

FEDERAL BUREAU OF INVESTIGATION

CHICAGO FIELD OFFICE — CYBER / ELECTRONIC SURVEILLANCE REPORT

Time-sensitive — ongoing conduct; contemporaneous forensic evidence enclosed

ELECTRONIC / MAIL / PORTAL TRANSMITTAL

Continuing electronic surveillance of a federal litigant — 39 timestamped Wi-Fi captures enclosed

TO:	FBI Chicago Field Office — Complaint Duty Agent / Cyber Task Force 2111 W. Roosevelt Road, Chicago, IL 60608
SEND VIA:	Online: tips.fbi.gov + ic3.gov Tel: (312) 421-6700 U.S. Mail (hard copy)
FROM:	Ehab Allababidi 8516 W. Winona St., Chicago, IL 60656 (773) 920-0030 defcon5ready@gmail.com
DATE:	July 15, 2026
RE:	Evil-Twin AP 1a:60:41:7a:87:2x cloning router 18:60:41:2a:87:2x; CellSpot femtocells
REF. CASES:	N.D. Ill. Nos. 1:25-cv-15800, 1:26-cv-01077, 1:25-cv-15786; S.D.N.Y. No. 1:26-cv-05881

SUMMARY

PAGES: 51 (incl. this cover + exhibit packet w/ signed declaration & SHA-256 manifest)

Report of suspected ongoing illegal interception (18 U.S.C. §§ 2511, 1030) and obstruction/retaliation against a federal litigant (§§ 1512, 1513): a hidden access point cloning the home router's MAC (Evil Twin 1a:60:41:7a:87:2x), a second cloned radio, and CellSpot cellular femtocells — the same infrastructure filed at Dkt. 32/37/51/61, documented still present July 11–13, 2026.

REQUEST FOR INVESTIGATION — ILLEGAL ELECTRONIC SURVEILLANCE OF A FEDERAL LITIGANT

Federal Bureau of Investigation — Chicago Field Office

2111 W. Roosevelt Road, Chicago, IL 60608

Attn: Complaint Duty Agent / Cyber Task Force

Also submitted via tips.fbi.gov and the Internet Crime Complaint Center (ic3.gov)

To the Special Agent in Charge and the Complaint Duty Agent:

I write to report what I believe to be ongoing illegal electronic surveillance of my home and communications, and to provide contemporaneous, self-authenticating forensic evidence. I am a pro se federal litigant; the activity is directly connected to matters already pending before the U.S. District Court for the Northern District of Illinois, and I have previously filed evidence of this same network on that docket. The thirty-nine enclosed captures, taken July 11-13, 2026, document that the network is **still present and adapting to my countermeasures**. I believe these indicators are consistent with continuing federal offenses, and I ask that they be examined now, while the emitters are live and can be located by direction-finding.

THE FORENSIC FINDING, IN PLAIN TERMS

Across the period **July 11 through July 13, 2026 (documented), continuing**, the undersigned captured thirty-nine (39) Wi-Fi spectrum scans at the residence, **8516 W. Winona St., Chicago, IL 60656**, using a standard commercial analyzer. Each image carries the device clock and an embedded EXIF DateTimeOriginal timestamp. They show a hidden access point at MAC **1a:60:41:7a:87:2x** at approximately zero metres from the home. That address is a **locally-administered bit-flip clone** of the resident's legitimate router at **18:60:41:2a:87:2x**: the first octet is altered from 18 to 1a (which sets the IEEE 'locally administered' bit, i.e. the address is hand-assigned, not burned in by a manufacturer) and the fourth from 2a to 7a. The IEEE registry returns **no manufacturer** for 1a:60:41 — it is not a registered hardware vendor prefix. In plain terms, an unauthorized device is advertising a clone of the home router's hardware identity: an **Evil Twin**.

The clone does not behave like a passing neighbor signal. It **follows the legitimate router across every band** (2.4 GHz Ch. 2/3, Exhibits E-1, E-5, E-30; and 5 GHz Ch. 40/153, Exhibits E-11, E-14, E-31), it shows the same 0-metre distance and near-identical signal, and **it tracked the router through a WPA3 / Wi-Fi 7 security upgrade in real time**: on July 13, 2026 the hidden clone began advertising the identical **WPA3 / Wi-Fi 7** profile on the same Ch. 40 (Exhibits E-27, E-28, E-31, E-32). Ordinary consumer hardware does not mirror another network's security generation this way; a device that re-clones the network within hours of each hardening step is adapting to the resident's countermeasures, not producing a random or transient signal. A second cloned radio is also present — **3e:f0:83:x7:d2:1c**, a 3c-3e bit-flip of the router's Arcadyan sibling 3c:f0:83 (Exhibits E-7, E-11) — matching the 'second 5 GHz Evil Twin' at Dkt. 51.

The named devices are not what their SSID names suggest. Manufacturer resolved from the IEEE OUI registry (Exhibit: Device Identification table): the '**CellSpot**' nodes (38:2c:4a:97:78:68/69/6a) are **ASUSTek** silicon — the T-Mobile 4G LTE CellSpot is an ASUS-built **femtocell, a home 'mini cell tower'** that carries licensed cellular traffic and pulls nearby phones onto itself; one such unit here broadcasts three SSIDs at once (Exhibits E-15, E-18). The **AT&T-named; nodes** ATT4k3T6T2 (f8:9b:6e) and ATTfSnPQ8S (ac:8f:a9) run on **Nokia Solutions and Networks** carrier small-cell silicon, not consumer Wi-Fi (Exhibit E-24) — the 'Nokia femtocell / IMSI-catcher' class pleaded at Dkt. 37 and Dkt. 51. Notably, '**Ring Setup 8d**' (Exhibit E-16) is an **open, unauthenticated access point on Texas Instruments silicon** (OUI 24:7d:4d) — a TI SimpleLink RF

transceiver whose operating band and transmit power are set in firmware. A genuine Ring emits a 'Ring Setup' SSID only for the few minutes of first-time pairing and then becomes a silent client; a **persistent open 'Ring Setup' AP** is consistent with a reconfigurable RF part left in pairing mode as an open join surface at close range.

A signal strength as high as **-20 dBm at ~0 metres** (Exhibit E-29) is consistent only with an emitter essentially at the antenna — inside or immediately adjacent to the residence. As the undersigned addressed at Dkt. 32, the FCC caps consumer Wi-Fi at roughly 1 watt (30 dBm EIRP); a received level this high, together with a software-defined TI part capable of elevating output and shifting bands, is consistent with a device operating **outside typical Part 15 power and band parameters** — a condition an FCC field office can confirm or exclude by measurement. This is the same infrastructure already placed before the U.S. District Court in **Case No. 1:25-cv-15800** (Dkt. 32 [6 GHz Evil Twin 1a:60:41:7a:87:22 and power analysis]; Dkt. 37 [credential compromise / femtocells]; Dkt. 40 [MITM contamination]; Dkt. 51 §III ['Evil Twin' network, 26 hostile devices, second 5 GHz twin]; Dkt. 61 [consolidated forensic]). These July 11–13, 2026 captures document that the same rogue-AP and femtocell indicators **remained present and active** — consistent with a continuing course of conduct.

WHAT IS NEW IN THESE CAPTURES (BEYOND THE DOCKET)

The record already names the 6 GHz Evil Twin **1a:60:41:7a:87:22** and the second 5 GHz twin (Dkt. 32, 51, 61). These captures add discrete, previously-undocumented facts:

- 1. New band-siblings of the Evil Twin.** The clone now also occupies **1a:60:41:7a:87:20 (2.4 GHz)** and **1a:60:41:7a:87:21 (5 GHz)** — the :20 and :21 companions of the docketed :22 6 GHz BSSID (Exhibits E-1, E-11, E-14). The clone has expanded from 6 GHz to every band the router uses.
- 2. Real-time WPA3 / Wi-Fi 7 mirroring.** Not previously documented: the hidden twin now advertises the router's newest WPA3 / Wi-Fi 7 profile on Ch. 40 (Exhibits E-27, E-31) — consistent with an operator that re-clones after each hardening step.
- 3. Per-band BSSIDs of the second twin.** 3e:f0:83:17:d2:1c (2.4 GHz) and 3e:f0:83:97:d2:1c (5 GHz) (Exhibits E-7, E-11).
- 4. Specific femtocell identities.** The Dkt. 37/51 'Nokia femtocells' now have concrete BSSIDs: ASUS CellSpot 38:2c:4a:97:78:68/69/6a and Nokia NSN f8:9b:6e:40:cb:c4 / ac:8f:a9:48:73:54.
- 5. Named IoT nodes whose silicon contradicts the name.** 'Ring Setup 8d' on Texas Instruments (24:7d:4d), 'Ring-614685' on USI (3c:e1:a1), and '[fridge]' on Seongji (88:57:1d) — camera/appliance-labelled radios acting as access points at the home.
- 6. Rotating locally-administered clones.** Single radios presenting multiple spoofed BSSIDs (76/6e/7a:63:9c:f4:93:cd; 52:a6:e6:93:c4:2e/2f; 42:0f:c1:8d:0b:d6/d0) — a surveillance-mesh signature.

METHODOLOGY AND WHY THE READINGS ARE RELIABLE

The captures were made with a commercially available Wi-Fi spectrum analyzer on a personal Android handset, held inside and immediately around the residence. The analyzer passively listens for the beacon and probe-response frames that every access point broadcasts; it does not transmit, inject, or connect. For each access point it records the **BSSID** (the radio's 48-bit hardware address), the SSID (network name, or "HiddenSSID" when suppressed), the channel and center frequency, the security suite (WPA2/WPA3, PSK vs. EAP), the received signal strength in dBm, and an estimated distance derived from that signal. Because the

BSSID is transmitted in the clear in every beacon, a cloned or spoofed BSSID is directly observable — which is exactly how the Evil Twin is caught.

Reading the two forensic tells. First, the **locally-administered (U/L) bit**: the second-least-significant bit of the first octet of a MAC address is, by IEEE 802 standard, set to 1 only when the address is hand-assigned rather than burned in by a manufacturer. The router's real address begins 18 (...0001 1000, U/L bit = 0, a factory address); the clone begins 1a (...0001 1010, U/L bit = 1, a software-set address). A legitimate second router does not spontaneously appear wearing a hand-edited copy of your address. Second, **received power versus distance**: free-space path loss means signal falls predictably with range, so a reading near **-20 to -30 dBm implies an emitter within a metre or two** of the phone. Repeated 0-metre, -20 dBm hidden emitters are not neighbors across a street; they are devices in or against the home.

AUTHENTICATION AND CHAIN OF CUSTODY

The enclosed packet is self-authenticating. It opens with a **Declaration of Authenticity and Chain of Custody** executed under penalty of perjury (28 U.S.C. § 1746; 735 ILCS 5/1-109), in which the undersigned attests that he personally captured each screenshot, that the images are true and unaltered, and that the on-screen and EXIF timestamps are the device's own. It closes with a **SHA-256 Hash Manifest** fixing a cryptographic fingerprint of every native file: any later change to a file — even a single pixel — alters its hash and is detectable by re-computation. The native files, with intact EXIF metadata, are preserved and available for forensic examination on request.

WHY THIS TARGETS A PROTECTED PERSON, AND WHY IT MATTERS

The undersigned is the pro se plaintiff and petitioner in pending federal proceedings in the Northern District of Illinois: a civil RICO / § 1983 action, No. 1:25-cv-15800 (Hon. Jorge L. Alonso, Mag. Judge Laura K. McNally); related CFAA cyber-sabotage matters, Nos. 1:26-cv-01077 and 1:25-cv-15786; a habeas matter, No. 1:25-cv-15181; and a related action in the Southern District of New York, No. 1:26-cv-05881. The court record already documents this same infrastructure: the “Evil Twin” network and 26 hostile devices (Dkt. 51 §III), the Nokia/CellSpot femtocells functioning as IMSI-catchers (Dkt. 37), the 6 GHz twin and the FCC power analysis (Dkt. 32), the man-in-the-middle contamination of the undersigned's legal-drafting tools (Dkt. 40, reporting foreign control artifacts and CHINANET IP 182.42.105.144), and the consolidated forensic record (Dkt. 61).

