# TANGODOWN

SECURITY

# Manual

Version 0.87.0 · 06 November 2026

Free hobby project by Lars Stahl – without warranty. Current version and download: https://tangodown.eu

# Contents


1 **New in recent versions** 5

2 **Getting started** 5

- Module overview 6
- What do the buttons mean? 6

3 **Basic terms** 8

4 **Abbreviations and acronyms** 9

5 **Case & analysis** 12

- Case file 12
- Case assistant 13
- Investigation Graph 13
- Analysis 16
- Search Around (neighborhood search) 17
- Classification (Admiralty code) 17
- Properties 17
- Timeline 18
- Matching 18
- Report Builder 18
- Data import 19

6 **Research** 19

- Investigation autopilot 19
- AI 20
- AI web search 21
- AI research 21
- AI analyst 22
- AI second opinion in modules 23
- AI tasks (recurring) 24
- Net intel 25
- Subdomains 25
- Domain tools 26
- Cyber intelligence 27
- Shodan 28
- OSINT tools 28
- Chain-Trace 29
- Bitcoin Discovery 29
- SOCMINT 30
- Platform accounts (signed-in research) 32

- Browser ..... 32
- Evidence capture ..... 35
- Case files & documents ..... 36
- File forensics ..... 36

**7 Matching ..... 36**

- Vehicle matching ..... 36
- Universal search ..... 37
- Registers & databases ..... 37
- Custom databases ..... 38
- Face matching ..... 38

**8 Situation & map ..... 40**

- Message center ..... 40
- Geo-Intel ..... 40
- Social search (the easy way) ..... 42
- World clock ..... 43
- Source monitoring ..... 43
- Outgoing webhooks ..... 44
- Situation picture ..... 45
- Alerts & watchlist ..... 45
- Camera pool ..... 46
- Webcams & video · ▣ Monitoring walls ..... 46

**9 Tools ..... 49**

- Remote cameras via VPN ..... 49
- Single-target scan (authorized) ..... 50
- Remote access ..... 51
- Terminal ..... 51
- Vault & connectors ..... 54
- Connection & cloaking ..... 55
- Types & symbols ..... 56
- Audit log ..... 56
- Help & info ..... 56
- Terms of use & disclaimer ..... 57
- Administration · ◐ Design ..... 58
- Streaming mode (privacy when presenting) ..... 58
- Demo mode ..... 60
- Sandbox & VMs ..... 61
- Connect Proxmox – step by step ..... 64
- Email analysis ..... 65
- PCAP and log analysis ..... 66
- Plugins ..... 67
- Data source status ..... 68

◧ Workspace templates 68

**10 Data, migration & portable mode 68**

Automatic backup 68
Back up & restore (single or all cases) 68
⇄ Where is my data? 69
How are the keys protected? 70
⇧ Migration package – take everything to a new PC 71
Portable mode (USB stick) 72

**11 Use cases 73**

Fake shop or fraud domain 73
Missing person 73
Vehicle from a lead 73
Situation picture for an event 73
Crypto money flow 73

**12 Principles 73**

**13 Keyboard shortcuts 74**

**14 Terms & abbreviations 75**

# TangoDown Security – Manual

TangoDown Security is a workspace for case handling, OSINT (open-source intelligence) and situation picture. Everything you research ends up in an **encrypted case**: people, companies, domains, wallets, vehicles, evidence, documents – with source, timestamp and checksum. Every work step is recorded in the **audit log**.

This manual describes every module: what it is for, how to use it and what it is typically used for. At the end you will find usage scenarios and principles.

> **Important:** Use of TangoDown and of all extensions (plugins, connectors, interfaces) is at your own risk. TangoDown provides leads, not finished truths. **Check every result yourself** before you use it – hits, assignments, similarity scores, translations, AI answers and data from third-party sources. Sources can be wrong, outdated or incomplete.

> 🍼 **Still in development and testing:** TangoDown is a free hobby project developed by a single person in their spare time. The software is still being tested – there are certainly still bugs and a lot to improve, and some areas or functions may not yet work fully. Feedback is very welcome and helps to improve things in a targeted way: ideally with the version, the exact steps leading to the error (reproducible), what you expected and what happened instead, preferably with a screenshot and the diagnostic report ("Help & info → Contact → 🩺 Create diagnostic report") – to info@tangodown.eu or via the contact form on tangodown.eu. If you would like to support the work, you are welcome to do so via crypto or PayPal (tangodown.eu → Support).

## New in recent versions

- **0.87.0 – Alerts in one place:** " +  New alert" for hashtag, place (e.g. "Berlin"), domain, crypto address or username with two inputs; all alert rules in one list to view, pause, change and delete; every received alert shows its source.
- **Situation picture:** clicking a signal flies to the country and marks it; evidence with origin, time and "↗ Open source".
- **Live situation:** sightings create the ship or aircraft as an element with all identifiers, linked to the sighting.
- **Portable with a fixed file name:** `TangoDown-Security-portable.exe` – shortcuts stay valid across updates.
- **Topic demos in English:** six short demos in Demo mode – alerts & situation picture, from a name to the picture (person), working with AI, Social Deck, video walls & live streams, built-in browser.

## Getting started

**Can't find where something is? Ctrl+K.** The command palette finds modules, functions deep inside the modules (e.g. "proxmox zugang", "alarme einstellen", "tracker", "yt-dlp"), elements of the case, map symbols and every section of the manual. Opened empty, it first shows what you **used last**, then the common case actions; rarely used setup functions appear as soon as you search for them. **German and English, other words too:** The search knows equivalent terms in both languages – "Nummernschild", "license plate" and "Kennzeichen" lead to vehicle matching, "wallet" or "money flow" to Chain-Trace, "metadata" or "remove metadata" to file forensics, "new computer" or "backup" to data & migration. Hits with the exact word come before similar ones. **Search scope:** Below the search field you choose **All**, **Without help** (no manual sections) or **Modules only**; **Tab**

switches, the choice is remembered. Manual sections where the word only appears in the text show the matching excerpt and come after the functions. When the search jumps into the manual, your search word is **highlighted** there; "hit 1 of n", ↑/↓ or Enter and Shift+Enter move from hit to hit.

- **Partial words are enough:** "zugangsd tik" finds "Plattform-Zugangsdaten".
- **Umlauts and typos** are forgiven: "quarantaene", "proxmx", "strem".
- **How it works:** The closest matches are at the top, Enter jumps straight to the first.

### ☷ Module overview

⧉ **In new window:** Every card in the module overview has, next to "↗ Open", the button "⧉ In new window" – the module opens as a separate window at full screen size and can be dragged onto a second screen. If it is already detached, that window comes to the front and is maximised.

**What for:** All TangoDown modules at a glance – grouped by area, each with a short explanation of what the module does.

