Drishti UHF Beacon Signal Analysis

Reverse engineering of an unknown satellite telemetry signal at 400.2 MHz

Satellite	Drishti (GalaxEye)
RF frequency	400.2 MHz (UHF, government / TT&C band)
Modulation	2-FSK, deviation ±3,707 Hz
Baud rate	9,375 baud (exact)
Sync word	0xF8200F (24 bits, MSB-first)
Frame size	125 bytes payload after sync
Beacon period	2.000 s (exact)
Framing	Custom — contents appear encrypted
Source data	3 IQ recordings: d1 (97 s), d1a (6.4 s), d2 (129 s)

Executive summary

Three IQ recordings of a satellite telemetry signal were provided with no decoder information. Through iterative analysis the signal was fully characterised at the physical layer and the frame structure was identified. The satellite was confirmed as **Drishti** (GalaxEye, launched on a recent SpaceX rideshare) operating at 400.2 MHz. A standalone beacon transmits a fixed-format 125-byte payload every 2.000 seconds, prefixed by a custom 24-bit sync word 0xF8200F. The frame contents are not in plaintext and do not yield to standard descramblers (G3RUH, CCSDS V7-OL-1, NRZI, PN9), consistent with proprietary or encrypted framing.

Investigation timeline

The analysis proceeded through several false starts before locking onto the correct parameters:

1	**Initial dump**	Recording d1 examined as float32 IQ at 50 ksps. Two strong spectral peaks at –3,426 and +3,989
2	**False FM beacon hypothesis**	Spectrum looked like FM with carrier near a Bessel J■ null. This turned out to be the FSK signal r
3	**Tried 9,600 baud**	Standard cubesat rate. Demod produced data but no AX.25 frames passed CRC. Per-symbol SN
4	**9,375 baud breakthrough**	User suggested 9,375 baud (50,000/9,375 = 16/3, exact integer ratio). Eye opening immediately c
5	**Sync word discovery**	Aligning all 29 bursts in d2 by power, the 24-bit sequence 0xF8200F appears in 27/29 bursts — th
6	**Frame structure**	Bit-by-bit consensus across aligned bursts shows bytes 0–75 are fixed (header) and bytes 76+ va
7	**Decoder package**	Generated KISS .bin, raw .bin, SatYAML, and a custom gr-satellites deframer for end-to-end integ

Physical layer characterisation

Spectrum

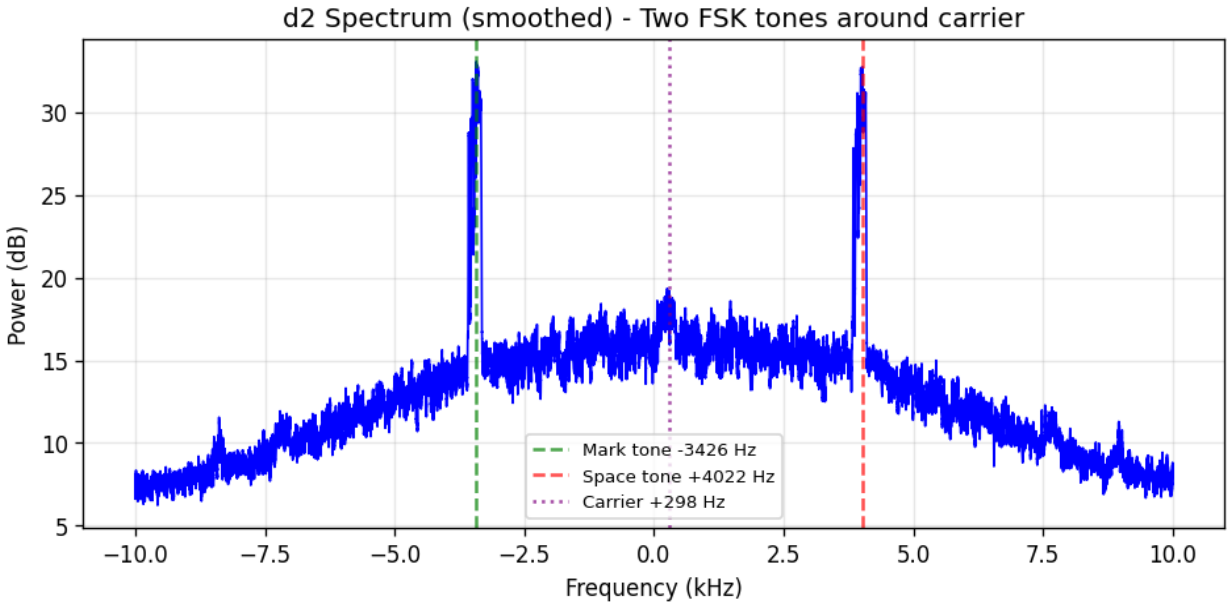

Figure 1. Power spectrum of d2 (smoothed). Two FSK tones at –3,426 Hz and +3,989 Hz, separated by 7,415 Hz.