Electronic surveillance directed at a litigant's communications and legal work product during active litigation, if confirmed, bears directly on the obstruction and witness-interference claims already pleaded in the RICO action. The prohibitions implicated include **18 U.S.C. § 2511** (interception of electronic communications), **18 U.S.C. § 1030** (unauthorized access to protected computers), and **18 U.S.C. §§ 1512 and 1513** (obstruction of, and retaliation against, a party and witness). The documented pattern — a router clone that reappears within hours of each security upgrade, alongside cellular small-cell hardware at close range — is consistent with sustained, targeted activity rather than a transient or accidental event, and warrants investigation.

THE FEDERAL OFFENSES THESE INDICATORS IMPLICATE

- 1. 18 U.S.C. § 2511 (interception of electronic communications).** The Evil Twin at 1a:60:41:7a:87:2x advertises a clone of my router's hardware identity, so that traffic intended for my network can be induced onto the cloning device (Exhibits E-1, E-5, E-9, E-11, E-14, E-31). An access point that clones another's BSSID is characteristically used to capture that network's associations; whether communications were in fact

intercepted is what direction-finding and device examination can establish.

2. 18 U.S.C. § 1030 (unauthorized access to protected computers). The open, unauthenticated 'Ring Setup' AP on Texas Instruments silicon (Exhibit E-16) and the open [ESS] profile on 06:aa:a0:cd:e6:b0 (Exhibit E-4) are open join surfaces positioned to reach my networked devices, consistent with the credential compromise already pleaded at Dkt. 37.

3. Use of cell-site simulators by a non-carrier party. The T-Mobile CellSpot femtocell (ASUS silicon, OUI 38:2c:4a; Exhibits E-15, E-18) and the Nokia small-cell nodes (Nokia silicon, f8:9b:6e and ac:8f:a9; Exhibit E-24) are licensed-band devices that pull nearby handsets onto themselves. Operated by someone other than the carrier, such devices can function as IMSI-catchers — a device class the Bureau and DOJ treat as significant.

4. 18 U.S.C. §§ 1512, 1513 (obstruction / retaliation). The timing — surveillance that persists and re-clones during active federal litigation in which this infrastructure is pleaded — supports a nexus to the proceedings that warrants investigation.

WHAT I AM ASKING THE BUREAU TO DO

1. Open, or associate with any existing matter, an investigation into the offenses above, and treat this as a referral to the Chicago Cyber Task Force.
2. Because the emitters are live, conduct or direct **radio direction-finding** to physically locate the cloned AP and the femtocell/small-cell devices operating at or against **8516 W. Winona St., Chicago, IL 60656**.
3. Issue **preservation letters** to the manufacturers and carrier identified in the enclosed Device Identification table (ASUS, Nokia, Texas Instruments; T-Mobile), whose provisioning and attachment records can identify who is operating the equipment.
4. Coordinate, as appropriate, with the U.S. Attorney (N.D. Ill.), to whom the undersigned submitted a related criminal referral on June 30, 2026, and with the pending civil docket.
5. Open a case and provide a complaint / reference number and a **written point of contact** (email or U.S. mail), so I may submit supplemental captures as the conduct continues. Given the litigation posture, I ask that any contact be made **in writing** (email or U.S. mail).

PRESERVATION AND AVAILABILITY OF THE ORIGINALS

This letter is written notice of relevance. I have preserved the native image files, their EXIF metadata, the SHA-256 hash manifest, and the analyzer session data, and I will make my device and the originals available for forensic imaging on request. I ask that the Bureau likewise preserve all records it generates in connection with this report.

Verification. I declare under penalty of perjury under the laws of the United States (28 U.S.C. § 1746) that the factual statements above are true and correct to the best of my knowledge, that the enclosed exhibits are true and correct copies of the screenshots as captured, and that I personally captured them on the dates and times shown.

How to reach me — in writing. Because of the active litigation posture of the related federal and state cases, I request that **all communication with me be made in writing** — by email at

defcon5ready@gmail.com or by U.S. mail at **8516 W. Winona St., Chicago, IL 60656**. I respectfully ask that you **open a case or complaint and send me the case or reference number in writing**, and direct any acknowledgment, questions, request for the native image files, or point of contact to me by email or U.S. mail. I will respond promptly to any written contact.

Respectfully,

/s/ Ehab Allababidi

Ehab Allababidi (DOB 09/24/1996)

Principal Investigator, Dark Deck LLC (CAGE 16QC7)

8516 W. Winona St., Chicago, IL 60656

(773) 920-0030 | defcon5ready@gmail.com

Dated: July 15, 2026

EXHIBIT PACKET

Continuing Electronic Surveillance of a Federal Litigant

39 WiFi-analyzer captures, July 11–13, 2026 — 8516 W. Winona St., Chicago

PURPOSE

This packet supplies the primary evidence for the accompanying notices and complaints: 39 timestamped Wi-Fi spectrum captures documenting that the rogue 'Evil Twin' access-point and cellular-femtocell indicators already pleaded in Case No. 1:25-cv-15800 (Dkt. 32, 37, 51, 61) remained present and active at the residence throughout July 11–13, 2026.

THE CORE FINDING

A hidden access point at MAC 1a:60:41:7a:87:2x is a locally-administered bit-flip clone of the legitimate router 18:60:41:2a:87:2x. It is reported at ~0 metres, tracks the router across the 2.4 GHz and 5 GHz bands and across a WPA3/Wi-Fi 7 upgrade, and is accompanied by a second cloned radio (3e:f0...) and by carrier 'CellSpot' femtocell and IoT camera nodes.

SCOPE — WHAT IS ESTABLISHED, AND WHAT REQUIRES INVESTIGATION

Established as fact by these captures: the cloned BSSIDs and the IEEE locally-administered address bit; the on-screen signal, distance, channel and timestamp readings; and the true silicon manufacturer of each radio, resolved from the IEEE OUI registry — which a spoofed SSID name cannot alter. These hardware identifications are not hedged. What remains for investigators — by radio direction-finding and device seizure — is who operates the equipment and whether the contents of specific communications were captured.

AUTHENTICATION

Every capture carries the device clock in the status bar and an embedded EXIF DateTimeOriginal timestamp. Distance and dBm figures are the analyzer's own computed values. The images are true and correct copies of the screenshots as captured, as attested in the signed Declaration of Authenticity on the following page.

SUBMITTED BY

Ehab Allababidi, pro se — 8516 W. Winona St., Chicago, IL 60656 — (773) 920-0030 | defcon5ready@gmail.com.
Reachable by email or U.S. mail at the foregoing.

DECLARATION OF AUTHENTICITY AND CHAIN OF CUSTODY

Executed under penalty of perjury pursuant to 28 U.S.C. § 1746 and 735 ILCS 5/1-109

I, Ehab Allababidi (DOB 09/24/1996), residing at 8516 W. Winona St., Chicago, IL 60656, declare as follows:

1. I am the plaintiff/petitioner, pro se, in the federal proceedings referenced in the accompanying documents, and I have personal knowledge of the facts stated here.
2. Between July 11 and July 13, 2026, I personally captured the thirty-nine (39) screenshots attached as Exhibits E-1 through E-39, using a commercially available Wi-Fi spectrum-analyzer application running on my personal Android device, inside and immediately around my residence at the address above.
3. Each screenshot was generated by the device at the date and time recorded both in the on-screen status bar and in the image file's embedded EXIF DateTimeOriginal field. The distance (metres) and signal-strength (dBm) values shown are the application's own computed readings; I did not alter them.
4. The images attached are true and correct copies of those screenshots. I did not edit, retouch, crop, or otherwise modify the pixel content of any image.
5. To fix the integrity of each file, I computed a SHA-256 cryptographic hash of every native image. The hash values are listed in the Hash Manifest appended to this packet. Any later alteration of a file, however small, would change its hash and be detectable by re-computation.
6. I have preserved, and will produce on lawful request, the native image files with intact EXIF metadata and the analyzer session data underlying these exhibits.

I declare under penalty of perjury under the laws of the United States and the State of Illinois that the foregoing is true and correct.

Executed on July 15, 2026, at Chicago, Illinois.

/s/ Ehab Allababidi

Signature of Declarant (conformed above; signed in wet ink on the mailed hard copy)

Ehab Allababidi (DOB 09/24/1996), Declarant, pro se

8516 W. Winona St., Chicago, IL 60656 | (773) 920-0030 | defcon5ready@gmail.com

The declarant may be reached by email at defcon5ready@gmail.com or by U.S. mail at the address above.

MASTER INDEX OF EXHIBITS

Ex.	Captured	Band	What it shows
E-1	Jul 11, 2026 01:48	2.4 GHz	The hidden Evil Twin sitting on top of the legitimate router. The hidden network at MAC 1a:60:41:7a:87:20 (~41 dBm, 0 m, Ch.
E-2	Jul 11, 2026 01:48	2.4 GHz	Enterprise-authentication SSID and legacy-crypto nodes in a residential band. A hidden SSID at 76:63:9c:f4:93:cd advertises WPA2-EAP/SHA1 — enterprise (RADIUS) authentication that has no ordinary place on a residential street — alongside a WPA2+TKIP legacy node (42:0f:c1:8d:0b:d6).
E-3	Jul 11, 2026 01:48	2.4 GHz	Three locally-administered clones of a single radio. The radio ending 63:9c:f4:93:cd appears simultaneously as 76:..., 6e:..., and 7a:... — three locally-administered (spoofed) variants of the same hardware.
E-4	Jul 11, 2026 01:48	2.4 GHz	The same radio broadcasting both secured and open (ESS) profiles. MAC 06:aa:a0:cd:e6:b0 is seen as both a locked WPA2 network and an open [ESS] network.
E-5	Jul 11, 2026 01:49	2.4 GHz	The twin tracks the legitimate router's signal. Sorted by strength: Winona5 (-28), its 3c:f0 sibling (-41), and the hidden clone 1a:60:41:7a:87:20 (-42) cluster together at the top with near-identical signal — the clone physically co-located with the router it imitates.
E-6	Jul 11, 2026 01:49	n/a	The measurement tool used to capture this evidence. The analyzer's tool page, including 'Signal Tracker — Locate WiFi devices using its signal strength.
E-7	Jul 11, 2026 01:49	2.4 GHz	The second-radio Evil Twin (3e:f0 clone of 3c:f0). A hidden SSID at 3e:f0:83:17:d2:1c (-71, Ch.
E-8	Jul 11, 2026 01:49	2.4 GHz	Channel graph — the legitimate router dominating Ch. 2 at ~0 m. The channel-overlap view shows Winona5 (~0 m) as an anomalously tall, wide envelope on Ch.
E-9	Jul 11, 2026 01:49	2.4 GHz	Channel graph — legitimate router and hidden twin overlaid at ~0 m. Winona5 (~0 m) and a HiddenSSID (~0 m) share the same Ch.
E-10	Jul 11, 2026 09:48	2.4 GHz	IoT interception surface: Seongji 'fridge' and USI 'Ring' camera nodes. Alongside the clone (1a:60:..., -37) and the router (-39): [fridge]_E30AJT5133517J on 88:57:1d:8b:c4:51 — silicon by Seongji Industry Co.
E-11	Jul 11, 2026 09:49	5 GHz	The Evil Twin pairing repeats on 5 GHz (Ch. 153). On 5 GHz the hidden 1a:60:41:7a:87:21 (-50) sits with the legitimate Winona5 18:60:41:2a:87:21 (-57) on Ch.
E-12	Jul 11, 2026 13:47	5 GHz	Channel graph — connected router versus a distant sibling. The connected AP (Winona5*, ~0 m) forms a dominant peak in the upper 5 GHz band while a weaker Winona5 (~46 m) and a HiddenSSID trail beneath — separating the in-home emitter from farther radios.
E-13	Jul 11, 2026 13:47	5 GHz	The device's own connection: 192.168.12.180 at 960 Mbps. The phone is associated to Winona5 (18:60:41:2a:87:21) at -30 dBm, 960 Mbps, IP 192.
E-14	Jul 11, 2026 13:47	5 GHz	Hidden twin at 0 m while connected to the real router. While connected to Winona5 (-30), the hidden 1a:60:41:7a:87:21 is reported at 0 m, -63 dBm on the same Ch.
E-15	Jul 11, 2026 13:47	2.4 GHz	Confirmed cellular femtocell (T-Mobile CellSpot / ASUS) in range. With the clone at -29 (0 m) and router at -33, the scan adds CellSpot_2.
E-16	Jul 11, 2026 13:47	2.4 GHz	TEXAS INSTRUMENTS radio broadcasting an open 'Ring Setup' pairing AP. 'Ring Setup 8d' is an OPEN [ESS] access point on 24:7d:4d:6a:01:8e — Texas Instruments silicon (a TI SimpleLink RF transceiver whose operating band and transmit power are set in firmware, not fixed like a normal doorbell).
E-17	Jul 11, 2026 13:48	2.4 GHz	Channel graph — dense co-channel crowding around the residence. The 2.
E-18	Jul 11, 2026 22:55	2.4 GHz	One ASUS femtocell radio broadcasting three CellSpot SSIDs. CellSpot_2.
E-19	Jul 11, 2026 22:55	2.4 GHz	Paired locally-administered variants (yoyo / 10:5a clone). yoyo (0a:5a:95:9a:ad:f4) and a HiddenSSID (10:5a:95:9a:ad:f2) are LAA variants of one radio; the scan also carries ATT4k3T6T2 and Bailey17 — mapping the surrounding node population for comparison.
E-20	Jul 11, 2026 22:55	2.4 GHz	TP-Link range extender and a hidden/visible Deco pair. Aldaw-WiFi_EXT_upstairs (TP-Link extender) and Pancevo (42:0f:c1:8d:0b:d0) — the visible counterpart of the hidden 42:0f:...:d6 seen earlier — show extender hardware pushing coverage toward the residence.
E-21	Jul 12, 2026 00:17	2.4 GHz	Channel graph — full neighbourhood spectral map. A wide 2.
E-22	Jul 12, 2026 00:17	2.4 GHz	Channel graph — hidden and named nodes overlaid. The same dense view emphasising how many hidden SSIDs sit interleaved with named networks across Ch.
E-23	Jul 12, 2026 00:17	2.4 GHz	Hidden/visible mesh pair: 52:a6 clone and 8522JosephHomeWifi_Deco. The hidden 52:a6:e6:93:c4:2e and the visible 8522JosephHomeWifi_Deco (...:2f) are one TP-Link Deco mesh radio presenting a hidden twin — the same hidden/visible cloning pattern as the Evil Twin, on third-party hardware.

