./how_to_read_the_codes

How to Read the Codes

El the Freedom Fairy (@el_freedomfairy)
Used in **El's Wrench Attack Coding Tool 2026** and **Map My Risk**
Dataset v2 · 13 November 2026 · page 1 of 2

MY DEFINITION OF A WRENCH ATTACK

Any event in which a person is targeted with **physical force**, **credible threat of physical force**, **real-world psychological coercion**, or **deception involving real-world presence**, with intent to compel the transfer, disclosure, or surrender of cryptocurrency or cryptographic access credentials (private keys, seed phrases, PINs, or passwords).

A burglary where the victim is absent does **not** qualify. What is distinctive is the combination: physical coercion meets direct control of cryptographic credentials, and the transfer is final and needs no institution, so the safeguards of traditional finance (limits, reversals, fraud holds) don't apply. A distinctive form of robbery and extortion, not an entirely new category of crime.

TYPE A — How the victim was chosen · multiple allowed

A-OP	**Opportunistic** — no prior selection; the attacker found out about the crypto by chance
A-TG	**Targeted** — victim deliberately selected before the attack (includes lure robberies)
A-RP	**Repeat victimisation** — same victim attacked more than once
A-PX	**Proxy** — a relative or associate used as leverage to reach the holder
A-TG/PX	**Targeted + proxy** — holder targeted and household members held as well

TYPE K — How the attacker knew · one main code

K-PUB	**Public profile** — social media, press, talks, being publicly known in crypto
K-LEAK	**Leaked or bought data** — e.g. tax-platform or exchange leaks, dark-web data
K-INS	**Insider / personal connection** — friend, relative, partner, colleague or business contact who knew
K-TRADE	**Self-identified in a trade** — victim made contact to buy or sell crypto (P2P, lure meetings)
K-NONE	**No prior knowledge** — discovered on the spot
UNKNOWN	**Not reported** — the reporting doesn't say how the attacker knew

More than one applies → main code in the order INS, LEAK, PUB, TRADE. Wrong-target cases are coded by the source the attacker used.

TYPE B — Level of planning

B-1	**None** — zero planning
B-2	**Semi-planned** — target identified, not thoroughly researched (e.g. wrong address)
B-3	**Fully planned** — research, surveillance, set entry method, briefed crew, equipment
B-4	**Organised** — B-3 plus a transnational network, division of labour, purchased or leaked data, or a remote orchestrator

CONF — Confidence rating · how well verified

A	**Court / LEA verified** — court documents, police or prosecutor statements, indictments
B	**Multi-source** — two or more independent credible media sources
C	**Single source** — one credible media report
D	**Community report** — unverified, internally consistent, uncorroborated

How to Read the Codes

El the Freedom Fairy (@el_freedomfairy)
Used in **El's Wrench Attack Coding Tool 2026** and **Map My Risk**
Dataset v2 · 13 November 2026 · page 2 of 2

TYPE C — Physical harm · highest level reached by any victim

C-0	**No physical harm** — threats only, including weapons shown or pointed; foiled before contact
C-1	**Minor force** — pushed, grabbed, held down, tied up, or struck with only minor bruising
C-2	**Injury** — more than minor: serious bruising, cuts needing stitches, knocked out, taser injuries, drugging
C-3	**Grievous harm** — broken bones, stabbing, shooting, burns, mutilation, torture, sexual violence
C-4	**Fatal** — a victim was killed during or because of the attack

Based on the injury thresholds for common assault, actual bodily harm (ABH) and grievous bodily harm (GBH).

W — Weapon · reported or not

Yes	**Weapon reported** — type shown where known: GUN · FAKE (replica) · BLADE · STUN · BLUNT · OTHER
No	**Ruled out** — only when the reporting says no weapon was used
UNKNOWN	**Not reported** — the reporting doesn't say

TYPE L — Loss of liberty · highest level reached

L-0	**None** — not restrained or confined
L-1	**Brief restraint** — tied up or held at the scene for under an hour, or for a length not reported
L-2	**Held 1 hour+** — held at the scene, usually their home, for an hour or longer
L-3	**Abducted** — forced to move to another place (vehicle, another building), any length

Lured to a meeting is not abduction unless the victim is then forced to move.

TYPE E — Access method · multiple allowed

E-UW	**Unlocked wallet** — device already unlocked or wallet open
E-PW	**Password / PIN coercion**
E-SP	**Seed phrase disclosure**
E-AT	**Forced transaction** — victim forced to sign or approve a transfer
E-LN	**Lightning Network**
E-MX	**Multi-sig coercion**
FAILED	**Nothing obtained** — crypto was sought but none taken; reason in brackets

TYPE D — Relationship · offender to victim

D-S	**Stranger** — no prior contact
D-P	**Pseudo-stranger** — posed as police, a courier, a buyer or a business contact
D-A	**Acquaintance** — known socially or professionally
D-I	**Intimate / family** — genuine partner, spouse, parent, child
D-R	**Romance lure** — offender built or faked a romantic or dating relationship to reach the victim
D-B	**Business associate** — current or former business partner, employee or provider

CODING RULES

- **UNKNOWN** — the reporting doesn't say. It is not the same as "none".
- **PROVISIONAL · UNDER REVIEW** — coded under my rules but not yet reviewed by me; may change
- **Outside my definition** — coded, but marked No or Unclear against the definition
- **N/A** — the field doesn't apply (e.g. Type E when no crypto was sought)
- **Multiple codes** allowed for Type A and Type E only; C and L take the highest level reached

SOURCE & METHOD

Cases come from **Jameson Lopp's Known Physical Bitcoin Attacks** database (2026 entries, 147 cases). Each case is coded with AI assistance under these rules from Lopp's summary, the sources he links and further reporting, then reviewed by me. Dataset v2: 11 cases reviewed so far; the rest are provisional. Codes may change as fuller reporting emerges.