G)	LTE (4G)
• **Firma Visiva:** Picchi stretti, multipli e irregolari (Burst). • **Tecnica:** TDMA (Slot temporali), larghezza canale stretta (200 kHz). • **Waterfall:** Strisce brevi e tratteggiate.	• **Firma Visiva:** Blocco largo, continuo, piatto e uniforme con bordi netti. • **Tecnica:** OFDMA, canali flessibili (1.4 - 20 MHz). Nessuna modulazione AM visibile. • **Waterfall:** Striscia solida, intensa e ininterrotta (es. VoLTE attivo).

La Minaccia Dormiente: Tracker e IoT

Il Vincolo Energetico

Capacità Batteria (C)

C = 100mAh
C = 1000mAh

$$T\ (Ore) = \frac{C\ (mAh)}{I\_medio\ (mA)}$$

Consumo Corrente Medio (I_medio)

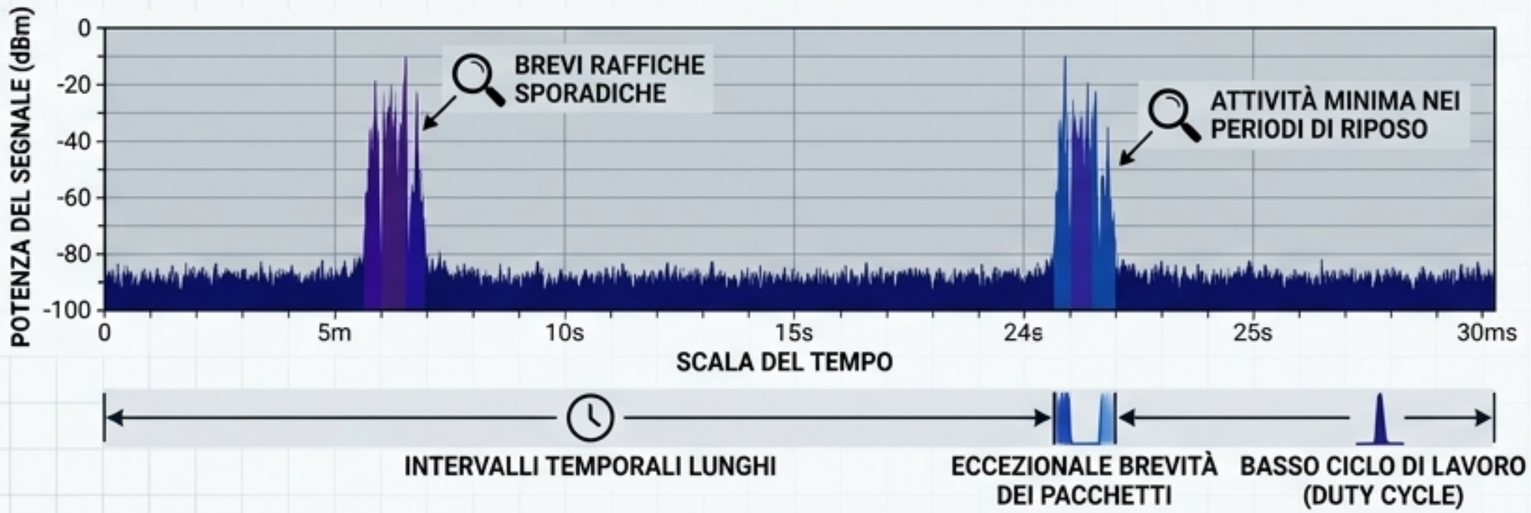
Standby: Dispositivo acceso, basso consumo (`I_standby`)

Attività: Dispositivo trasmette audio o dati, alto consumo (`I_active`)

`T (Ore)`: Autonomia Stimata in ore.
`C (mAh)`: Capacità della Batteria in milliampere-ora.
`I_medio (mA)`: Consumo di Corrente Medio in milliampere.

Per sopravvivere settimane, i dispositivi nascosti (Tracker GPS, sensori IoT) non possono trasmettere continuamente. Devono dormire.

La Firma RF



Diagnostica:
Brevità eccezionale dei pacchetti, **duty cycle** bassissimo, intervalli lunghi.

Rilevamento:
Richiede analisi Waterfall a lunga persistenza e triggering avanzato.

Identificazione del Target (Senza Intercettazione)

Rilevare la **Frequenza Centrale** del blocco LTE piatto (es. 847 MHz)

↓

Incrociare il dato con il **PNRF** (Piano Nazionale Ripartizione Frequenze)

Uplink B20 - 800 MHz	
TIM:	832 – 842 MHz
Vodafone:	842 – 852 MHz
WindTre:	852 – 862 MHz
Iliad:	Non assegnata

Spiare.com

⚠ TACTICAL NOTE

Un segnale centrato a **857 MHz** è **WindTre**, non Vodafone.
La **lettura visiva** senza l'incrocio con il PNRF porta a falsi positivi.

Protocollo Operativo TSCM: Le 5 Fasi

1. Calibrazione (Noise Floor)

Spegnere i dispositivi noti nell'ambiente.

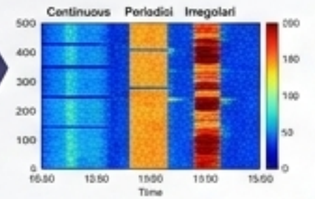
Acquisire per 30-60 secondi per stabilire il rumore di fondo.

2. Scansione (Peak Hold)

Mantenere Peak Hold attivo per 5-10 minuti.

Cattura le emissioni intermittenti, burst GPS e heartbeat.

3. Analisi Temporale



Osservare la struttura sul Waterfall.

Continui = Attivi.
Periodici = Standby/Polling.
Irregolari = Anomalia.

4. Contesto (PNRF)

Incrociare le frequenze anomale con le tabelle di assegnazione ministeriali (Operatore/Tecnologia).

5. Documentazione

Salvare screenshot con timestamp, frequenza centrale, larghezza di banda e potenza per la catena documentale.

Spiare.com

Sintesi: Il Confine Legale tra Metadati e Contenuti

Metadati RF (Lecito)

- Identificare presenza, pattern temporale, potenza, frequenza e operatore (tramite PNRF).
- Consentito: Analisi del Comportamento.
- Assimillabile all'uso di un analizzatore professionale. Pieno rispetto normativo.

Decodifica Traffico (Illecito)

- Intercettare l'audio, identificare numeri chiamanti o associare il segnale a persone senza mandato.
- Vietato: Analisi del Contenuto.
- Violazione dell'Art. 617 c.p. (Codice Penale).

⚠ TACTICAL NOTE

Il vero potere della bonifica TSCM non risiede nell'ascolto della comunicazione, ma nella maestria di **decifrare il comportamento del segnale elettromagnetico**.