Ex.	Captured	Band	What it shows
E-24	Jul 12, 2026 00:17	2.4 GHz	Nokia/Arcadyan carrier nodes: TMO-Recall64 and AT&T; surfaces. TMO-Recall64 on 18:a5:ff:22:65:50 — Arcadyan, the same carrier-gateway ODM as the router — with at&t9378; / at&t9378-Guest; (Netgear) and a [fridge] node.
E-25	Jul 12, 2026 00:17	2.4 GHz	One SSID at wildly inconsistent distances (synergy 313 m vs 15 m). 'synergy' is computed at 313 m on one BSSID and 15 m on another within the same scan, and 'synergy-guest' clusters at 8 m — signal readings inconsistent with static neighbour APs and consistent with mobile or power-varying emitters.
E-26	Jul 12, 2026 12:45	5 GHz	Security-generation mismatch: WPA3/Wi-Fi 7 router vs WPA2 clones. The legitimate Winona5 is WPA3 / Wi-Fi 7 (600 Mbps, Ch.
E-27	Jul 13, 2026 16:36	5 GHz	Wi-Fi generation table isolating the genuine router. Winona5 (Wi-Fi 7, -45, Ch.
E-28	Jul 13, 2026 16:36	5 GHz	Isolated twin pair, only two radios in range. With interference filtered, only Winona5 Wi-Fi 7 (Ch.
E-29	Jul 13, 2026 16:36	5 GHz	Physically anomalous signal strength: -20 dBm. Winona5 is reported at -20 dBm — an extraordinarily strong reading.
E-30	Jul 13, 2026 16:36	2.4 GHz	Router on Ch. 3 at -25 with the hidden 76:63:9c present. Winona5 (Wi-Fi 7, WPA3, Ch.
E-31	Jul 13, 2026 16:37	5 GHz	The clone now mirrors WPA3 / Wi-Fi 7 on Ch. 40 at 0 m. Critically, the hidden 1a:60:41:7a:87:21 now advertises Wi-Fi 7 / WPA3 at 0 m, -46, on Ch.
E-32	Jul 13, 2026 16:37	5 GHz	Genuine router and matched clone side by side. Winona5 Wi-Fi 7 (-37) and the hidden Wi-Fi 7 clone (-46) shown together on Ch.
E-33	Jul 13, 2026 16:38	2.4 GHz	Extender and femtocell nodes persist on 2.4 GHz. Aldaw extender, CellSpot_2.
E-34	Jul 13, 2026 16:38	5 GHz	Channel graph — hidden twin overlaid on connected router (Ch. 40-44). The connected Winona5* (~0 m) and a HiddenSSID (~0 m) occupy the same Ch.
E-35	Jul 13, 2026 16:45	5 GHz	Channel graph — twin overlay confirmed minutes later. The same overlaid HiddenSSID (~0 m) and Winona5* (~1 m) on Ch.
E-36	Jul 13, 2026 16:50	5 GHz	Channel graph — tightest twin overlay. HiddenSSID (~0 m) and Winona5* (~0 m) drawn as nearly coincident envelopes on Ch.
E-37	Jul 13, 2026 16:50	5 GHz	Channel graph — isolated genuine-router envelope (baseline). A single Winona5* peak on Ch.
E-38	Jul 13, 2026 17:59	2.4 GHz	Channel graph — 2.4 GHz twin overlay amid dense neighbours. On 2.
E-39	Jul 13, 2026 17:59	5 GHz	Channel graph — final capture, twin still overlaid on Ch. 40. The last capture (Jul 13, 17:59) shows Winona5* (~0 m) and a HiddenSSID (~0 m) still overlaid on Ch.

DEVICE IDENTIFICATION — WHAT THE HARDWARE ACTUALLY IS

Manufacturer resolved from the IEEE OUI registry; the advertised SSID name is not evidence of what the silicon is.

SSID (as broadcast)	BSSID / OUI	Real manufacturer (IEEE)	What the silicon is	Forensic note
Winona5	18:60:41:2a:87:2x	No IEEE registration	The home router's primary BSSID prefix is not in the IEEE OUI registry.	An unregistered OUI on the 'legitimate' router is itself an anomaly; the Arcadyan silicon only shows on its sibling radio (below).
Winona5 (sibling)	3c:f0:83:e7:d2:1x	Arcadyan Corporation	ODM that builds ISP/carrier home gateways (AT&T;, T-Mobile, etc.).	The genuine router radio; the anchor the clones imitate.
(HiddenSSID) EVIL TWIN	1a:60:41:7a:87:2x	Locally-administered — unregistered	A spoofed BSSID: 18-1a bit-flip of the router's own prefix.	The 6 GHz twin 1a:60:41:7a:87:22 was pleaded at Dkt. 32/51/61; the :20 (2.4 GHz) and :21 (5 GHz) band-siblings here are NEW and show the clone now spans every band.
(HiddenSSID) 2nd twin	3e:f0:83:x7:d2:1x	Locally-administered — unregistered	A spoofed BSSID: 3c-3e bit-flip of the Arcadyan radio.	The 'second 5 GHz Evil Twin' pleaded at Dkt. 51 (3c:f0:83:e7:d2:1d), now seen on both 2.4 GHz (...17:d2:1c) and 5 GHz (...97:d2:1c).
CellSpot_2.4GHz_Net 1 / Net2 / 7868	38:2c:4a:97:78:68/6a	ASUSTek Computer	T-Mobile 4G LTE CellSpot — an ASUS-built femtocell (a home 'mini cell tower' that carries licensed cellular traffic over broadband).	One unit broadcasting three SSIDs. A femtocell forces nearby phones to attach to it; this is the cellular device class capable of intercepting attachments, pleaded as IMSI-catchers at Dkt. 37/51.
ATT4k3T6T2 / ATTFnPQ8S	f8:9b:6e / ac:8f:a9	Nokia Solutions and Networks	Carrier small-cell / base-station infrastructure silicon — not consumer Wi-Fi.	Carrier-grade Nokia radios in a residential band directly corroborate the 'Nokia Femtocell / IMSI-catcher' devices pleaded at Dkt. 37 and Dkt. 51.
TMO-Recall64	18:a5:ff:22:65:50	Arcadyan Corporation	T-Mobile-branded gateway ODM (same vendor as the router radio).	SSID name 'Recall64' on carrier ODM silicon positioned near the residence.
Ring Setup 8d	24:7d:4d:6a:01:8e	Texas Instruments	A TI SimpleLink RF transceiver. 'Ring Setup XX' is the OPEN access point a Ring device emits only while being provisioned; the band/power of a SimpleLink part is firmware-set.	A genuine Ring should broadcast 'Ring Setup' for minutes during first pairing, then join the home network as a client and stop. A persistent open 'Ring Setup' AP is a device stuck in, or repeatedly re-entering, pairing mode — an open join/MITM surface at 0 m.
Ring-614685	3c:e1:a1:61:46:85	Universal Global Scientific (USI)	A wireless-module ODM used in some Amazon/Ring hardware.	A camera radio operating as a persistent, named access point near the home rather than as an ordinary Wi-Fi client.
[fridge]_E30AJT51335 17J	88:57:1d:8b:c4:51	Seongji Industry Company	A contract-electronics manufacturer; the SSID asserts a refrigerator.	An appliance-labelled node whose silicon vendor does not match a major appliance brand, broadcasting within metres of the residence.
Kokkinias / ATT7Rf2dDv	cc:ab:2c:*	Humax	Set-top-box / gateway ODM.	Included for completeness of the local transmitter census.
synergy / synergy-guest	30:fd:38 & 70:3a:cb (Google); 32:fd:38 & 72:3a:cb (LAA)	Google (genuine) + locally-administered clones	Google/Nest radios shadowed by spoofed 'guest' BSSIDs (bit-flips of the Google prefixes).	The same clone-a-real-network pattern as the Evil Twin, on third-party hardware.
Rotating hidden clones	76/6e/7a:63:9c; 52:a6:e6; 42:0f:c1; 06:aa:a0; 10:5a:95	All locally-administered — unregistered	Multiple spoofed BSSIDs, several from single physical radios presenting rotating identities.	Rotating locally-administered BSSIDs are more consistent with coordinated spoofing than with ordinary consumer behaviour.

The hidden Evil Twin sitting on top of the legitimate router



WHAT THIS SCREENSHOT SHOWS

The hidden network at MAC 1a:60:41:7a:87:20 (-41 dBm, 0 m, Ch. 2) is listed directly above the legitimate home router Winona5 at 18:60:41:2a:87:20 (-40 dBm, 0 m, Ch. 2). The two BSSIDs differ only by a locally-administered-address bit flip (18-1a in the first octet; 2a-7a in the fourth) — the textbook signature of a cloned/rogue access point. This is the same Evil Twin pairing pleaded in Dkt. 51 §III and Dkt. 61, still broadcasting at roughly zero meters from the residence.