- **Open:** click a card or "↗ Open"; "? Manual" jumps to the matching section in this manual.
- **Search:** the field at the top filters by name, purpose and keyword (e.g. "map", "Bitcoin", "video"). Experimental modules are marked with 🧪.
- **Call up:** Ctrl+K → "Module overview" or via the area selection.

**Without an open case:** Investigation modules (graph, browser, evidence capture, queries, maps, monitoring etc.) only work in an open case. If none is open, the module shows the note "… needs an open case" with "▤ Open or create a case" and "✦ Case wizard" instead of its content. Usable without a case: case file, case wizard, vault & connectors, connection & cover, data & migration, administration, design, types & icons, plugins, data source status, world clock, module overview, manual, help & info and the demo mode – as well as the cross-case collections **custom databases**, **camera pool** and **monitoring walls**, which you can maintain without a case.

### What do the buttons mean?

**In short:** Three kinds of buttons appear in many modules – they are named the same everywhere.

- **"＋ Add as element"** stores results permanently as **elements** in the case (e.g. person, domain, IP, account – with links and source). They then appear in the graph, in "Properties", in the timeline and can be included in the report.
- **"◈ Show in graph"** stores nothing – it only jumps to an element that is already in the case, zooms in and briefly highlights it. ("◈ Add to graph as element" in "Case files & documents", in contrast, first creates an element from a record and then jumps to it.)
- **"▦ Add to report"** creates no element – it inserts a text block (e.g. AI answer, evaluation, explanation) into the draft in the report editor; there it can be edited and appears in the PDF/DOCX.
- **Saved** (web pages, images, videos) means: stored as an immutable record in the case – found in "Case files & documents", not as an element in the graph.

**✂ Snipping everywhere:** Every area has a **✂ button** at the top right of its header (also in separate windows), the status bar at the bottom has **"✂ Section"**, and Ctrl+K finds "section". You choose **"Select an area in TangoDown"** (windows stay visible) or **"Select an area on the whole computer"** (TangoDown is briefly hidden, also Ctrl+Shift+X). The section is stored with checksum in files & documents; the preview offers "Into the graph", "To report" and "Show in files".

📊 **Resources in the status bar:** "CPU · RAM · GPU" shows how much TangoDown itself loads the computer – CPU share of the whole computer, memory of all TangoDown processes and whether graphics acceleration is running (✓) or missing (⚠, then face matching, maps and graph are much slower). A click shows the usage per area (main process, windows, browser tabs) and the computer's free memory. Measured locally only, nothing is sent. Hide: click → "Hide resource display"; show again: Ctrl+K "resource display". If your own AI (Ollama) runs on the CPU only, the AI area additionally shows "⚠ CPU" next to "● local".

1. **Create a case:** Start page → "New case". Enter case number, title, client, **legal basis**, **purpose** and **retention deadline**. No purpose, no research – this protects you and the people concerned. **Free mode (only in the edition for private investigators – PI, "private investigation" –, only when creating):** in the form under **"▸ Advanced: special cases without mandatory details or logging"** (collapsed so nobody ticks it by accident). "Without required details" – justifications, purpose and legal bases are no longer requested anywhere (e.g. face matching, queries, registers, deletion). "Without logging" – actions and queries are not written to the audit log; only the creation and the mode itself are recorded there. The case is marked at the top with "NO LOG" or "FREE", reports state it, and both can be switched back on in the case file (but not switched off afterwards). Responsibility for purpose limitation and data protection remains with you; without a log it cannot later be shown who queried what – such a case has **no audit trail** and is marked accordingly. The Agency edition has no free mode.
2. **Open modules and find elements:** in the bar on the left, via the command palette (**Ctrl+K**, search terms like "karte", "kennzeichen", "zeit") or by right-clicking an entity. Ctrl+K also finds all elements of the case (parts of name, type, details, notes – e.g. "ip 66.147") and the map symbols on the map (e.g. "panzer 77"); Enter jumps straight there in the graph or on the map.
3. **Layout per case:** Every case remembers its layout – which modules are open, which are popped out as a separate window and on which screen, at which position and in which size they were. The next time you open the case, everything comes back that way. Can be switched off under "◐ Design → Usability". A layout can also be saved as a **view** (View ▾ → "Save view …") and loaded again in any case, including the window positions.
4. **Arrange the workspace:** Modules can be moved like windows, docked side by side, popped out as a separate window (⤢) and maximized. Right-click a tab: close, pop out, enlarge. Popped-out windows carry the name of their active area (Windows taskbar, Alt+Tab). With many tabs in one area, the active tab always stays visible; you reach the others via the "+N" button. Popped-out windows (e.g. the monitoring wall on the second screen) open again as **separate windows** at the next start; after that the main window comes to the front. The ✕ of a popped-out window – also the Windows ✕ at the top right – **closes the window together with its areas**. "↘" (top right in the window or right-click on the tab) brings it back into the main window. If you prefer ✕ to put the area back: right-click on the tab → switch off "Window ✕ (also the Windows ✕ at the top right) closes the area" (or Ctrl+K "Own windows"). This then applies to all areas, including monitoring walls and webcams & video; they come to the front visibly in the main window. An area that returns to the main window briefly lights up there (the main window comes to the front). Only the ✕ of the main window quits TangoDown. **Opening links:** Wherever TangoDown opens a link (searches, sources, profiles, explorers …), a choice appears at the mouse: **"🌐 In TangoDown browser"** (via your network route, session in memory only), **"↗ In system browser"** (your own IP) or **"⧉ Copy link"**. "Always in …" remembers the choice; change it under **Design** → **Usability** → **Opening links**. In tunnel mode the system browser never opens (it would run with your own IP) – the link then goes to the clipboard. **Running:** Buttons with an ongoing operation ("searching …", "loading …", "capturing …") show a spinning circle and a pulsing border – so you can see everywhere that work is still going on. **Tidy:** TangoDown automatically removes

empty areas (without content); if a module opens into a strip that is too narrow, it is widened. If the layout is still messed up: **View** → **"↺ Restore default view"**.

5. **Zoom:** Ctrl+mouse wheel enlarges the display, Ctrl+0 resets it – also in popped-out windows.
6. **Right-click is your best friend:** Almost everything has a context menu – entities, map, graph, symbols, geofences, table entries.
7. **Watch the demo:** Module "✪ Demo mode" (Ctrl+K → "Demo" or at the top of the manual). There, choose speed, modules, full screen and demo case, then "▶ Start demo".
8. **Search across cases:** Module "⌕ Universal search" or Ctrl+K, type a term → "Search all cases".
9. **Help right in the area:** The "?" at the top right of every area opens the matching section of this manual. The whole manual is available as a PDF at the top.
10. **Jump there:** After every hand-over ("Into the case", "Into graph", backup, plugin result …) the confirmation at the bottom right has a button like "⌬ Show in graph" or "⎙ View capture" – it takes you straight to the result.
    - 🕘 **Recent:** Every such result is also listed at the bottom of the status bar under **"🕘 Recent (n)"**. A click shows the list of the latest results (captured page, recording, hits in the graph, pool entry …); an entry jumps straight to where it is stored – even long after the message has disappeared.
    - **Longer-running tasks** (video download, livestream recording) show a message that **stays**: during recording with progress and "■ Stop", afterwards with the result and "⎘ Open recording" or with the error. Close with ×.
    - **Errors are always reported:** If an action fails, the cause appears at the bottom right – no button silently does nothing.