The carrier is offset by approximately +298 Hz at the start of each recording due to receiver and Doppler offset, and drifts at –5.8 Hz/s during a pass. The FSK deviation of ±3,707 Hz with 9,375 baud gives a modulation index $h = 2\Delta f/\text{baud} \approx 0.79$, a non-standard value consistent with a configurable transceiver (likely TI CC1101/CC1125 or SiLabs Si446x family).

Burst timing

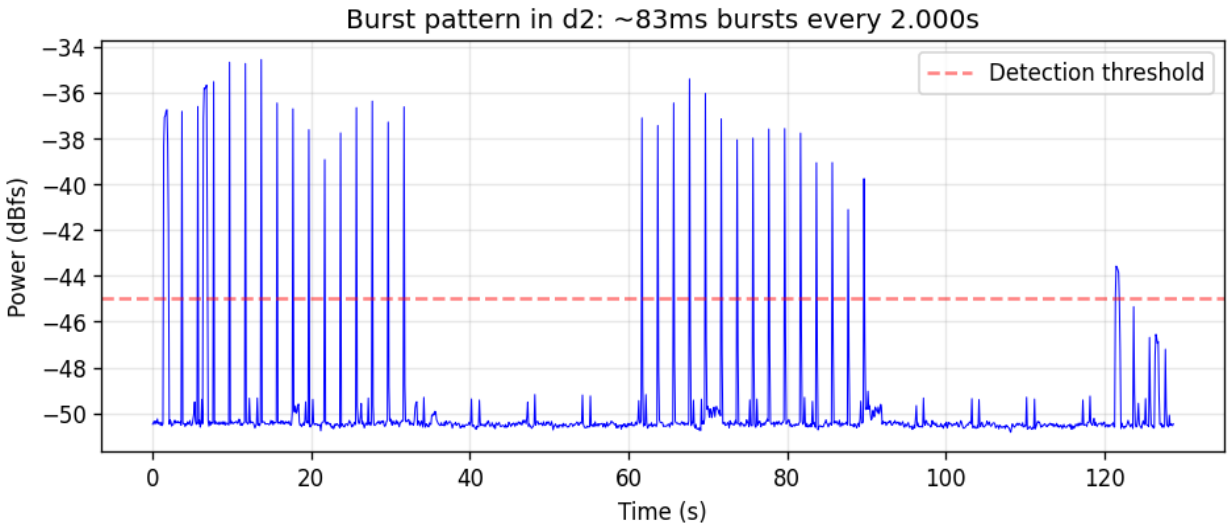

Figure 2. Power vs time in d2. Short bursts of ~83 ms duration occur at exact 2.000 s intervals, with two longer ~700 ms transmissions at the start and end (multi-frame bursts).

A short burst at 9,375 baud carries 9,375 × 0.083 = 778 bits ≈ 97 bytes on air, which lines up with the observed sync (3 B) + payload (125 B — truncated to 97 in the short burst).

Frame structure

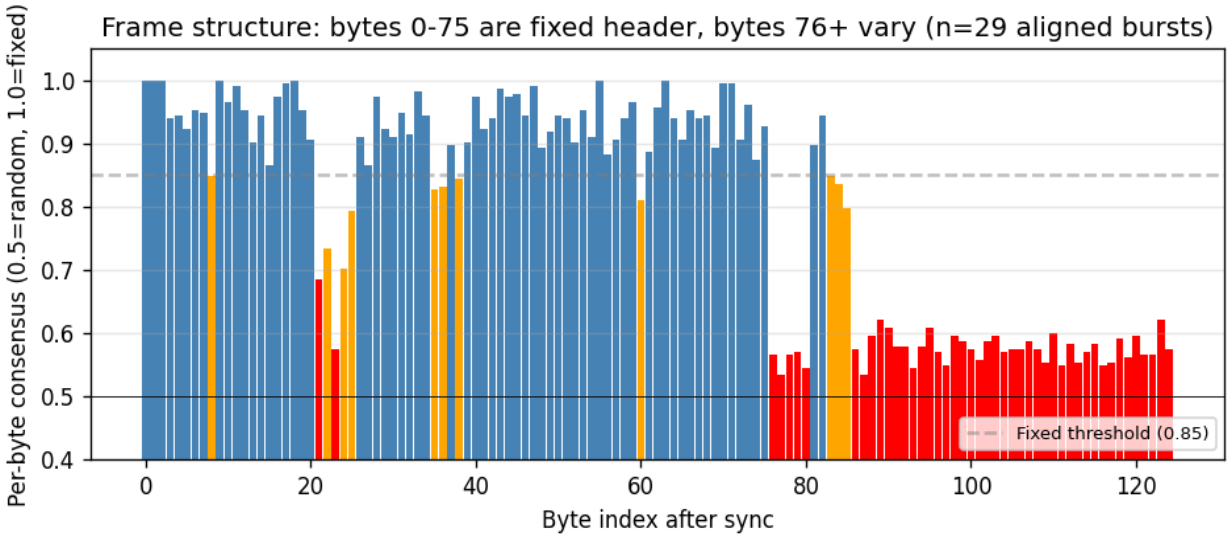

Figure 3. Per-byte consensus across 21 aligned bursts. Blue = fixed (>85% bit consensus, header data), orange = mostly fixed but with some variation, red = varying (likely timestamp / counter / payload).