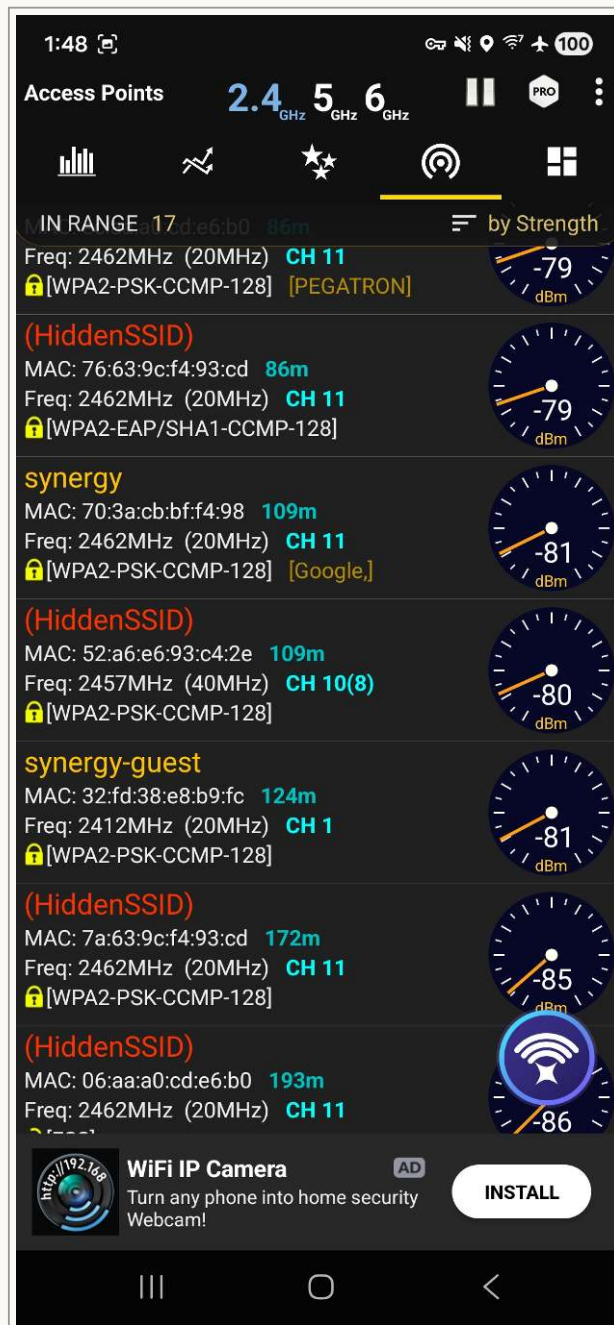
Enterprise-authentication SSID and legacy-crypto nodes in a residential band



WHAT THIS SCREENSHOT SHOWS

A hidden SSID at 76:63:9c:f4:93:cd advertises WPA2-EAP/SHA1 — enterprise (RADIUS) authentication that has no ordinary place on a residential street — alongside a WPA2+TKIP legacy node (42:0f:c1:8d:0b:d6). Enterprise auth and downgraded crypto are consistent with a purpose-built interception deployment rather than neighbor Wi-Fi.

Three locally-administered clones of a single radio



WHAT THIS SCREENSHOT SHOWS

The radio ending 63:9c:f4:93:cd appears simultaneously as 76:..., 6e:..., and 7a:... — three locally-administered (spoofed) variants of the same hardware. A single physical device presenting multiple rotating locally-administered BSSIDs is a coordinated MAC-spoofing pattern, not ordinary consumer behaviour.

The same radio broadcasting both secured and open (ESS) profiles



WHAT THIS SCREENSHOT SHOWS

MAC 06:aa:a0:cd:e6:b0 is seen as both a locked WPA2 network and an open [ESS] network. A device that simultaneously offers an open join surface is consistent with a rogue AP inviting association / man-in-the-middle capture.

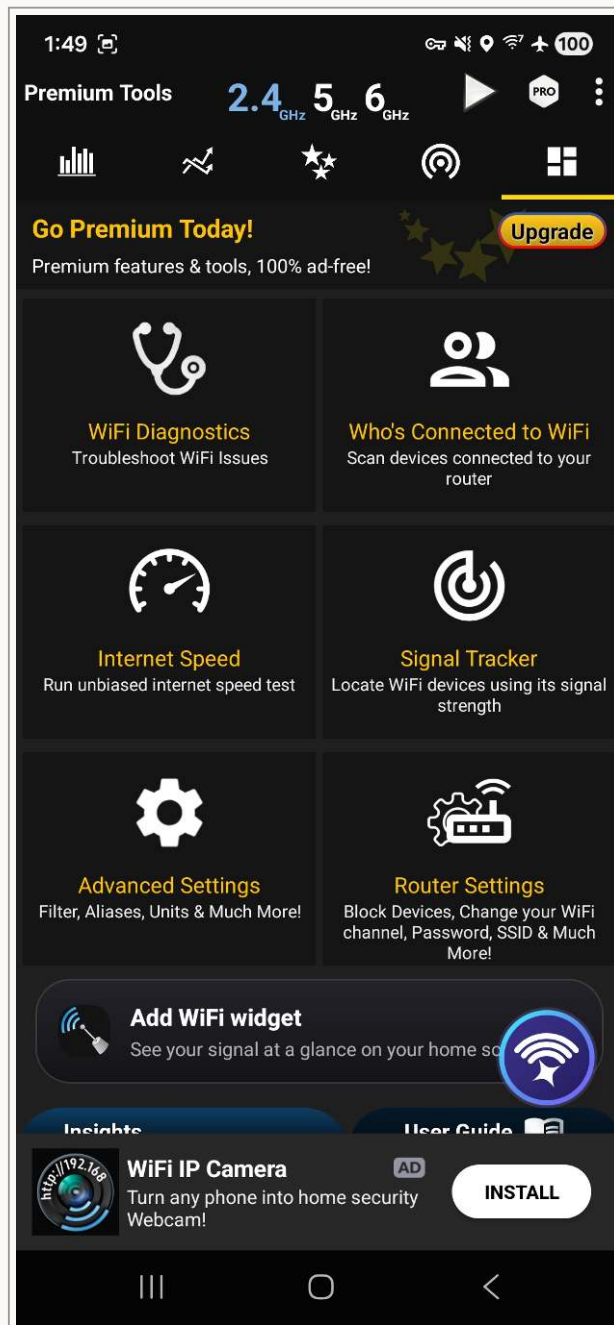
The twin tracks the legitimate router's signal



WHAT THIS SCREENSHOT SHOWS

Sorted by strength: Winona5 (-28), its 3c:f0 sibling (-41), and the hidden clone 1a:60:41:7a:87:20 (-42) cluster together at the top with near-identical signal — the clone physically co-located with the router it imitates.

The measurement tool used to capture this evidence



WHAT THIS SCREENSHOT SHOWS

The analyzer's tool page, including 'Signal Tracker — Locate WiFi devices using its signal strength.' Included to authenticate the instrument used for every capture in this packet and to show the distance/"metres" readings are the app's own computed values.

The second-radio Evil Twin (3e:f0 clone of 3c:f0)



WHAT THIS SCREENSHOT SHOWS

A hidden SSID at 3e:f0:83:17:d2:1c (-71, Ch. 1) appears beside the legitimate Winona5 3c:f0:83:e7:d2:1c — again a locally-administered bit-flip clone (3c-3e). This corroborates the 'second 5 GHz Evil Twin' pleaded in Dkt. 51 (3c:f0:83:e7:d2:1d).

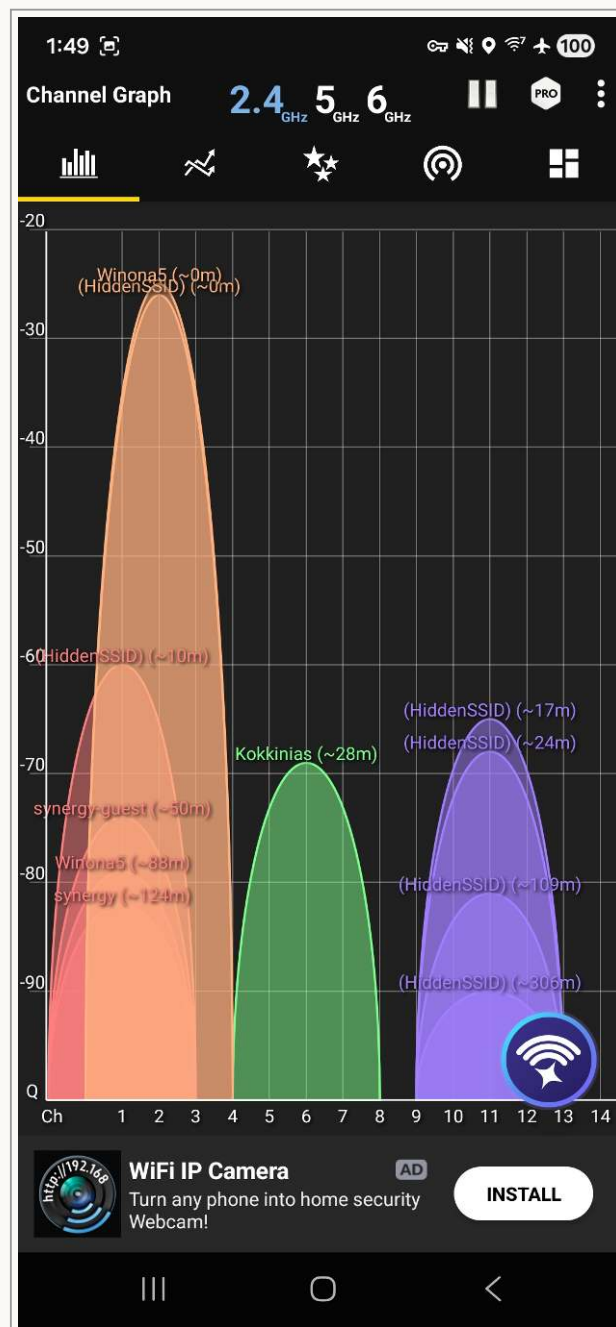
Channel graph — the legitimate router dominating Ch. 2 at ~0 m



WHAT THIS SCREENSHOT SHOWS

The channel-overlap view shows Winona5 (~0 m) as an anomalously tall, wide envelope on Ch. 1-3, with overlapping hidden/“synergy” lobes underneath — the spectral picture of a high-power emitter at the measurement point.

Channel graph — legitimate router and hidden twin overlaid at ~0 m



WHAT THIS SCREENSHOT SHOWS

Winona5 (~0 m) and a HiddenSSID (~0 m) share the same Ch. 2 peak, one drawn on top of the other — two 'zero-metre' emitters occupying the identical frequency envelope, i.e. the clone superimposed on the original.

IoT interception surface: Seongji 'fridge' and USI 'Ring' camera nodes



WHAT THIS SCREENSHOT SHOWS

Alongside the clone (1a:60..., -37) and the router (-39): [fridge]_E30AJT5133517J on 88:57:1d:8b:c4:51 — silicon by Seongji Industry Co., not a major appliance brand — and Ring-614685 on 3c:e1:a1:61:46:85 — Universal Global Scientific (USI), a camera-module ODM — operating as a persistent named access point. Networked cameras acting as APs at close range expand the monitoring surface described in the credential-compromise notice (Dkt. 37).

The Evil Twin pairing repeats on 5 GHz (Ch. 153)



WHAT THIS SCREENSHOT SHOWS

On 5 GHz the hidden 1a:60:41:7a:87:21 (-50) sits with the legitimate Winona5 18:60:41:2a:87:21 (-57) on Ch. 153, and a hidden 3e:f0:83:97:d2:1c mirrors the 3c:f0 radio. The clone follows the router across every band it uses.