## Basic terms

- **Case:** all data of an investigation in one encrypted file – can only be opened on your workstation (portable: only with the master password).
- **Entity:** an element in the case – person, username, account, email, domain, IP, company, place, photo, phone, crypto address, organization, hoster, post, note, topic, event, webcam, vehicle – or a custom type.
- **Link:** a justified relationship between two entities ("Managing director", "Registered keeper", "uses phone number").
- **Classification (Admiralty):** reliability of the source (A–F) and credibility of the information (1–6), e.g. "B2".
- **Audit log:** every query, change and export with time, person and justification – later changes would be noticed immediately.
- **Subgraph:** a named section of the case, e.g. the result of an investigation.
- **Recovery key:** a long code to print out, with which a forgotten master password or a lost administrator access can be replaced.
- **2FA (two-factor sign-in):** in addition to the password, a changing 6-digit code from an app on your phone (TOTP = time-based one-time password).
- 🧪 **Experimental:** Areas marked this way (e.g. face matching, VM sandbox, platform accounts, AI research, camera recording) work, but depend heavily on third-party programs, platforms or AI models. Check results

there with particular care – like all results (see Principles). The notice can be minimized with one click or switched off entirely under **"◐ Design"** ("Show 🧪 Experimental notices").

- **Confirm file access:** Files you drag in via drag & drop or via "Choose…" are used by TangoDown directly. If TangoDown is to access a file you did not select yourself, it asks first. Network paths (shares on other computers) only work via drag & drop or selection.

## Abbreviations and acronyms

A short explanation of what the abbreviations in TangoDown and in this manual mean – no expert knowledge needed. Missing one? Press Ctrl+K and type the abbreviation to find the place in the manual.

| Abbreviation | Stands for | What it means for you |
|---|---|---|
| **A1 … F6** | Admiralty code | Rating of a lead: letter = how reliable the source is (A very, F cannot be judged), digit = how certain the information is (1 confirmed, 6 cannot be judged). |
| **ADS-B** | Automatic Dependent Surveillance – Broadcast | Radio signal aircraft use to broadcast position and identity; the aircraft on the situation map come from it. |
| **AES-256** | Advanced Encryption Standard, 256 bit | Encryption method protecting cases and backups. |
| **AIS** | Automatic Identification System | Radio signal ships use to broadcast position, name and course; the ships on the situation map come from it. |
| **API** | Application Programming Interface | Interface through which programs talk to each other – e.g. TangoDown with a data service. An "API key" is your access to such a service. |
| **ASN / AS** | Autonomous System (Number) | Number of a network operator on the internet (e.g. a hoster or provider); shows who owns an IP range. |
| **BDSG** | German Federal Data Protection Act | German data protection law that supplements the GDPR. |
| **BOS** | authorities and organisations with security tasks (Germany) | Police, fire brigade, rescue services, THW etc. – a group of map symbols. |
| **BTC / ETH / XRP / BNB** | Bitcoin / Ether / Ripple / BNB | Cryptocurrencies whose public payments Chain-Trace can follow. |
| **BUS · ENT · LNK · evt** | event bus · entities · links · events | Abbreviations from the status bar up to version 0.61: number of internal events, elements and links. Since 0.62 it shows plain words ("50 elements · 48 links"). |
| **CNAME / MX / TXT / NS** | DNS record types | Entries in the internet's phone book: CNAME = alias to another name, MX = responsible mail server, TXT = free text (e.g. SPF), NS = responsible name server. |
| **CPU / RAM** | processor / memory | Computing power and memory, e.g. when setting up a VM. |
| **CSV / TSV** | comma- / tab-separated values | Simple tables as a text file (columns separated by comma or tab), e.g. for import. |
| **CVE / CVSS / KEV** | Common Vulnerabilities and Exposures / … Scoring System / Known Exploited Vulnerabilities | CVE = ID of a known security hole; CVSS = severity from 0 to 10; KEV = list of holes known to be exploited (US agency CISA). |

| Abbreviation | Stands for | What it means for you |
|---|---|---|
| **DKIM / SPF / DMARC / BIMI / MTA-STS** | e-mail checks | Rules of a domain that let you check whether an e-mail really comes from there (signature, permitted sending servers, policy, logo, transport encryption). |
| **DMS** | document management | Storage of documents with origin and versions ("Files & documents" module). |
| **DNS** | Domain Name System | The internet's "phone book": translates names like example.com into IP addresses. |
| **DOCX / PDF** | Word document / Portable Document Format | File formats for reports: DOCX can be edited further, PDF cannot. |
| **DPAPI / TPM** | Windows data protection / security chip | Protection by Windows or a security chip in the computer: keys are bound to your user account or device. |
| **DSGVO** | GDPR (General Data Protection Regulation) | EU data protection law; governs among other things the purpose, legal basis and retention deadline of every case. |
| **EXIF** | Exchangeable Image File Format | Extra data in photos, e.g. time taken, camera and sometimes the GPS location. |
| **FIDO2 / TOTP** | hardware key / time-based one-time codes | Second factor when unlocking: a USB key (e.g. YubiKey) or a 6-digit code from an app. |
| **FIN / RDW / DVLA / NHTSA** | vehicle identification number / vehicle registers NL, UK, USA | VIN = 17-character number of a vehicle; the others are authorities whose open vehicle data the vehicle check uses. |
| **GDELT / OTX / RSS** | news database / Open Threat Exchange / news feed | Public sources: worldwide news, threat intelligence, subscribable news lists. |
| **GPS** | Global Positioning System | Satellite positioning; provides coordinates (latitude/longitude). |
| **HLS / RTSP / MJPEG / ONVIF / VOD** | video formats and protocols | Ways webcams and live videos are transmitted; VOD = recording on demand. |
| **HTTP(S) / TLS / URL** | web protocol / encryption / web address | HTTPS is the encrypted form (TLS); a URL is the full address of a page. |
| **IBAN** | International Bank Account Number | Account number of a bank account. |
| **ID / UID** | identifier | Unique number of an element, account or device. |
| **IMEI** | International Mobile Equipment Identity | Device number of a mobile phone. |
| **IP** | Internet Protocol (address) | The "house number" of a device on the internet, e.g. 203.0.113.9. |
| **ISO / WSL / QEMU / VM** | disk image / Windows Subsystem for Linux / emulator / virtual machine | A VM is an isolated computer inside the computer (e.g. for suspicious files); an ISO is the installation file for it. |
| **JSON** | JavaScript Object Notation | Text format for structured data, e.g. for plugins and interfaces. |
| **KI** | AI (artificial intelligence) | Language models that summarise texts and make suggestions – always check the results. |

