00 OVERVIEW

SPECTRAL-OEM · OVERVIEW · HARDWARE · SUPPORTED · CTN · FULL BILL OF MATERIALS

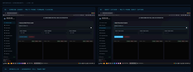
SPECTRAL-OEM · OEM SPECTRUM MANAGEMENT PLATFORM

SPECTRAL-OEM is a software-based, cloud-native OEM hardware and SDR management platform for fleets of Ettus USRP, LimeSDR, and HackRF devices. It provides centralized device provisioning, firmware management, real-time spectrum monitoring, GSM/LTE/5G protocol analysis, IMSI/IMEI capture, and automated security response — all from a single browser dashboard.

Deployed on a Raspberry Pi 5 or any Linux server, SPECTRAL-OEM turns distributed SDR hardware into a coordinated sensor network with full operator control over every device, every frequency, every protocol.

Supported hardware: Ettus USRP (B200, B210, N210, X310), LimeSDR (USB, Mini), HackRF One. Multi-device operation is supported on all platforms.

Fleet Overview Live dashboard showing all connected SDR devices, their status, firmware versions, and active operations.	**Auto Quiet** Automatically silences non-critical SDR devices when a critical operation starts, to prevent interference.	**Capture Burst** Single-shot IQ capture triggered by a specific event, saved to disk for offline analysis.	**Intercept** Real-time GSM/LTE/5G protocol decoding and IMSI/IMEI capture on selected frequencies.	**Archive & Plan** Long-term IQ recording and scheduled capture jobs for post-incident analysis.
Multi-Vendor Interface Unified management for Ettus USRP, LimeSDR, and HackRF devices from one browser tab.	**Live Spectrum** Real-time waterfall and FFT display, per-device frequency and gain control.	**Target IMSI Catcher** Forced 2G downgrade and IMSI capture against specified target subscribers.	**Silent SMS Sender** Stealth SMS delivery for presence verification and network probing.	**AT2 Counter** Automatic detection of 2G downgrade events and IMSI capture attempts.
GPS Catcher Passive GPS L1 C/A capture and decoding, with optional NMEA export.	**Target GMS Catcher** Multi-target IMSI capture across multiple GSM channels simultaneously.	**Silent SMS Sender** Stealth SMS delivery for presence verification and network probing.	**Burst Data Analyzer** Post-capture analysis of saved IQ files: protocol identification, timing, and frame extraction.	**Burst Data Intercept** Real-time GSM burst decoding and frame extraction from live spectrum.
Monitoring Continuous spectrum scanning with configurable alerts and threshold notifications.	**Active GMS Interceptor** Full GSM MITM: downgrade, IMSI capture, and SMS interception against a target.	**Operator's Map** Geographic visualization of cell towers and capture events on a map.	**Spectrum Hunt** Automated search for unknown transmitters across a configurable frequency range.	
Radio / Spectrum Live waterfall and FFT display, per-device frequency and gain control.	**Automated Response** Rule-based actions triggered by detection events: alerts, logging, and device control.	**Cell Database** Local database of observed cell towers, frequencies, and operators.	**Intercept / Video** Live video feed from camera devices, synchronized with SDR operations.	



01 SDR/GPS SERVER

SDR · GPS · SPECTRUM · SERVER · DEVICE MANAGEMENT

WHY YOU THE NEED

The Raspberry Pi 5 with a USRP B200 or LimeSDR Mini is a 2000 USD system. It ships with no firmware, no GPS, no remote access, no multi-device support, and no way to share the spectrum with anyone else. SPECTRAL-OEM turns that hardware into a shared, managed, remotely accessible sensor node. Multiple operators can connect from any browser, see the same live spectrum, and coordinate without stepping on each other's sessions.

B Multidimensional Multi-dimensional spectrum analysis: time, frequency, and power domains.	**Universal Binary** Single binary for Linux x86_64 and ARM64. Runs on Raspberry Pi 5 and any Linux server.	**Thin Client Logic** All processing on the server. Browser receives only what it needs to display.
Phase-Coherent Selection Multi-channel coherent receiver with per-channel frequency, gain, and bandwidth control.	**Web Tuning** Frequency, gain, and bandwidth control from any browser, from anywhere.	**Drop-Off** Lightweight client-side capture: IQ recording without full spectrum streaming.
Gain Control Per-channel gain control with automatic and manual modes.	**Local IMSI/IMEI Off** Disable IMSI/IMEI capture locally for privacy-sensitive deployments.	**Multi-Target Filter** Capture only specified IMSIs or IMEIs, ignore all others.
Multi-Channel Simultaneous capture on multiple frequencies from one SDR device.	**Operator Lockup** Exclusive device ownership per operator. Prevents conflicts between multi-operator sessions.	**Signal Strength Utility** Real-time RSSI measurement and logging for antenna alignment and site survey.
Multi-Operator Multiple operators connect to the same device simultaneously. Sessions are isolated.	**Remote Access** Full remote operation over network. Deploy anywhere, manage from anywhere.	**LTE Bandwidth Detect** Automatic LTE bandwidth detection from downlink signal.