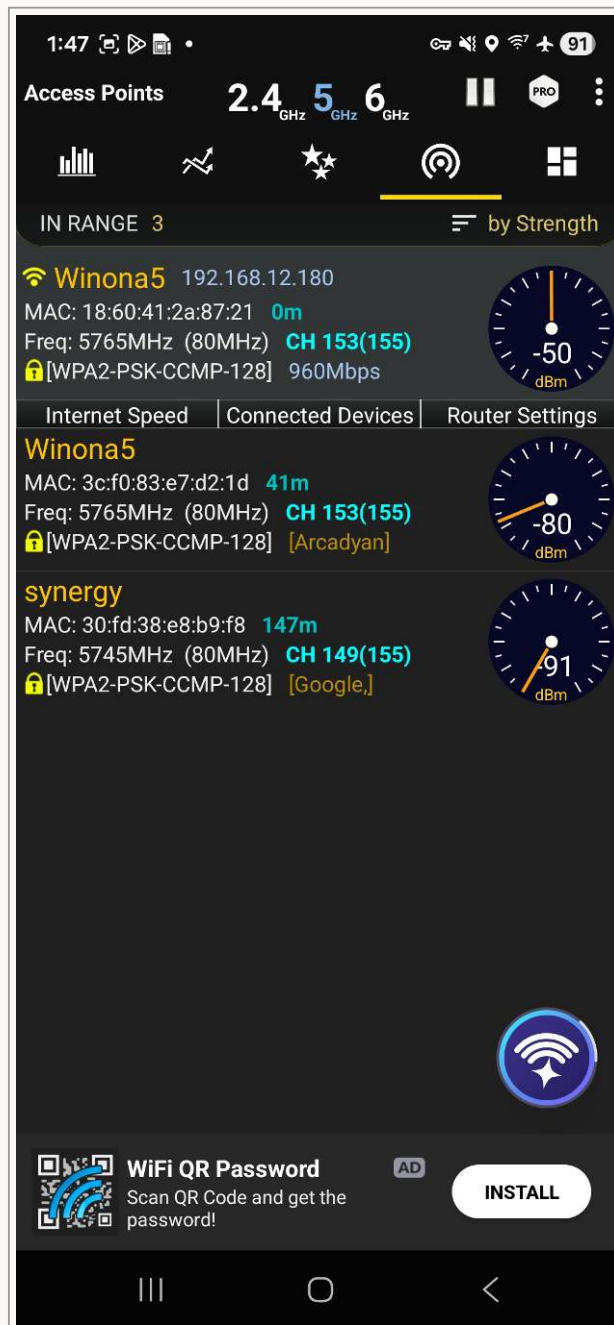
Channel graph — connected router versus a distant sibling



WHAT THIS SCREENSHOT SHOWS

The connected AP (Winona5*, ~0 m) forms a dominant peak in the upper 5 GHz band while a weaker Winona5 (~46 m) and a HiddenSSID trail beneath — separating the in-home emitter from farther radios.

The device's own connection: 192.168.12.180 at 960 Mbps



WHAT THIS SCREENSHOT SHOWS

The phone is associated to Winona5 (18:60:41:2a:87:21) at -30 dBm, 960 Mbps, IP 192.168.12.180 — establishing the legitimate router's identity and subnet as the reference point against which the clone is measured.

Hidden twin at 0 m while connected to the real router



WHAT THIS SCREENSHOT SHOWS

While connected to Winona5 (-30), the hidden 1a:60:41:7a:87:21 is reported at 0 m, -63 dBm on the same Ch. 153, with the 3e:f0 clone beneath — the rogue AP present at the measurement point in real time.

Confirmed cellular femtocell (T-Mobile CellSpot / ASUS) in range



WHAT THIS SCREENSHOT SHOWS

With the clone at -29 (0 m) and router at -33, the scan adds CellSpot_2.4GHz_Net1 on 38:2c:4a:97:78:69 — ASUSTek silicon. The T-Mobile 4G LTE CellSpot is an ASUS-built femtocell: a home 'mini cell tower' that carries licensed cellular traffic over broadband and forces nearby phones to attach to it. That is precisely the cellular-interception device class pleaded as an IMSI-catcher surface in Dkt. 37 and Dkt. 51.

TEXAS INSTRUMENTS radio broadcasting an open 'Ring Setup' pairing AP



WHAT THIS SCREENSHOT SHOWS

'Ring Setup 8d' is an OPEN [ESS] access point on 24:7d:4d:6a:01:8e — Texas Instruments silicon (a TI SimpleLink RF transceiver whose operating band and transmit power are set in firmware, not fixed like a normal doorbell). A genuine Ring emits a 'Ring Setup XX' SSID only for the few minutes of first-time provisioning, then joins the home network as a client and stops broadcasting. A persistent, open 'Ring Setup' AP is consistent with a device stuck in — or repeatedly forced back into — pairing mode: an open, unauthenticated join surface at close range, on a software-reconfigurable RF part, sitting beside a second [fridge] node. The TI SimpleLink part is firmware-reconfigurable, not a fixed-function doorbell radio; read with the -20 dBm reading (Exhibit E-29) and the FCC power-limit analysis at Dkt. 32, its actual transmit output and operating band warrant measurement by a field office.

Channel graph — dense co-channel crowding around the residence



WHAT THIS SCREENSHOT SHOWS

The 2.4 GHz envelope shows the router at ~0 m plus a stack of hidden/“synergy”/CellSpot lobes crowded onto Ch. 1-6, the congested spectral fingerprint of multiple co-located transmitters.

One ASUS femtocell radio broadcasting three CellSpot SSIDs



WHAT THIS SCREENSHOT SHOWS

CellSpot_2.4GHz_Net2 (...6a), CellSpot_2.4GHz_Net1 (...69) and CellSpot_2.4GHz_7868 (...68) all originate from the single ASUSTek radio 38:2c:4a:97:78 — one T-Mobile CellSpot femtocell presenting three networks at once. A single cellular small-cell fanning out multiple SSIDs maximizes the number of devices it can pull onto itself.

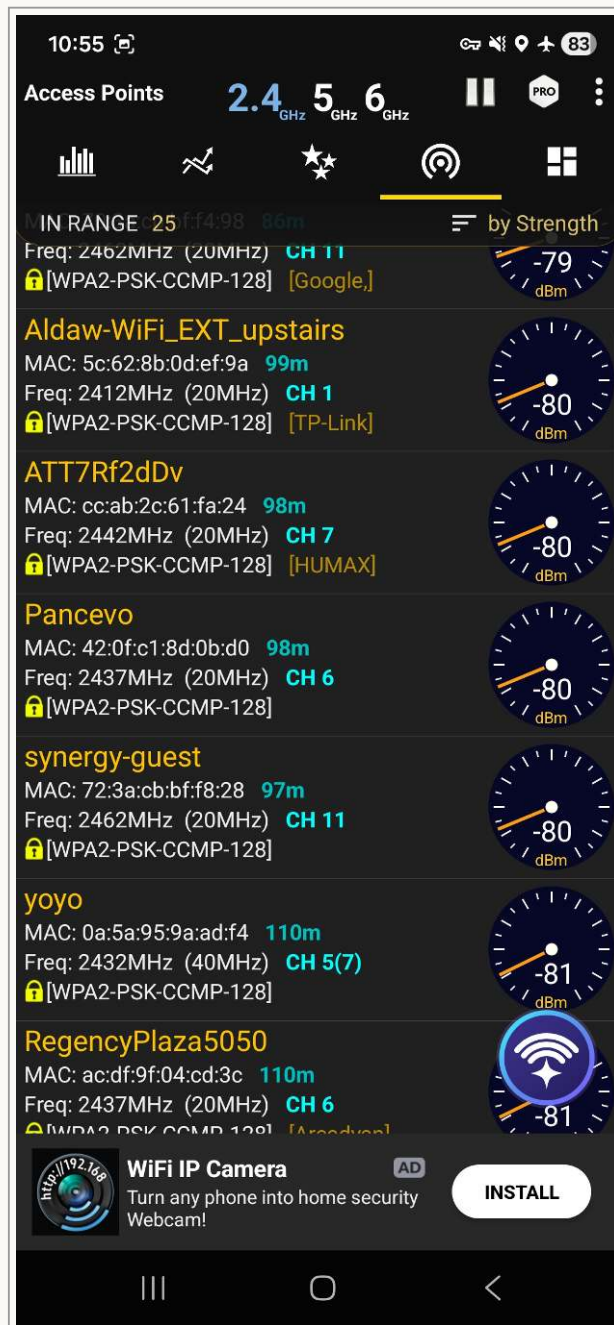
Paired locally-administered variants (yoyo / 10:5a clone)



WHAT THIS SCREENSHOT SHOWS

yoyo (0a:5a:95:9a:ad:f4) and a HiddenSSID (10:5a:95:9a:ad:f2) are LAA variants of one radio; the scan also carries ATT4k3T6T2 and Bailey17 — mapping the surrounding node population for comparison.

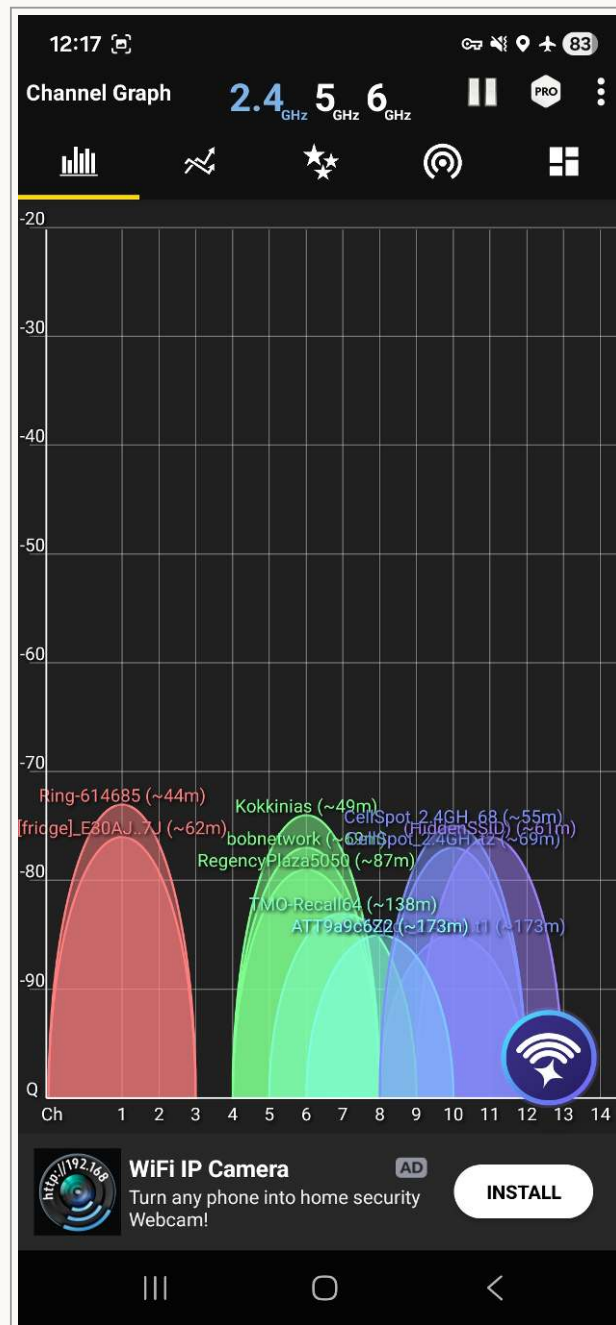
TP-Link range extender and a hidden/visible Deco pair



WHAT THIS SCREENSHOT SHOWS

Aldaw-WiFi_EXT_upstairs (TP-Link extender) and Pancevo (42:0f:c1:8d:0b:d0) — the visible counterpart of the hidden 42:0f:...:d6 seen earlier — show extender hardware pushing coverage toward the residence.