| Abbreviation | Stands for | What it means for you |
|---|---|---|
| **MCP** | Model Context Protocol | Standard through which AI programs can use TangoDown tools (see developer guide). |
| **MHTML / PNG / JPEG** | web page archive / image formats | In evidence capture: the page as a file with its content (MHTML) and as an image (PNG). |
| **MMSI** | Maritime Mobile Service Identity | 9-digit radio identifier of a ship. |
| **NAS / USB** | network storage / USB drive | Possible destinations for backups. |
| **NAT / DHCP** | address translation / automatic address assignment | Network technology in the router; you meet it with VMs and in PCAP analysis. |
| **OSINT** | Open Source Intelligence | Investigation from publicly available sources – the core of TangoDown. |
| **PCAP** | packet capture | Recording of network traffic as a file (e.g. from Wireshark). |
| **PI** | private investigation | Edition for private investigators. |
| **RDAP / WHOIS** | registration lookup | Query of who registered a domain or IP (as far as public). |
| **REST** | Representational State Transfer | Type of web interface; TangoDown offers one for your own programs (see developer guide). |
| **SHA-256 / HMAC** | checksum methods | Digital fingerprint of a file or entry: if even one character changes, the checksum changes – this shows that nothing was altered. |
| **SMS** | Short Message Service | Text message to a mobile phone, e.g. as an alert channel. |
| **SOCKS / VPN / Tor** | proxy protocol / Virtual Private Network / The Onion Router | Ways to hide your real IP address: the connection runs via an intermediate computer (proxy, VPN) or several (Tor). The top right shows whether you are cloaked. |
| **SOCMINT** | Social Media Intelligence | Investigation in social networks (profiles, usernames, posts). |
| **SSH / SFTP / FTP / RDP** | remote access protocols | Connections to other computers: commands (SSH), files (SFTP/FTP) or screen (RDP). |
| **StPO** | German Code of Criminal Procedure | German law for criminal proceedings; legal basis in the agency edition. |
| **UTC / LOC** | Coordinated Universal Time / local time | Clocks at the top right: UTC is the uniform world time (used in the log), LOC the time of your computer. |
| **VS-NfD** | German classified – restricted | Lowest German classification level; a possible classification of a case. |

# Case & analysis

## ▤ Case file

🔒 **Finalize case:** When a case is finished, click "🔒 Finalize & archive …" in the case file and enter a closing note (e.g. "Report handed over to client"). Then the following happens:

- TangoDown records an audit checkpoint.
- The case's watchlist, monitoring and AI tasks are paused.
- From then on all contents are **read-only**. This is locked in the case database itself, not just in the interface.
- **"🔓 Undo closure …"** requires a justification and is recorded in the audit log; in the Agency edition only for management or administration.
- The case selection then shows the case in the **"Archive"** tab instead of among the active cases.
- Tip: create the final report in the Report Builder beforehand.

**Leaving is not finalizing:** "⏏ Leave case" at the bottom of the case file only closes the case and goes to the case selection – it stays among the active cases and can still be edited. "⇄ Open another case" shows the case selection without leaving the case. A case only goes to the archive via "🔒 Finalize & archive …": it is then closed, and the case selection opens on the "Archive" tab.

**Case selection:** Two tabs – **"Active cases"** (active and dormant) and **"Archive"** (finalized, with date and note). Each card shows the **status** at the top right (active, dormant, 🔒 finalized) and the **classification** below it (OFFEN or VS-NfD). The **"Filter cases"** field searches for partial words in case number, title, client, purpose and closing note – several words must all appear, case does not matter. If a hit is in the other tab, TangoDown offers to switch. Esc clears the field.

**Change status directly:** Clicking the status of a card (e.g. "active ▾") opens a menu: **active**, **dormant**, **"🔒 Finalize & archive …"** (with a note) or, for archived cases, **"🔓 Undo closure …"** (with a justification). This also works without opening the case; every change is recorded in the case's audit log.

**Retention deadline:** At startup TangoDown reminds you of cases whose retention deadline has passed and, if you wish, jumps to the case overview. There you delete the case or extend the deadline with a justification.

👥 **Team · Exchange state:** Several investigators work on the same case, each in their own encrypted copy.

- **"⇧ Send my state …"** creates an encrypted case package. You agree on the passphrase together and share it separately, not in the same email.
- **"⇩ Import a colleague's state …"** merges their package into your open case:
  - New elements and links are added.
  - For elements both of you have, the more recent details win; properties are merged.
  - **You see a preview first:** which elements would be added and which values would change (current vs. new). Only "Merge" takes over; "Cancel" leaves everything as it is.
  - Nothing is ever deleted.
  - Can go back and forth as often as you like, without duplicates.
- Every import is recorded in the audit log, every imported property with the provenance "Team sync · Name" (Properties → Provenance).
- The initial copy is obtained as usual via case export or import on the start page.

**What for:** Master data of the case – assignment, legal basis, purpose, classification, retention deadline, compliance status, key figures.

**How to use:** Edit fields directly; the retention deadline shows how many days remain. Under **"External queries"** you see whether the case may query the internet; "Block for this case" turns on the **query lock** (work in the case file only).

**Typical:** Document the case properly before researching; check whether all required details are present.

### ✧ Case assistant

**What for:** From the occasion to a workable case in four steps.

**How to use:** Choose the case type (vehicle, person, crypto, domain/server, situation), enter the occasion, paste known starting values one per line – license plates, names, emails, domains, IPs, phone numbers and wallets are detected automatically. Then set legal basis, purpose, retention deadline and classification and click "✧ Create case". The assistant creates the starting values as elements, loads the matching workspace template and, if you wish, prepares the investigation autopilot (each step only after approval).

### ⌬ Investigation Graph

**What for:** All entities and links as a network – visible who is connected to whom.

**Explain connection:** Right-click an element → "⇋ Explain connection with …", then click the second element (or select two elements and right-click). TangoDown shows all short paths between the two, highlights the chosen path in the graph and names the weakest link (Admiralty code) – the chain is only as strong as its weakest link. For each step the supporting evidence is listed (source, classification, who and when). Optional: "✦ AI explanation" with mandatory citations (the AI may only use this evidence, every sentence needs an evidence number) and "⇄ Second opinion" from a second model with comparison. "▦ Add to report" takes everything over with its evidence.