02 CELL SCANNER

CELL · SCANNER · GSM · LTE · 5G · NEIGHBOR · TOWER · CAMPER

WHY YOU THE NEED

Knowing the cells you're actually connected to and the ones you're being forced onto is the difference between a working deployment and a black box. Rogue BTSs and IMSI catchers are a real threat in any deployment that matters. This module gives the operator full visibility into every cell in range, its signal strength, its neighbor relations, and any anomalies that suggest an attack in progress.

G Cells Active GSM, UMTS, LTE, 5G NR cell towers in range.	**Local MCC/MNC Off** Ignore cells from your own network. Focus on foreign towers only.	**Neighbor / Serving / Camper** Full neighbor relation table. Detect cells being forced as neighbors.	
ARFCN Discovery Automatic channel number detection across all supported bands.	**Operator Lookup** Identify operators from MCC/MNC against a local database.	**Signal Strength Utility** Real-time RSSI measurement and logging for antenna alignment and site survey.	**LTE Bandwidth Detect** Automatic LTE bandwidth detection from downlink signal.

03 BURST CATCHER

BURST · CAPTURE · GSM · LTE · ANALYSIS

WHY YOU THE NEED

Most attacks leave a trace in the raw spectrum. Burst Catcher captures every GSM burst and LTE frame in a configurable window, then hands them off for offline analysis. Protocol identification, timing extraction, and frame decoding happen after the fact, not in real time.

Use cases: post-incident forensics, rogue BTS detection, protocol reverse engineering, training data for custom ML classifiers, regulatory compliance logging.

ARFCN / Phase Target specific channels or capture all active channels.	**Idle Burst Filter** Discard idle frames automatically to reduce storage.	**Up to 4 Phases** Multi-channel capture. Each phase runs independently.	
Phase Count Number of independent capture phases. Each phase runs on a separate channel.	**Hard Capture** Force capture regardless of signal quality. Useful for weak signal environments.	**Drop-Off** Lightweight client-side capture: IQ recording without full spectrum streaming.	**Radio Off / Enable** Remote control of the SDR hardware. Power cycle or re-enable from the dashboard.

04 SILENT SMS

SILENT · SMS · 3 · TYPE · 0 · GSM · PRESENCE · PROFILE · AUDITING

WHY YOU THE NEED

The Silent SMS (type 0 SMS) is a GSM feature that delivers a message without a visible notification. The handset receives it, the network logs it, the operator's subscriber profile updates, and the user sees nothing. It's used for presence verification, network probing, and subscriber profile updates in legitimate telecom operations.

In security research, it is used to confirm a subscriber's current cell tower, detect roaming status, and map network boundaries. The same mechanism that makes it useful for telecom operations makes it useful for tracking a specific target.

Silent SMS Send a type 0 SMS to a target MSISDN. Confirms presence and current cell tower.	**Simple SMS** Standard SMS delivery. Visible to the recipient. Used for comparison testing.	**GSM SMS Sender** Full SMS sender with encoding support.	
Mobile Used Identify which phone model is being used by the target. Useful for profiling and tracking.	**SMS Type Selector** Choose between Silent SMS, Flash SMS, and standard SMS per message.	**SMS Mobile Detector** Automatic detection of active mobile subscribers in the target network.	**Burst Sent Filter** Suppress repeated Silent SMS to the same target within a configurable window.
Message Count Number of Silent SMS messages sent to the target this session.	**Auth Log** Full audit log of all Silent SMS operations. Timestamps, targets, and results.		

05 IMSI CATCHER

IMSI · CATCHER · GSM · 2G · DOWNGRADE · CAPTURE · MITM · SMS · TARGETED

WHY YOU THE NEED

The IMSI is the permanent identity of a subscriber on the network. Once the network knows its IMSI, it can page it, route calls to it, and deliver SMS to it. Normal 4G/5G operation keeps the IMSI encrypted. Forcing a device into 2G strips that protection and makes the IMSI visible in plaintext on the air interface.

This module forces target devices into 2G downgrade, captures the IMSI, and logs it against a target list. The operator then decides what to do with the capture: alert, log, or trigger a follow-up action.