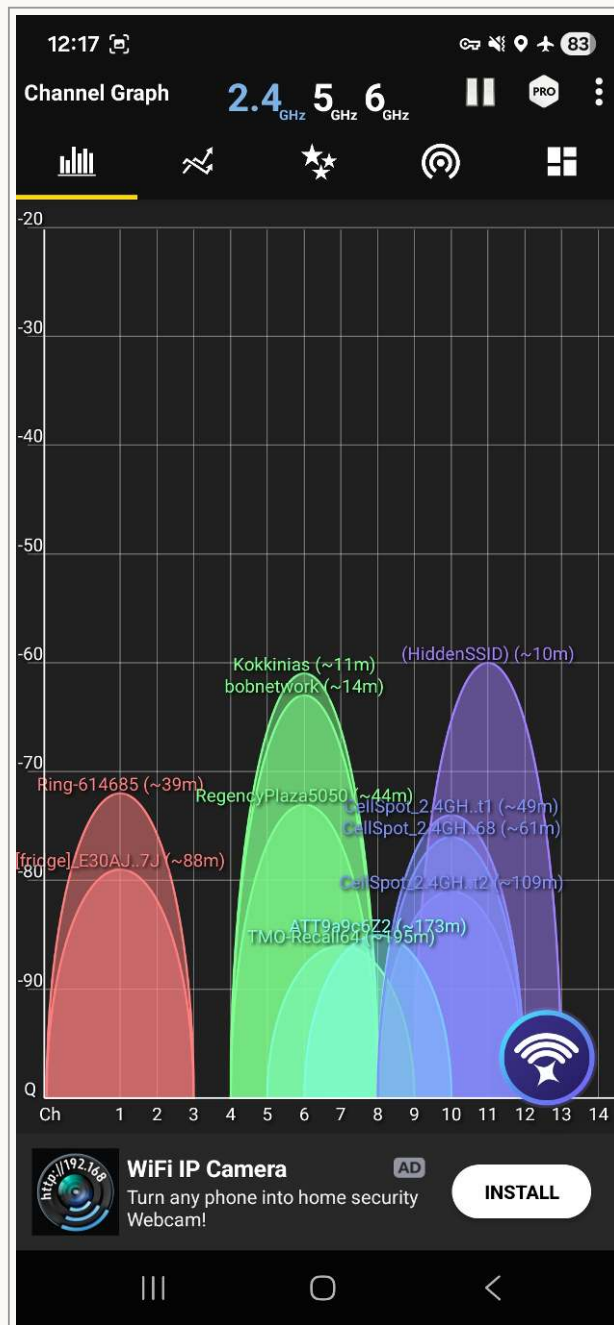
Channel graph — full neighbourhood spectral map



WHAT THIS SCREENSHOT SHOWS

A wide 2.4 GHz capture (Ring, [fridge], Kokkinias, CellSpot, TMO-Recall64, RegencyPlaza) documenting the complete transmitter population for context and to defeat any claim the clone is merely an ordinary neighbour.

Channel graph — hidden and named nodes overlaid



WHAT THIS SCREENSHOT SHOWS

The same dense view emphasising how many hidden SSIDs sit interleaved with named networks across Ch. 1-11 at close range.

Hidden/visible mesh pair: 52:a6:clone and 8522JosephHomeWifi_Deco



WHAT THIS SCREENSHOT SHOWS

The hidden 52:a6:e6:93:c4:2e and the visible 8522JosephHomeWifi_Deco (...:2f) are one TP-Link Deco mesh radio presenting a hidden twin — the same hidden/visible cloning pattern as the Evil Twin, on third-party hardware.

Nokia/Arcadyan carrier nodes: TMO-Recall64 and AT&T surfaces



WHAT THIS SCREENSHOT SHOWS

TMO-Recall64 on 18:a5:ff:22:65:50 — Arcadyan, the same carrier-gateway ODM as the router — with at&t9378 / at&t9378-Guest (Netgear) and a [fridge] node. Note that the AT&T-named small cells elsewhere in this packet (ATT4k3T6T2 f8:9b:6e; ATTFsnPQ8S ac:8f:a9) run on Nokia Solutions and Networks carrier silicon — the 'Nokia femtocell' class from Dkt. 37/51.

One SSID at wildly inconsistent distances (synergy 313 m vs 15 m)



WHAT THIS SCREENSHOT SHOWS

'synergy' is computed at 313 m on one BSSID and 15 m on another within the same scan, and 'synergy-guest' clusters at 8 m — signal readings inconsistent with static neighbour APs and consistent with mobile or power-varying emitters.

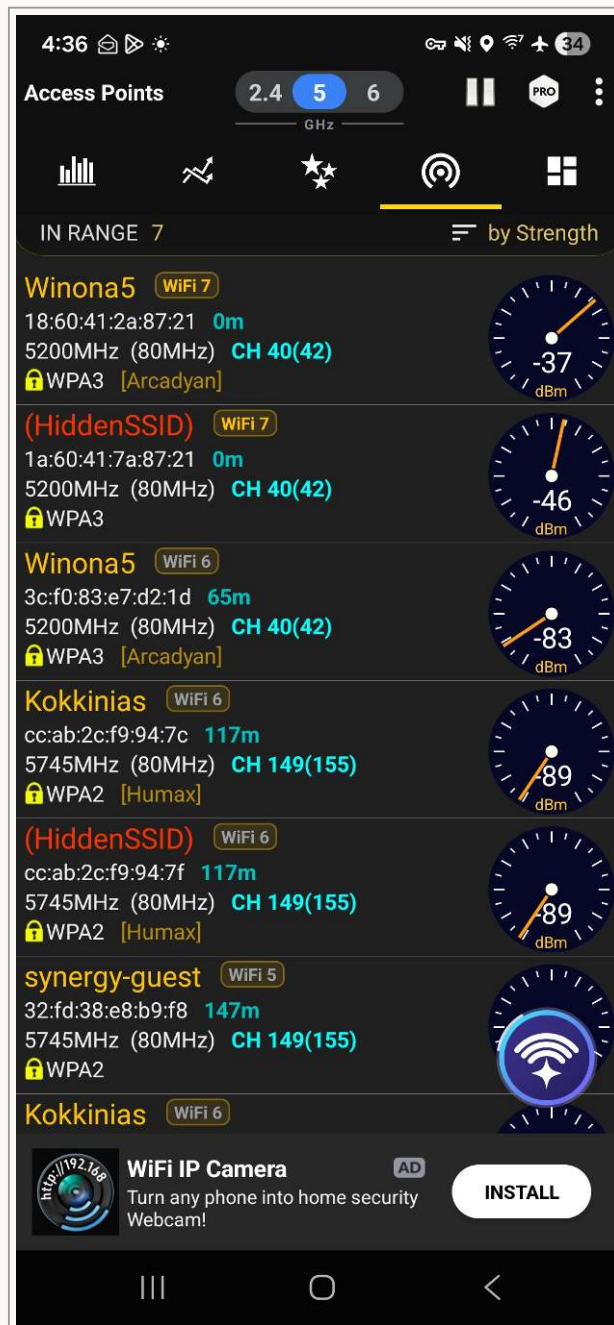
Security-generation mismatch: WPA3/Wi-Fi 7 router vs WPA2 clones



WHAT THIS SCREENSHOT SHOWS

The legitimate Winona5 is WPA3 / Wi-Fi 7 (600 Mbps, Ch. 40) while the co-located clones downgrade to WPA2 — a security-and-generation mismatch between the genuine router and the devices imitating it.

Wi-Fi generation table isolating the genuine router



WHAT THIS SCREENSHOT SHOWS

Winona5 (Wi-Fi 7, -45, Ch. 40) versus its Wi-Fi 6 sibling (-81) and WPA2 hidden nodes — a clean side-by-side of protocol generations distinguishing the real AP from imitators.

Isolated twin pair, only two radios in range



WHAT THIS SCREENSHOT SHOWS

With interference filtered, only Winona5 Wi-Fi 7 (Ch. 40, -23) and its Wi-Fi 6 sibling (-37) remain — the cleanest view of the paired radios.

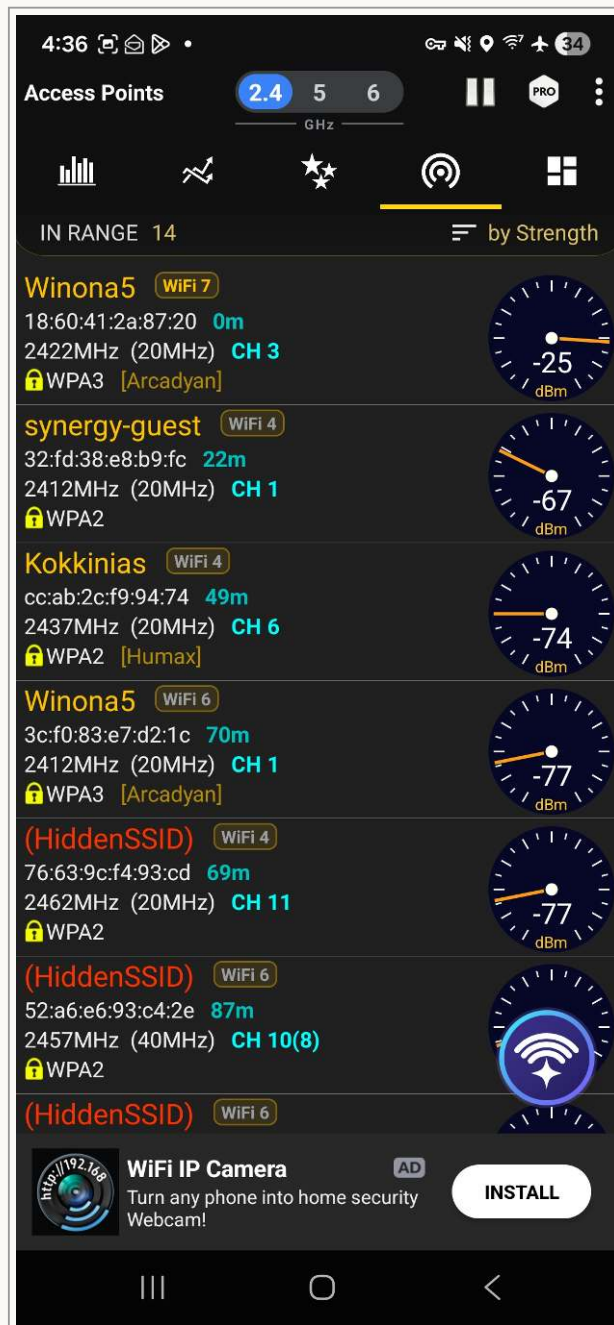
Physically anomalous signal strength: -20 dBm



WHAT THIS SCREENSHOT SHOWS

Winona5 is reported at -20 dBm — an extraordinarily strong reading. As argued in Dkt. 32, a -20 to -25 dBm signal at ~0 m implies an emitter essentially at the antenna, exceeding what ordinary consumer placement produces and consistent with an in-premise device.