**How to use:** Drag to arrange, double-click to focus, right-click for queries (transforms), link by dragging. The queries in the right-click menu are grouped by area (e.g. "Network", "Domain tools", "Crypto"): expand an area and choose a query – or **"▶ Run all from this area"**. As in Maltego, the findings appear around the clicked element, linked and highlighted; from there you continue by right-clicking. Create subgraphs to work on one aspect.

**Several graphs, windows, closing vs. deleting:** Via the **"⌬ Graphs"** menu (graph bar) you open every graph of the case (overall graph + all subgraphs); the item **"⧉ Each graph in its own window"** pulls them all out into separate windows – handy for multiple monitors. You pop out a single graph window (or any tab) via right-click → "Pop out into separate window". **Important: Closing** a graph window or tab **with X deletes nothing** – the graph stays saved in the case and can be opened again via "⌬ Graphs". **Deleting** is a separate action in the "⌬ Graphs" menu ("✕ Delete this graph") **with a confirmation prompt**; even then the **elements stay in the case**, only the grouping is removed. The same applies to all module tabs: X closes the view, data stays in the case.

▣ **Image of the graph:** The **"▣ Image ▾ "** button in the graph bar takes a snapshot – of the **whole graph** or the **visible section**, always with real labels. Either **save it into the case** (files & documents with checksum; then a preview with "To report", "As element into the graph"), **save it as a PNG file** or **copy it to the clipboard** (to paste into mail, chat, Office). Below that you find the free selection (snipping).

**Search and filter:** The search field at the top of the graph – substring in name, type, properties (name and value), notes and source. Several words must all match; `typ:ip` (or `art:firma`) narrows to one kind, e.g. `typ:ip 66.147`. Hits are highlighted in yellow, the rest dimmed; "◐ Highlight" switches to "▼ Hits only" (rest hidden). Enter or ⌖ fits the hits into view, Esc clears the search.

**Edit and add (at the top of the right-click menu): "◎ Edit in Properties"** opens the element for editing (fields, classification, place, note); **"⧉ Edit in separate window"** does the same as a separate window; **" + Create new entity and link ..."** – choose a type, enter a name: the new element appears next to the clicked one, is linked right away and can be completed in the Properties panel.

★ **Recommended:** At the top of the right-click menu, the one or two queries that yield the most for this type and the current state of the investigation appear **in yellow with ★** (e.g. for a domain without an IP "Resolve DNS", for a hashtag "Fetch recent posts"), with a short reason. In the expandable areas the same queries are marked with ★. If a label looks like a hashtag ("#...") or username ("@...") but the type does not match, "Change type" is recommended first.

🔎 **Hits directly into the graph:** For persons, companies, email addresses, user names, phone numbers and domains, the area "Web search: hits into the graph" offers queries whose results are **offered to you for adoption**: **"Web search"** (pages that mention the name or address – as a finding with address and excerpt), **"Search profiles"** (LinkedIn, Xing, Facebook, Instagram, X, TikTok – as a possible account) and **"Where is ... mentioned?"**. For persons and companies they appear as ★ recommendation at the top.

**Adopting hits:** After the search, TangoDown shows all candidates in a list – with kind (finding, possible profile, "mentioned on", Google Places entry), address, excerpt and reason. **Preselected** is only what demonstrably contains the value searched for (name, number in any spelling, address); the rest is listed with "check first". "↗" opens a page for checking – the hits window collapses to a bar at the bottom (also when clicking beside it), the selection is kept; "▲ Back to selection" reopens it. While the search runs, the message at the bottom right shows which query is running, how many hits there are so far and which search service does not answer; "■ Cancel" stops it after the current query. Only **" + Adopt selected"** creates and links the elements. All hits are **unverified** (F6) – people with the same name are common; check yourself whether a hit belongs, and delete what does not fit (Ctrl+click for several, then Del). Ctrl+Z undoes the whole query. The search term is sent to the search service (DuckDuckGo, with a Brave key Brave) and recorded in the audit log.

**How each type is searched (at most three queries):**

- **Person:** name in quotes; if a company or place is linked (or entered as a field), also name + company or name + place – this separates people with the same name. Profile search separately for professional (LinkedIn, Xing) and private platforms.
- **Company/organization:** name + "Impressum" (imprint), name without legal form + place, name without legal form. In addition **"🏛 Registers, company data & reviews"**: specifically North Data and OpenCorporates, Bundesanzeiger, company and commercial registers as well as kununu, Trustpilot and ProvenExpert – hits are labelled by source in the adoption list (e.g. "Company data (North Data)", "Employer reviews (kununu)").
- **▶ Check all round:** Below the ★ recommendations, "Check all round (investigation autopilot)" starts the complete workflow for the type – e.g. for domains DNS/Whois, start page, imprint, subdomains and mentions, for companies imprint, registers, company data, reviews and profiles. You tick what should run; the results land in their own sub-graph.
- **Phone number:** in common spellings (e.g. "04121 231 0", "04121/231-0", "+49 4121 231 0"). Websites whose hits literally mention the number are linked as **"mentioned on"** – usually the owner's imprint (phone directories and review portals excluded). Possible owner, not verified.
- **Email:** For **free mail providers** (gmail.com, gmx.de, web.de, outlook.com, t-online.de ...) the domain says nothing – user name and mentions are recommended. For an **own domain** TangoDown first recommends **"Capture the domain's imprint"** (operator, address, responsible persons) and the domain check; for role addresses (info@ ...) that is the actual lead. The search covers the exact address, the obfuscated spelling

("name [at] domain"), for personal addresses local part + domain; websites that mention the address are linked as for phone numbers.

- **User name:** exact name and "@name". **Domain:** mentions outside its own pages.

**Searching with Google (own key):** Without a key, TangoDown searches via DuckDuckGo. Better hits come from two official Google interfaces – enter them in the vault:

**Metasearch:** Every web search (right-click "Web search: hits into the graph", investigation automation, AI research, AI web search) queries all available sources **at the same time**: DuckDuckGo (no key), **SearXNG** (one or more instance addresses in the vault under "SearXNG (metasearch)" – the instance must allow JSON output; own or local instances are the most reliable; public ones are listed on searx.space), Brave and Google (each with your own key). Identical addresses are merged; a hit found by several search engines ranks higher, and the finding notes which search engines found it. If a source blocks (e.g. DuckDuckGo with bot protection), the others still deliver – the message names what was unreachable.

**Without a key:** Besides DuckDuckGo, every web search always also queries the free interfaces **Marginalia** (independent search index), **Wikipedia (German and English)** and **Wikidata**. If DuckDuckGo blocks, these still deliver hits; the reason is shown as a note. For broad web searches, your own keys (Google, Brave) or your own SearXNG instance remain the best addition.