CLASS	DESCRIPTION
`IMSI`	Subscriber identity. Permanent identity of the subscriber.
`TMSI`	Temporary identity. Rotated periodically by the network.
`IMEI / IMEISV`	Device identity. Hardware fingerprint. Persistent across SIM changes.
`Cipher / Downgrade`	Encryption negotiation. Forced downgrade to weaker or no encryption.
`MCC / MNC`	Mobile Country Code and Mobile Network Code.
`LAC / CI`	Location Area Code and Cell Identity. Physical location of the cell.
`Auth`	Authentication. Challenge-response exchange between SIM and network.
`Paging`	Network paging. Used to locate a subscriber before a call or SMS.
`Attach / Detach`	Registration events. Device joining or leaving the network.
`Handover`	Cell handover. Device moving between cells.
`Location Update`	Periodic location update. Device reporting its current cell to the network.

Passive Surveillance Passive IMSI/IMEI capture without downgrade. Monitor all subscriber activity on the target network.	**Live Search Filter** Filter the capture stream by IMSI, IMEI, or MCC/MNC in real time.	**Identity Correlation** Cross-reference IMSI and IMEI to track device changes and SIM swaps.
Multi-Target Simultaneous IMSI capture against multiple target subscribers.	**Auto Downgrade** Automatic 2G downgrade on supported devices. Forces IMSI capture without manual intervention.	**Alert On Persistence** Notify when a target IMSI appears for the first time or after a configurable absence.

06 TARGET IMSI CATCHER

TARGETED · IMSI · SUBSCRIBER · CAPTURE · TRACKING · MITM · STATIONARY

WHY YOU THE NEED

The Target IMSI Catcher is the operational version of the IMSI catcher. Instead of capturing all IMSIs in range, it locks onto a specific target IMSI. The operator enters a target list, and the system ignores everything else. Alerts fire only when the target appears.

Use cases: law enforcement surveillance, asset tracking, presence verification, network boundary mapping. Legal and ethical constraints apply. Deploy only against subscriber identities you have authorization to track.

Target IMSI Single IMSI or comma-separated list of target subscriber identities.	**Detection Events** Log of every target IMSI detection with timestamp, cell, and signal strength.	**Alert Mode** Notify on first detection, on every detection, or on target disappearance.	

CLASS	DESCRIPTION
`IMSI`	Subscriber identity. Permanent identity of the subscriber.
`TMSI`	Temporary identity. Rotated periodically by the network.
`MCC / MNC`	Mobile Country Code and Mobile Network Code.
`LAC / CI`	Location Area Code and Cell Identity. Physical location of the cell.
`Auth`	Authentication. Challenge-response exchange between SIM and network.
`Paging`	Network paging. Used to locate a subscriber before a call or SMS.
`Attach / Detach`	Registration events. Device joining or leaving the network.
`Handover`	Cell handover. Device moving between cells.
`Location Update`	Periodic location update. Device reporting its current cell to the network.

07 WORKSPACE

WORKSPACE · SESSION · MANAGEMENT · MULTI-OPERATOR · SHARED · PRESENCE

WHY YOU THE NEED

Multi-operator deployments need a shared workspace. SPECTRAL-OEM lets multiple operators connect to the same device, see the same live spectrum, and coordinate without stepping on each other's sessions. Presence indicators show who is connected and what they are doing. Session locks prevent two operators from starting conflicting operations. Operator logs provide a complete audit trail of every action taken on the system.

Initiative Workspace Shared workspace for multi-operator sessions. Presence indicators show who is connected and what they are doing.	**Other Workspaces** Switch between workspaces. Each workspace is independent.	**Workspace Log** Shared operation log. Every action by every operator is recorded with timestamp and operator identity.

08 PROCESSING

PROCESSING · CAPTURE · ANALYSIS · DEMODULATION · STORAGE · QUEUE · JOBS

WHY YOU THE NEED

Raw IQ samples are useless without processing. Burst Catcher captures GSM bursts and LTE frames, but the operator still needs to demodulate, decode, and extract the relevant information before any analysis can begin. This module handles the full processing pipeline: from raw IQ to decoded frames, ready for the next stage.

Batch processing runs on saved IQ files after the fact. Real-time processing runs on live streams as they are captured.

Auto Jobs On Capture Automatically queue processing jobs when new IQ files are saved.	**Auto Demodulate, GMS** Automatic GSM demodulation on saved IQ files. Runs in the background.	**Process Log** Processing job log. Shows queued, running, and completed jobs with timestamps and results.	

09 A5/1 CRACKER

A5/1 · CRACKER · GSM · 2G · CIPHER · TABLE · DECRYPTION · RAINBOW

WHY YOU THE NEED

A5/1 is the GSM voice encryption cipher. Rainbow table cryptanalysis can recover the session key from a captured ciphertext in minutes. Once the session key is recovered, every frame in that session can be decrypted. This module automates the entire workflow: from raw IQ capture to decrypted GSM frames.

The pipeline: Burst Catcher captures GSM bursts → Processing extracts the relevant frames → A5/1 Cracker recovers the session key → Decrypted frames are available for analysis.