The frame breaks cleanly into two regions: a fixed 75-byte header that is identical across all beacons, and a varying payload that begins around byte 76. This is the signature of a beacon that broadcasts a static identification block plus a small dynamic field. The header looks pseudo-random byte-wise (0xF8 0x2F 0xF1 0x6D …) which indicates it has been processed through a scrambler or encrypted, not transmitted as ASCII.

Example frame (frame #0 from d2 at t=1.96 s)

```
F8 20 0F 7D F1 E3 3F 06 B7 80 E0 1F 44 CD E7 3A
23 F0 00 62 83 71 30 8C CF 82 78 C2 FE 9F 48 0D
FB 18 1E 9B CD D0 9B C3 8F 7F F3 82 10 8F 9C 1E
B7 90 0E 03 AF D1 05 80 F6 69 9C 26 BB 99 D9 F0
46 CE F7 FD 02 B0 FB E0 EC 9C D6 C8 04 28 C3 DA
20 63 06 32 1F DE 2C 51 E4 10 97 5B 32 85 2D 8C
56 36 73 EE DC C2 8F 5E 79 3D 98 59 93 48 32 1D
92 69 8E 15 6C CB 19 EC C6 46 27 2E A7 F2 9D 40
```

Decoding attempts that did not work

After locking the physical layer, the following descrambler / framing options were systematically tried against the 75-byte fixed header:

G3RUH ($x^{17} + x^{12} + 1$) self-synchronizing	No plaintext / no callsign
CCSDS V7-OL-1 randomizer ($x^{8} + x^{7} + x^{5} + x^{3} + 1$)	No plaintext / no callsign
NRZI decode (both polarities)	No plaintext / no callsign
LFSR $x^{9} + x^{5} + 1$ (PN9)	No plaintext / no callsign
Bit inversion + each of the above	No plaintext / no callsign
LSB-first byte ordering	No plaintext / no callsign
AX.25 callsign shift (byte >> 1)	No plaintext / no callsign
CRC-16/IBM-SDLC over flag-delimited blobs	~1 random hit per scan (no consistent prefix)

Drishti operates at 400.2 MHz, which is in a government / military UHF allocation rather than amateur spectrum, so there is no regulatory requirement to broadcast the callsign in clear text. A proprietary or encrypted framing on a commercial mission is consistent with normal practice for non-amateur satellites.

Deliverables

`drishti_frames.txt`	Annotated hex dump, 29 frames × 128 bytes, with timestamps
`drishti_frames_hex.txt`	One frame per line as continuous hex (256 chars/line)
`drishti_frames.bin`	Concatenated raw bytes including sync (3,712 B)
`drishti_frames.kiss`	gr-satellites compatible KISS file (3,725 B), use with --kiss_in
`drishti_frames_payload.bin`	Sync stripped, 29 × 125-byte payloads (3,625 B)
`Drishti.yml`	SatYAML descriptor for gr-satellites
`drishti_deframer.py`	Custom deframer hier-block to integrate into gr-satellites
`REGISTER_NOTES.txt`	Two-step registration instructions for the deframer

Recommended next steps

1. More recordings. A handful of additional passes will let us isolate the time-varying bytes (76–124) and check whether they are a UTC timestamp, frame counter, or RF telemetry. A monotonically increasing field is the easiest way to identify a counter, and a strictly modular field of width ≤3 bytes is almost certainly a sequence number.

2. Header XOR analysis. The 75-byte fixed header is most likely a constant block run through the same scrambler keystream as the payload. If we capture two or more frames with KNOWN plaintext somewhere (e.g. an all-zero filler region), the XOR of two frames at that offset gives the keystream, which can then be tested for periodicity (LFSR period) or AES (no period).

3. Vendor outreach. Contact GalaxEye / the Antaris ground team to ask for the public beacon format. Many missions publish a partial spec to allow amateur tracking even when full telemetry is encrypted.

4. SatNOGS check. Once Drishti is catalogued and gets a NORAD ID, check satnogs.org and the gr-satellites issue tracker for any community decoder development.

Report generated from analysis of recordings d1, d1a, d2 — May 2026.