- **Google Programmable Search** (entry "Google Programmable Search"): in the format **API key:search engine ID**. Key in the Google Cloud Console (enable "Custom Search API"), search engine ID (cx) at programmablesearchengine.google.com (switch on "Search the entire web"). Once stored, all web searches run via Google. Google states a small free daily quota; beyond that it costs money.
- **Google Places API** (entry "Google Places API"): finds the entry for a **phone number** or **company** as in the Google info box – name, address, website, coordinates. For phone numbers the owner is created as a company/organization and linked as **"owner according to Google Places"** (only if the number matches), the website as a domain; for companies empty fields are filled. Paid according to Google's prices.

The Google search page itself is not read out – Google's terms do not allow that. Costs and quotas are set by Google; check them in your Google account.

**DuckDuckGo has no key – and sometimes blocks:** There is nothing to store for DuckDuckGo. When DuckDuckGo sees many automated requests it sends a bot check instead of results; TangoDown then reports **"DuckDuckGo is currently blocking automated searches (bot protection)"** instead of "no hits" and offers **"🌐 Search in browser"** – this opens the same search in the built-in browser, where you search yourself (free of charge). The check is not bypassed. Automated web searches become reliable with your own key in the vault under **API keys** (not under connectors): **"Brave Search API"** (a paid plan at Brave with a monthly free credit; a payment method must be on file – prices are set by Brave) or **"Google Programmable Search"** (see above). While the search runs, "🔎 Web search running …" stays at the bottom right – also in a detached window – until it is replaced by the result: number of candidates, "nothing new" or no hits with a tip.

**Hashtag / topic – direct search:** Right-click → **"# Fetch current posts (24 h)"** or "… of the last 7 days". One click is enough: the public posts (Bluesky, Mastodon; X with credentials in the Vault) land in the graph immediately – each post on the hashtag, the **author as an account** ("authored") and a **detected place** with coordinates (also on the map). The newest 25 are taken over; each post has link, time, language and text as properties. "📣 Open in social search with map" offers more filters, live streams and web search.

**Hits attach to the element:** If a query opens another module (e.g. "Open in SOCMINT", subdomains, social search, registers), the elements you take over into the case there that are not attached to anything existing are **automatically linked to the clicked element** ("Hit: …") – for 15 minutes or until the next such query. The opened module or window comes to the front, even if it is popped out on another screen.

**Webcam elements:** Right-click → **"▶ View webcam"** opens it in "Webcams & video"; **"▣ Put on monitoring wall …"** groups the walls in a submenu – an element can be on any number of walls; "✓ already on it" shows where it already is (a click then opens the wall), a full wall (16 tiles) is reported.

**Change type:** Right-click → "◇ Change type …" (also for several selected elements) – e.g. turn a person into a topic/hashtag. Details are kept; Ctrl+Z restores the old type.

**Selecting several: Ctrl+click** adds an element to the selection (again: removes it), **Shift + drag** on an empty area draws a frame around several. **Del** deletes all selected ones (with confirmation, Ctrl+Z brings them back). **Shift+click** on an element, by contrast, connects the currently selected element to the clicked one.

**Delete and restore:** Right-click an element → "✕ Remove"; with several selected elements "✕ Delete selected (n) …". Right-clicking the empty area offers **"Delete selected"**; **"Delete all (n) …"** (in a subgraph: "Delete everything in this graph") sits inside the expandable entry **"⊘ Clear graph"** so it is not clicked by accident next to "Fit all". The **Del key** deletes the selection. There is always a **confirmation prompt** first with the number of elements and links. **Ctrl+Z** (or right-click → "↶ Undo") brings everything back – with the same identifiers, all links, properties and subgraph membership – as long as the case stays open. Deleting and restoring are recorded in the audit log.

⎘ **Copy & paste (Ctrl+C / Ctrl+V):** Select elements (click, **Ctrl+click** adds more, Shift + drag draws a frame around several), **Ctrl+C** or right-click → "⎘ Copy". Then in the target graph **Ctrl+V** (pasted at the mouse position, the arrangement is kept) or right-click on the empty area → "📋 Paste here". The links between the selected elements are copied too.

▧ **Images on elements:** When something with an image goes into the graph, the image comes along and appears as a preview in the node: snippets and photos from "Files & documents" (same file, same checksum), post images from the social deck, thumbnails of YouTube recordings and images via the browser right-click **"▧ Image into the case"**. Images from web addresses are loaded over the same network route "Browser & web capture"; every request is in the audit log, and the address stays on the element as "bild_quelle". Formats such as WebP or GIF are stored as PNG. In the **properties** the image is shown with name, size and SHA-256 – **click shows it large**, "⛓ Verify" checks the checksum. If an image is missing, **"↓ Image from source"** or **"🌐 From address"** loads it. The switch **"▧ Images: auto / off"** in the graph toolbar turns off automatic loading (images from the files still come along because they are already in the case).

- **Within the same case** (e.g. from the overall graph into a sub-graph): **no duplicates** are created – the same elements appear in the target graph.
- **Into another case:** First open the other case, then paste. Because of purpose limitation a **justification** is required (except in free mode); it is recorded in the audit log of both cases. The copies carry the source "kopiert aus Fall <file number>". If an element already exists there (same type and name), only empty fields are completed; differing values are shown via "View differences". If the elements come from a VS-NfD case and the target case is OFFEN, TangoDown asks first. Images, evidence captures and documents stay in the original case. **Ctrl+Z** undoes the paste.
- In addition, a readable list (type and name) goes to the Windows clipboard, e.g. for an email or spreadsheet.

**Typical:** Build a company's network; detect connections between accounts, domains and wallets.

## ▥ Analysis

**What for:** The case at a glance in charts: **elements per type**, **central elements** (most links – who is most strongly connected?), **timeline** per month (date from time properties such as "Date", "published", "seen", otherwise creation date), **link types**, **classification** (Admiralty) and **provenance** of the data. After a bank

statement or call data import, additionally **money flow** (largest transfers) and **communication** (most frequent contacts).

**How to use:** Clicking a bar highlights the corresponding elements in the graph. "as table" shows all values as a table (for copying, accessible).

### ⊛ Search Around (neighborhood search)

**What for:** Find the **neighborhood** starting from one or more elements – e.g. "all bank accounts this person transfers to within at most 2 steps" or "all phone numbers around this radio cell".

**How to use:** Select in the graph → right-click → **"⊛ Search Around …"**. Set: **steps** (1–3), **direction** (both, outgoing, incoming), **link contains** (e.g. "transfers", "calls") and **only types**. Every finding shows the **shortest path** as evidence. "◎ Highlight in graph", "⌬ As new graph" (keep working cleanly separated) and **"⌕ Search other cases"** (the same values across cases, read-only, in the audit log).