A5/1 CRACK Start a cracking job against a captured session. Requires rainbow tables.	**Rainbow Tables** Manage rainbow table sets. Upload, select, and monitor table coverage.	**IQ Decrypt Map** Map decrypted frames back to their original IQ timestamps. Enables time-aligned analysis.	
Cracked Frames Log Log of successfully decrypted frames. Shows session key, frame count, and timestamp.	**Decrypt Stream** Live decryption of GSM frames using recovered session keys.	**Burst Frames** Extract individual GSM frames from saved IQ files. Output ready for further analysis.	**Log** Cracker log. Shows job status, errors, and table coverage.

10 CRACKED DAT

A5/1 · DATA · CRACKED · DATA · DECRYPTED · DOWNLOAD · DELETE · STORAGE

WHY YOU THE NEED

Raw A5/1 cracker output is useless for most analysis. Decrypted frames need to be stored, indexed, and exported in a format that downstream tools can read. This module manages the full lifecycle of cracked data: from the moment it lands on disk to the moment it is deleted.

Without access to this data, the cracker runs but the results are lost. Storage is the last mile between cracking and analysis.

DECRYPTED DATA `.dat` `.bin` `.raw` Decrypted GSM frames ready for analysis. Binary format, one frame per record.	**DOWNLOAD** Download a file to your local machine. Use for offline analysis or archival.	**DELETE** Remove a file from the server. Free disk space. Irreversible.	
DELETE ALL Remove all decrypted data from the server. Use with caution.	**Refresh** Refresh the file list. Shows new files as they are created by the cracker.		

11 REAL-TIME INTERCEPT

REAL-TIME · INTERCEPT · GMS · 2G · TMSI · SMS · STREAMING

WHY YOU THE NEED

Burst Catcher captures GSM bursts and LTE frames for offline analysis. Real-time intercept does the same thing live, as the frames arrive, so the operator can see what is happening on the network right now instead of waiting for a capture to finish and a file to be processed.

Use cases: IMSI collection, live SMS interception, real-time TMSI tracking, and immediate alerting on specific events.

ARFCN Target specific channels or capture all active channels.	**IQ Ring / Mem** Ring buffer size in memory. Controls how much recent IQ is available for retrospective analysis.	**Video Video** Enable video capture alongside SDR. Synchronized with the SDR capture timeline.	
ARFCN Count Number of channels being monitored simultaneously. Each channel runs independently.	**IQ Ring / Mem** Ring buffer size in memory. Controls how much recent IQ is available for retrospective analysis.	**Video Video** Enable video capture alongside SDR. Synchronized with the SDR capture timeline.	**Intercept Streams / IQ** Live streams. Subscribe to receive real-time IQ and decoded frames.

12 MONITORING

MONITORING · GMS · TMSI · SMS · LOCATION · TARGETS · ALERTS · TIME · DISPLAY

WHY YOU THE NEED

Intercept gives you the raw stream. Monitoring gives you the operational layer on top of it: which targets are being tracked, which SMS are being sent, which TMSIs are being assigned, and when something changes that matters.

Use cases: target presence tracking, SMS monitoring, TMSI rotation tracking, and alerting on specific events.

Location Tracking Track target location based on cell tower changes. Log every handover and location update.	**Alerts Table** Log of all alerts. Filterable by type, severity, and time. Exportable for analysis.	**Alerts Time** Display alerts in local time or UTC. Toggle between formats.	
Alerts Count Total number of alerts in the current session. Resets on restart.	**Alerts Clear** Clear all alerts from the current session. Irreversible.	**Intercept Streams / IQ** Live streams. Subscribe to receive real-time IQ and decoded frames.	

13 CACHED SMS INTERCEPTOR

SMS · CACHED · GSM · LTE · 3GPP · TS23.040 · DECODER · STORAGE · DELETE · EXPORT

WHY YOU THE NEED

The Silent SMS module sends SMS without a visible notification. Cached SMS Interceptor is the other side of that: it decodes and stores every SMS that arrives on the network, including Silent SMS, standard SMS, and SMS-PP commands. Without this module, Silent SMS sent by the operator leave no record on the system.

Use cases: presence verification, network probing, subscriber profile updates, and long-term SMS monitoring for specific targets.

CLASS	DESCRIPTION
`Silent SMS`	Type 0 SMS. Delivered without a notification. Used for presence verification.
`Flash SMS`	Type 1 SMS. Displayed immediately on the handset. Used for network probing.
`Normal SMS`	Standard SMS. Visible to the recipient. Used for comparison testing.
`Type 2`	Type 2 SMS. Used for network probing and subscriber profile updates.
`Type 3`	Type 3 SMS. Used for network probing and subscriber profile updates.
`Type 4`	Type 4 SMS. Used for network probing and subscriber profile updates.
`Type