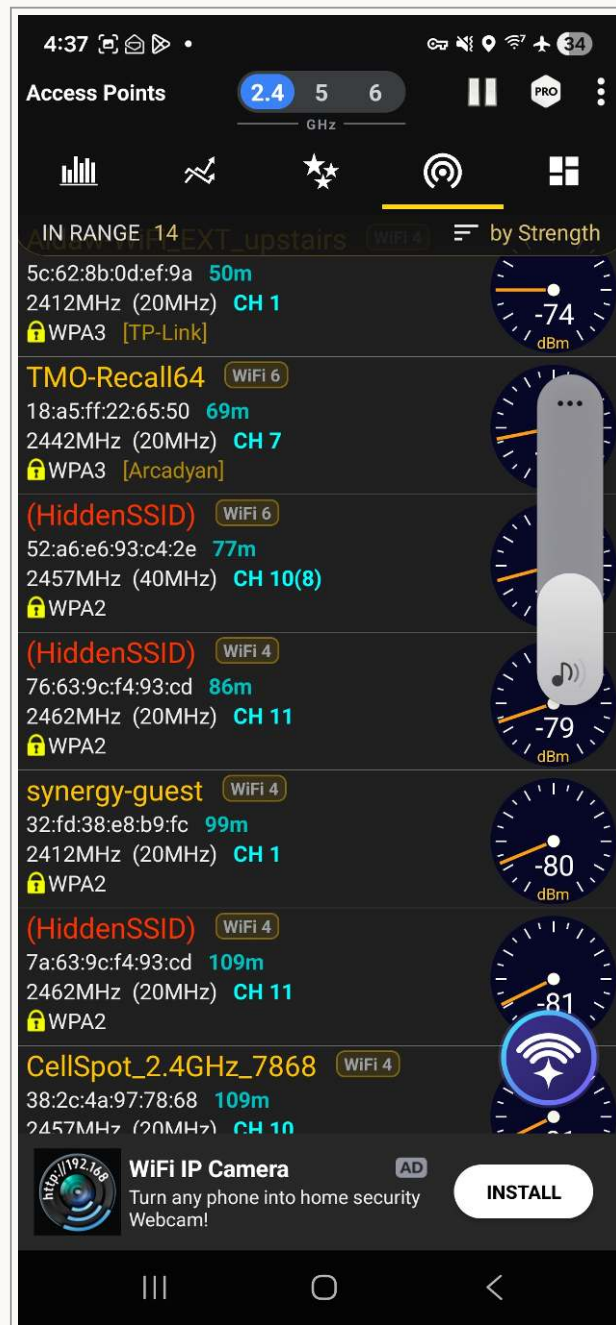
Router on Ch. 3 at -25 with the hidden 76:63:9c present



WHAT THIS SCREENSHOT SHOWS

Winona5 (Wi-Fi 7, WPA3, Ch. 3, -25) leads a 14-network scan that still includes the hidden 76:63:9c:f4:93:cd and 52:a6:e6 clones — the surveillance nodes persist two days into the capture window.

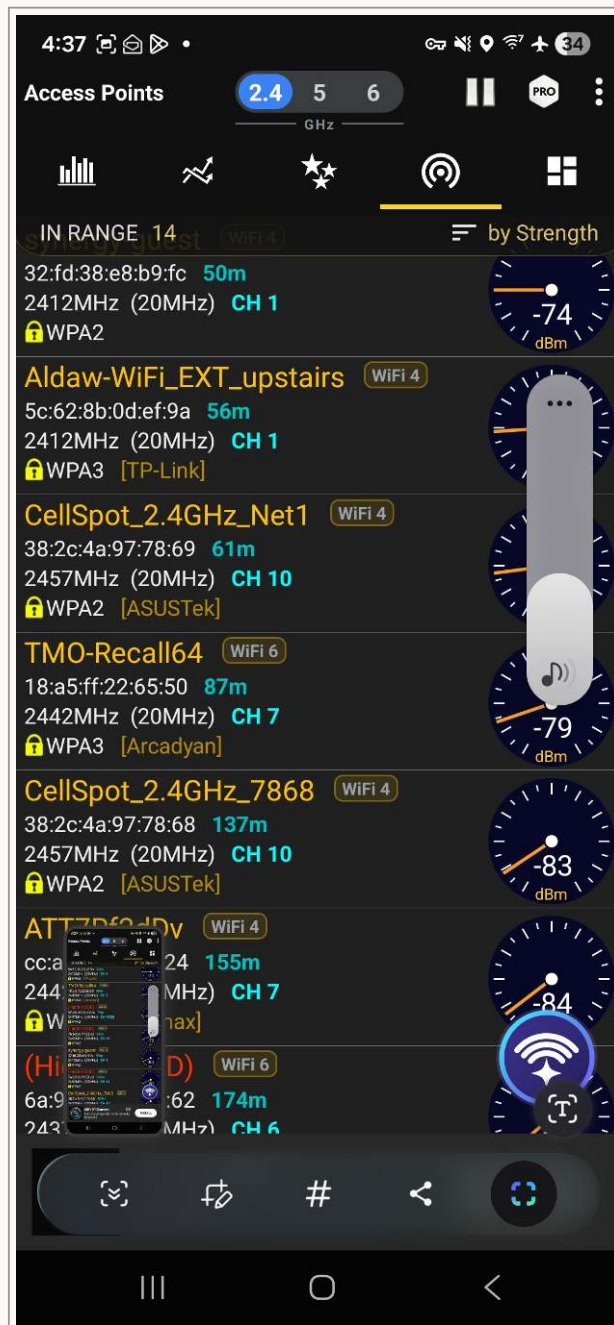
The clone now mirrors WPA3 / Wi-Fi 7 on Ch. 40 at 0 m



WHAT THIS SCREENSHOT SHOWS

Critically, the hidden 1a:60:41:7a:87:21 now advertises Wi-Fi 7 / WPA3 at 0 m, -46, on Ch. 40 — matching the genuine router's newest security profile. The clone tracks the router's upgrades, which random neighbour hardware would not do.

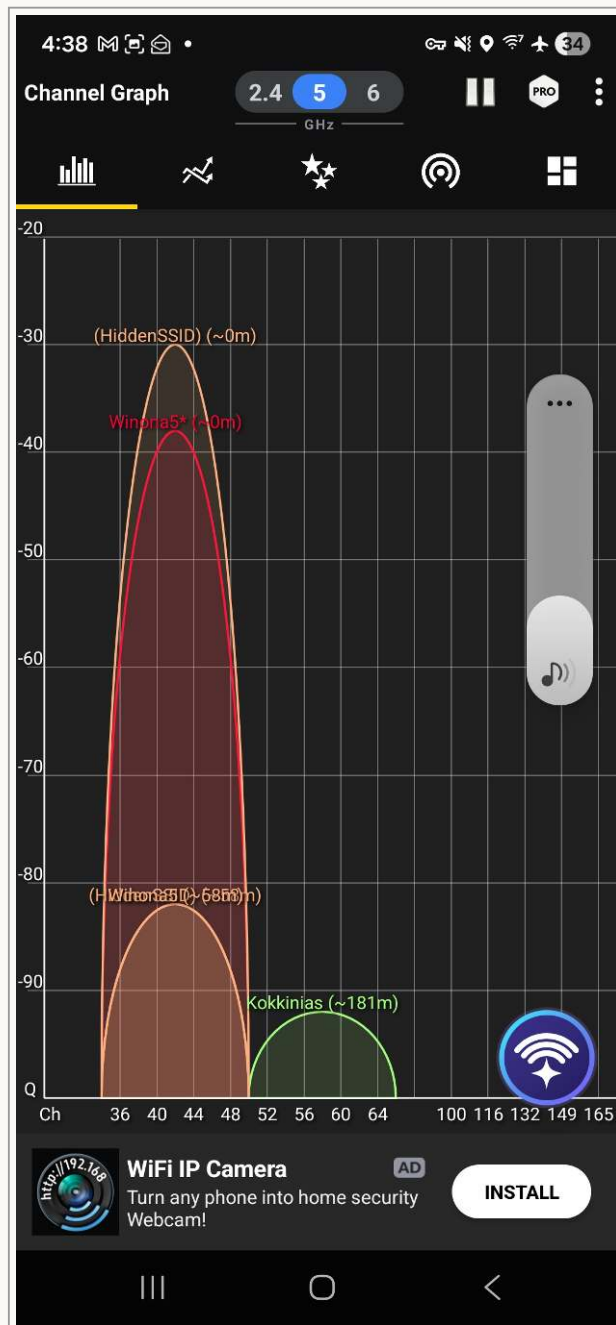
Genuine router and matched clone side by side



WHAT THIS SCREENSHOT SHOWS

Winona5 Wi-Fi 7 (-37) and the hidden Wi-Fi 7 clone (-46) shown together on Ch. 40 — the matched pair after the clone's profile change.

Extender and femtocell nodes persist on 2.4 GHz



WHAT THIS SCREENSHOT SHOWS

Aldaw extender, CellSpot_2.4GHz_Net1, CellSpot_2.4GHz_7868 and TMO-Recall64 remain in range — the auxiliary interception hardware is still deployed.

Channel graph — hidden twin overlaid on connected router (Ch. 40-44)



WHAT THIS SCREENSHOT SHOWS

The connected Winona5* (~0 m) and a HiddenSSID (~0 m) occupy the same Ch. 40-44 envelope, with synergy-guest far off on Ch. 149 — the clone superimposed on the router on 5 GHz.

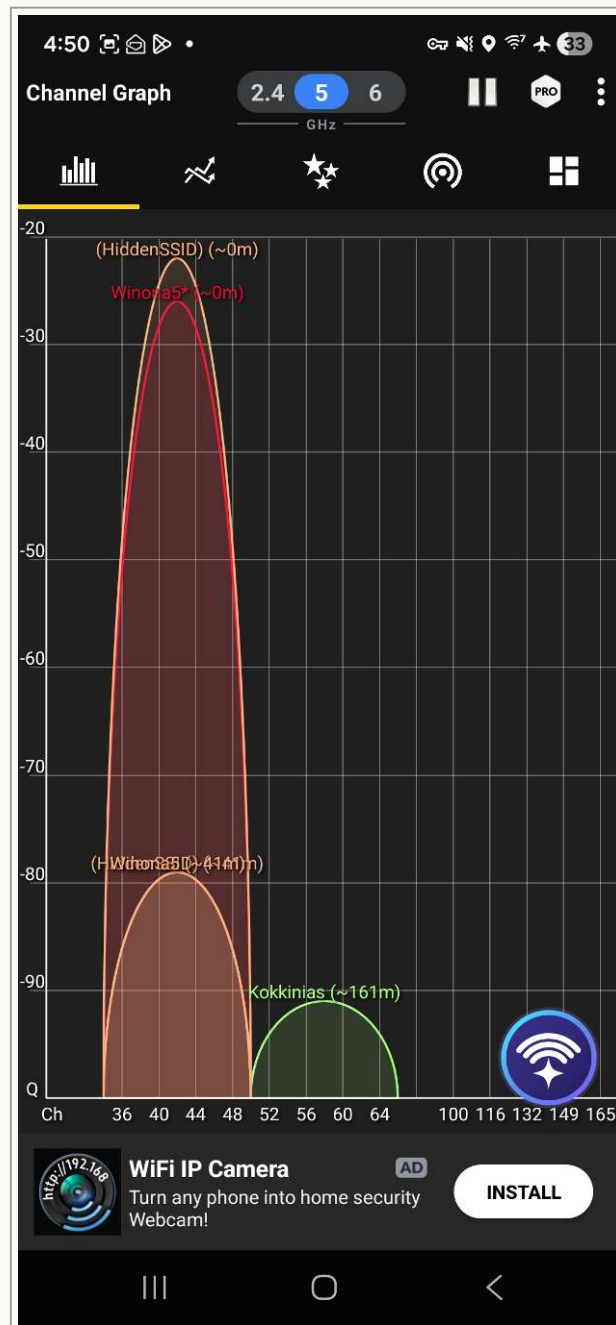
Channel graph — twin overlay confirmed minutes later



WHAT THIS SCREENSHOT SHOWS

The same overlaid HiddenSSID (~0 m) and Winona5* (~1 m) on Ch. 40, captured seven minutes after the prior graph — the pairing is stable, not a momentary artefact.