## Classification (Admiralty code)

Every element carries a classification such as **B2** or **C3**. This is the **Admiralty code** (also NATO system), the usual rating scheme in investigations, intelligence and OSINT. It rates two things **separately**:

| Letter: reliability of the **source** | Digit: credibility of the **information** |
|---|---|
| **A** completely reliable | **1** confirmed by other sources |
| **B** usually reliable | **2** probably true |
| **C** fairly reliable | **3** possibly true |
| **D** not usually reliable | **4** doubtful |
| **E** unreliable | **5** improbable |
| **F** cannot be judged | **6** cannot be judged |

**Examples:** Commercial register extract = **A1**; legal notice (imprint) of a company website = **B2**; account with the same username on a platform = **C3** (same name does not mean same person); AI finding or unknown tip = **F6**.

**Why TangoDown classifies cautiously:** Automatic hits deliberately get a low classification (e.g. SOCMINT hits C3, AI findings F6). Only after your check (profile picture, bio, links, second source) do you raise them. This keeps it visible in the report and in "Explain connection" how reliable a chain is – it is only as strong as its weakest link.

**Change:** in the Properties panel, the selection next to the name or **"? What does B2 mean?"** – shows both scales and sets the letter or digit with one click. Every change is recorded in the audit log and in the provenance of the properties.

### ◎ Properties

**What for:** All details of the selected entity – fields, images, notes, classification, sources, links.

**How to use:** Edit fields, attach images, use field templates per type (person: date of birth, address …). The matching queries are at the bottom.

**Provenance per property:** In the Properties panel, expand "▸ Provenance of properties" below the properties: for each property, **where the current value comes from** (creation with source, query via right-click, data import, by hand in the Properties panel …), **when** and **by whom** – clicking a row shows the **history** (earlier values, removals). This way you can show for every single value where it comes from.

**Match place and map:** Coordinates under **Geolocation** take effect after Enter or when leaving the field – map and graph follow immediately. **"◍ Locate from address/place"** looks up the entered address or place via OpenStreetMap and sets the position (with several hits, you choose). If the address or place changes, a message offers **"◍ Relocate"**; "◍ On the map" jumps to the situation map.

**View image:** In the image field, **"⤢ View large"** (or a click on the preview) shows the image at full size – without changing anything; click or Esc closes. "↻ Replace", by contrast, swaps the image.

### ⏱ Timeline

**Jump and add:** A **click** on an entry opens the capture or the element in the properties (there also "▶ Play video"). **Right-click** offers everything at once: "◈ Show in graph", "Open in properties", "▶ Play recording", "▤ Show in files", "☝ View capture", "🌐 Open address in TangoDown browser", "▦ Add to report" (with the time) and "⧉ Copy entry".

**What for:** All time data of the case chronologically on one axis.

**How to use:** Choose the kinds at the top (time data in entities, evidence captures, alerts, entry into the case, audit log). The bars show the density per day – clicking filters to that day. Time range, free-text filter and time zone are selectable. Clicking an entry opens it in the Properties panel; ⧉ copies the list.

**Typical:** Reconstruct the course of an incident; show what happened before and after an event.

**Tip:** Time data in fields such as "Time", "Recorded", "Last seen" (2026-10-28 21:40 or 28.10.2026 21:40) appear automatically.

### ≋ Matching

**What for:** Detect and merge duplicate people, accounts and elements – within the case and across cases.

### ▦ Report Builder

**Reports are saved:** Title, selected sections, format, summary and all adjustments ("Adjust items") are stored encrypted in the case – everything is back the next time you open it, also on another computer with the same case. Every exported report (PDF or Word) is additionally stored as a document in **"Files & documents"** (category "Report", same checksum as the exported file); the message after export takes you there with "▤ Show in files".

**Search the data before creating the report:** In "✎ Adjust items" the search field searches all report data – entries, all columns, headings, introductions and the summary. Part of a word is enough (e.g. "collab"). Sections with hits expand automatically, all hits are shown and highlighted in yellow, with the count next to them. This lets you find exactly what you want to change, hide or delete before export. Esc clears the search.

**Add to report – from anywhere:** What you add via right-click "▦ To report" (e.g. a browser selection as a quote with source) goes into the report's **summary**. The draft is stored encrypted in the case – even when the report builder is closed, and it is kept after closing. It appears in the preview after "Refresh preview".

**What for:** Report as PDF or Word: summary, entities, links, graph, queries and sources, evidence, AI use, audit log.

**How to use:** Choose sections, check the preview, export. The report's checksum is recorded in the audit log. Logo, header and footer in Administration.

✎ **Adjust elements:** Every entry of the report can be edited **for this report only** – the case stays unchanged. Expand a section (▸), then per row or image: ✎ change text (or double-click; each column separately), 🚫 hide (stays struck through in the list), ✕ delete for this report (below the section "↺ restore deleted"), ↺ back to original. Whole sections can likewise be hidden or deleted, heading and introduction changed. The filter field finds entries across all sections. The adjustments stay saved per case until you discard them with "↺ reset all". **Traceability:** The cover page notes "Adjusted for this report: n element(s) hidden · m detail(s) changed", and the export is recorded with these numbers in the audit log.

### ⇪ Data import

**What for:** Take tables into the case – **bank statements**, **call data** (calls/SMS) or **any lists** (e.g. contact lists, customer data, exports from other tools). Formats: CSV, TSV, TXT and Excel (.xlsx); umlauts from bank exports (Windows-1252) are read correctly.

**How it works:** "📂 Choose file" or drag the file into the module. TangoDown detects the header row and the **kind** of data and suggests the **column mapping** – everything can be changed. On the right you see a preview of the file and the **result** (how many elements of which kind, the strongest connections). "+ Add as elements" creates everything and shows it in the graph.

- **Bank statement:** booking date, amount (or separate debit/credit columns), counterparty, IBAN, payment reference. Result: **bank accounts** (IBAN checked via check digit), holder as person or company, links **"transfers to (count, total, period)"** and totals of incoming/outgoing per account. Your own account comes from a column or is entered at the top.
- **Call data:** line A and B, start, duration, type, radio cell (with coordinates), IMEI. Result: **phone numbers** (uniformly +49…), **"calls (count, total duration, period)"**, "SMS to", **radio cells as places on the map** with "connected to", IMEI on the line.
- **General list:** choose per column: **element** (with type – email, phone, IP, domain, IBAN etc. are detected), **property** of another column's element, or ignore; plus any **links per row** ("uses", "works for" …).

**Merging:** Identical elements (same type and same label) are **added to instead of created twice**, links of the same kind are updated. The file name with SHA-256 checksum is recorded as the source; the import is recorded in the audit log.