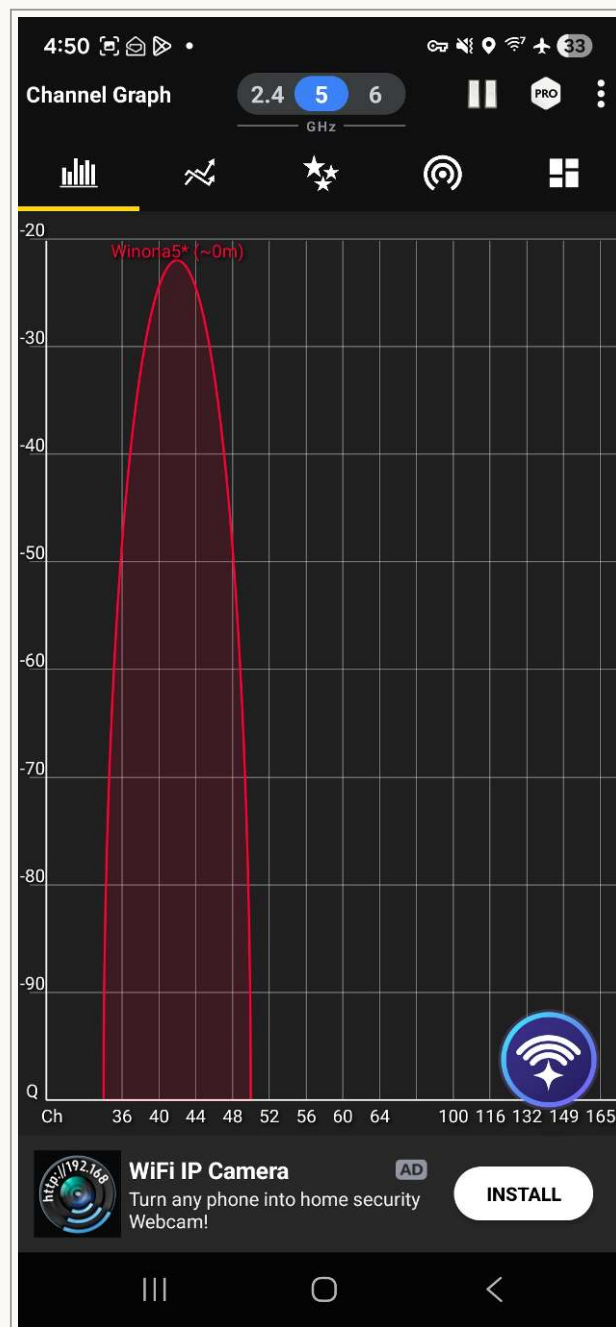
Channel graph — tightest twin overlay



WHAT THIS SCREENSHOT SHOWS

HiddenSSID (~0 m) and Winona5* (~0 m) drawn as nearly coincident envelopes on Ch. 40 — the clone and the router indistinguishable in spectral position.

Channel graph — isolated genuine-router envelope (baseline)



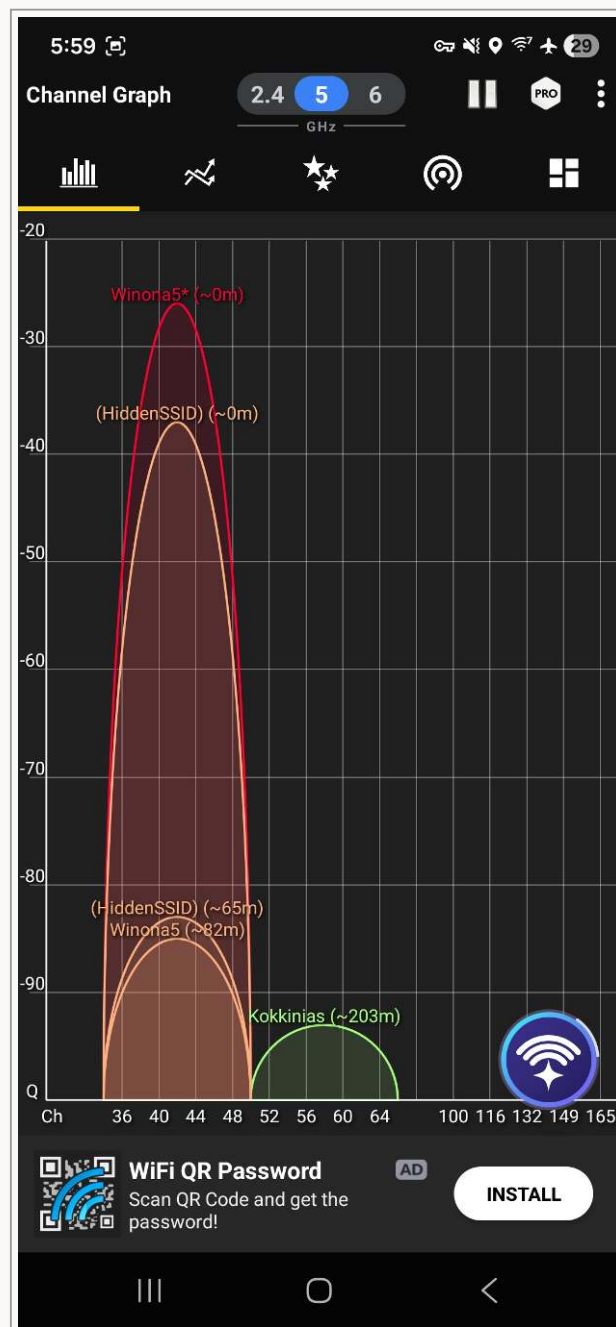
WHAT THIS SCREENSHOT SHOWS

A single Winona5* peak on Ch. 40 with the clone filtered out — the baseline shape of the genuine router alone, for comparison against the overlaid captures.

WHAT THIS SCREENSHOT SHOWS

Continuing electronic-surveillance evidence packet — Ehab Allababidi — July 15, 2026

Channel graph — final capture, twin still overlaid on Ch. 40



WHAT THIS SCREENSHOT SHOWS

The last capture (Jul 13, 17:59) shows Winona5* (~0 m) and a HiddenSSID (~0 m) still overlaid on Ch. 40, with Kokkinias distant — documenting that the Evil Twin remained operational continuously across the three-day window.

HASH MANIFEST — SHA-256 INTEGRITY RECORD

Cryptographic fingerprint of each native screenshot file, per the Declaration of Authenticity. Recompute with any SHA-256 tool to verify no file has changed.

Ex.	File	EXIF capture (local)	SHA-256
E-1	2492.jpg	2026:07:11 01:48:02	90b2b0f36ce3edc8bed3f49d8c94af35ca2af2200936d4875f9716c8c37ea66d
E-2	2494.jpg	2026:07:11 01:48:10	15d3afec660bfd8d9aedf328dd8c9a920da9f99a8f6ab2dc953e9ac559b928ad
E-3	2496.jpg	2026:07:11 01:48:17	236b9a58b3346975b33f684b13d65f80693559680edb7c6883e3428799ed50ec
E-4	2498.jpg	2026:07:11 01:48:22	55fe0056310b9e98fc434228137f04a4b5f686d69bcacf5d35408f701f6a0244a
E-5	2500.jpg	2026:07:11 01:49:25	68ea4467ad71caa30bb42088d3e915c64b9f1e8d40c565ff8157d7bf3e31fb4c
E-6	2502.jpg	2026:07:11 01:49:30	704631b1d220c2e6daaabbf0a4b1630e2d81b95b72dacd4badccfccc0c4fffd4
E-7	2504.jpg	2026:07:11 01:49:38	4013b91d73d734c288c25360f9fa2b12aa96ab32cdbbfff33a954143b4d87e46e
E-8	2506.jpg	2026:07:11 01:49:53	b139a4e97ec4095131d82796bbf6d36f3b7da1c0e6566fe6ab6cab19c24b8717
E-9	2508.jpg	2026:07:11 01:49:59	0cef6e251da08cc9d651060e65467a0678643db0eb8665796e25b3ac6996b5c1
E-10	2510.jpg	2026:07:11 09:48:53	9b0a6f43a1b3da437c324c074eb42dff4c55163225c036cb32d7e941973dcf11
E-11	2512.jpg	2026:07:11 09:49:10	376c5e5fb8eba60fdec4f0731740ff9face2f24369b2f2721cfe0ec9332efa1
E-12	2514.jpg	2026:07:11 13:47:25	68745b3fce181e146bbdbd0ee60d09d05ca545b90112f3b4b868fbd664e2ce86
E-13	2516.jpg	2026:07:11 13:47:32	740d3e1f9da69b742a776105c9e0c930362db2c3ee334f7c9dad0ce2b4e39a5
E-14	2518.jpg	2026:07:11 13:47:39	299996d54e556cd06783bf5441f8216d2a7864b04be5cb9731844809467a02b
E-15	2520.jpg	2026:07:11 13:47:49	22609a2da6755237bb6ca7c5558569462d047b71dcd203e8d948f4a2656803ad
E-16	2522.jpg	2026:07:11 13:47:57	d7619100857b2bfea9d6de4afad59d5245f2c3eeb8ba150f0d13156aacaac5f3
E-17	2524.jpg	2026:07:11 13:48:57	c0d91c4377f6b7c66aef43f5e1e7d204b5e86c1ad1210240ed7be0fd179ec41
E-18	2527.jpg	2026:07:11 22:55:15	08300f2fc68f8305c4d12063456c5bf79817db7f734709a030731dc9ec73e926
E-19	2529.jpg	2026:07:11 22:55:26	1084a3632898071acd8d0dcb8ba4a9999693c50e878fb777c4a018b303527db
E-20	2531.jpg	2026:07:11 22:55:51	b03135929b8ab3a646ca7f9fa1730a9b674381ab2f17735776af5c3aa1e80e8
E-21	2533.jpg	2026:07:12 00:17:03	84daa7f6a6c7051e3ea58dc313dc8463edf23e49eaf3d9a464bf95ff8252cd1e
E-22	2535.jpg	2026:07:12 00:17:12	0d15568f8aad9832e846bab30aab319a3b2631dc3c9b2c22cea7425808943b48
E-23	2537.jpg	2026:07:12 00:17:23	651e33597b5588e104b8fec36c045bbac95bd3b3f74e0087bf2223cf1133e641
E-24	2539.jpg	2026:07:12 00:17:31	b1d4eedbaeba83ff1aeb44988a30e7abd8eb1c102360d4edde6502e19a56be8f
E-25	2541.jpg	2026:07:12 00:17:39	cf3a5c552bfbb49096e9f63cd4276f710e56d0c16c6f49b5e94a682c2b5e58e2
E-26	2543.jpg	2026:07:12 12:45:39	123c69d1055adcc3fab14829ea02d30f08b68e48f26ac98d1dd66119422293fe
E-27	2559.jpg	2026:07:13 16:36:14	d746f27869bb84e6ba7701693bec3de75f430ed0275da266777b88a1f8dc1488
E-28	2561.jpg	2026:07:13 16:36:24	74063978b65110e39ccf681405ac4760b5cb1e975c5a93e82117558781290dd3
E-29	2563.jpg	2026:07:13 16:36:28	c7a4e6d2ca0e32bf526f9faf91d26b378efa6e23dd300bda36820802cee9bdf7
E-30	2565.jpg	2026:07:13 16:36:58	1fc3ad0ce071e3086ab651b9eadb514f924f3d819073fb5b679c5e04bcd1ab8
E-31	2567.jpg	2026:07:13 16:37:14	4c10abba8d70d3688e2f246a422e62d997cb61fc7ae196c9b384d2bfb11e3464
E-32	2569.jpg	2026:07:13 16:37:16	00dcf9892a7e09793cf53b322b21a9a1b0c39ab7228e1c8f0b59daf3b05605ae
E-33	2571.jpg	2026:07:13 16:38:24	6b51d17460d04fd3ff6d1b8799b1703b97fd525280ac9aef1286478e1550fb30
E-34	2573.jpg	2026:07:13 16:38:34	15ae983e4d11b6e7dda220f3566d4c07d8ce2291c8a33e4902d4f7d880fe2452
E-35	2575.jpg	2026:07:13 16:45:37	f9f1902e4aff07cf0edb87bf1b6f1f6ff4185554eebdfb14023171ad70f6abf7
E-36	2577.jpg	2026:07:13 16:50:25	dc9cd1d5e34436dbef0dc61b79b1873a4d7299bc5b550a8f58e13f67f356d21e
E-37	2579.jpg	2026:07:13 16:50:31	5869a6237dce1e06700bf123e96538f3edf5d9be85dc74a4cbb301d19dee8f8a
E-38	2581.jpg	2026:07:13 17:59:31	8b21ed50fdf1cfe0eeb0941ce3d07148ff895a85e32e1747b0abe21f3b9f4ae1
E-39	2583.jpg	2026:07:13 17:59:38	e402b04f1dc749e165a359663565dba4e0eb09383e5557c33eba4cfe1afc40d4