**Undo:** An import can be undone all at once in the graph with **Ctrl+Z**.

## Research

### ▶ Investigation autopilot

**What for:** A complete investigation from a single starting value – without operating each module one by one.

**Open and jump:** Rows with a domain or address have **"🌐"** (opens it – TangoDown browser or system browser). Every step row has **"↗"** – opens the matching module with its results and settings. For **Subdomains**, **"⚙ Word list & settings"** takes you straight to maintaining the subdomain names to check (word list) and the sources.

**How to use:**

1. Enter a starting value: domain, IP, email, URL, username, crypto address, license plate, VIN, phone number, name or company (with legal form, e.g. "… GmbH"). From the graph ("▶ Check all round") the kind is taken

from the element. The kind is detected (changeable on the right).
2. Enter the purpose/justification (required).
3. The workflow appears as a list – check or uncheck each step, adjust values. "☆ Remember selection" remembers which steps are ticked – they then apply automatically to every new start value of the same type (e.g. every IP address). Afterwards the button reads "★ Selection saved ▾" (remember again or delete); in the type selection, types with a saved selection are marked with ★, and the "★ N" button next to it lists all saved selections for deletion.
4. "▶ Start workflow". Each step runs through the matching module; results land in their own subgraph.
5. Follow-up steps from the results (new IPs, domains, profiles, findings) are suggested – and only run after your approval.

**Names – 🔎 Web search:** For a name, the "Web search" step searches the internet (request to DuckDuckGo; with a Brave key in the vault to Brave). Up to 10 hits go into the case as **findings** (title, address, excerpt) and are linked to the person. Capturing these pages is suggested as a follow-up step. **Important:** findings are unverified – people with the same name are common. Check yourself whether a hit concerns the person you are looking for. The search term is sent to the search service; untick the step if needed. An evaluation with a summary is done by the 🌐 **AI web search**.

1. Result: subgraph, timeline, report, summary, optional AI evaluation. **"⌬ Add to graph ..."** adds the results to an existing graph or creates a new one (the main graph contains everything anyway).

**Without a justification** nothing starts – the field is then marked red.

**Typical:** "Who is behind this domain?", "What do we know about this license plate?".

**Also by right-click:** on any entity, "Start investigation (automatic)".

### ✦ AI

**One area for all AI work on the case.** Instead of four separate modules you set just two things at the top of the "✦ AI" area:

| Switch | Choice | Meaning |
|---|---|---|
| **Source** | ▤ Case | only the data in the case – no outbound request |
| | 🌐 Internet | the AI searches the web and social media itself |
| | ▤🌐 Case + internet | the AI knows the case and additionally searches the web – to check and extend what is known |
| **Mode** | 💬 Answer | ask a question, answer with evidence from the case or with numbered sources |
| | ✧ Plan with approval | the AI plans steps with TangoDown tools, you approve each one; results go into the graph |
| | ↻ Recurring | recurring AI tasks on a schedule |

The sections below describe the parts in detail: **Case + Answer** is the AI analyst, **Internet** or **Case + internet + Answer** the AI web search, **Plan with approval** the AI research, **Recurring** the AI tasks. Switching keeps everything – conversation, running search and plan. With "Plan with approval" and "Recurring", the plan or the task itself determines where data is read from.

**Open:** rail "Research" → ✦ AI, or Ctrl+K – the former names ("AI analyst", "AI web search", "AI research", "AI tasks") also lead here, preset accordingly.

**All parts use an AI language model** – the one you set up in the AI settings (⚙ with "Case + Answer"). Where your case data goes depends on the chosen model: with a **local model** (e.g. Ollama on your computer) it does not leave the computer; with a **cloud provider** (e.g. Anthropic, OpenAI) the question and the necessary case data are sent to that provider – also with "Case + Answer" and "Case + internet". With "Case + internet" a summary of the case goes to the AI model; the search services only receive the search terms the AI derives from it. With cloud AI, "Case + internet" is blocked while redaction is switched on – the search needs real names.

### 🌐 AI web search

**What for:** The AI researches the open internet **by itself**: it searches, reads hits (e.g. legal notice, press articles, profiles), searches further in a targeted way and in the end delivers a **report with numbered sources** and a list of **findings** (people, companies, domains, accounts …).

**How to use:** Enter the task in your own words (e.g. "What is publicly known about Muster Logistik GmbH from Hamburg?"), choose tools (🔎 **Web search**, 📄 **Read pages**, 💬 **Social media** – Bluesky, Mastodon, Reddit, Lemmy, Hacker News, with a key X and YouTube –, 📰 **News** – Google News, GDELT –, 🎯 **Platforms** – TikTok, Instagram, Facebook, Telegram, LinkedIn, Threads, X, YouTube, Xing, VK, Twitch via the search engine index, i.e. publicly indexed pages without signing in), the number of steps (up to 4/8/12/16) and **"🌐 Let AI search"**. During the search you see every step live (what the AI intends, which search, which page); **"■ Cancel"** stops immediately.

**Result:** Report with clickable sources **[n]** (opens the page in the built-in browser), **findings** with a supporting quote and source, **source list** with "📥 capture" (evidence capture). Only findings with a source from this run can be added; findings without a real source are shown as "unsourced". **" + Add selected as elements"** creates a note with the report and sources and attaches the findings to it (classification F6 – check first). "▦ Add to report" copies the text into the Report Builder.

**Privacy and traceability:** The task and the search terms go to the configured AI provider and to search services (DuckDuckGo; with the key "brave" in the vault, Brave Search). **Case data is not sent.** It only starts with a justification (purpose limitation); every search and every page read is in the audit log, and the run appears in the report under "Use of AI". With local AI (Ollama), only the search queries and page fetches leave the house. Pages are fetched over the configured network route (e.g. Tor), without signing in.

### ✧ AI research

**What for:** A task in your own words ("Find everything about …"). The AI suggests a research plan, you approve, TangoDown runs only checked steps and evaluates them.

**Pre-filling modules:** The task can be a whole sentence, e.g. "Search for live webcams for the largest German cities and watch #example". Webcam requests become steps per place: the place is located on the map, and a prepared live-cam search is ready in the Webcams module. Every hashtag mentioned is set up as a watch and is ready to search in the situation picture under "# Hashtag". Webcam addresses that the AI only guesses are not pre-approved.

**Tools the AI may plan with:** Net intel (domain, IP, email), chain trace (crypto), SOCMINT (user names), web capture (save a page), situation picture watch, webcams, 🔎 **Web search** (search term; hits as findings) and 👤 **Platform profile** (a public profile on Facebook, Instagram, X, LinkedIn, YouTube, TikTok or Threads is created as an account and the page is captured). For person names the AI always plans a web search. For well-known public persons, companies and organizations it suggests their official profiles – these come from the AI's knowledge, are therefore **not ticked** and must be checked (wrong or outdated profile possible). Some platforms only show a login page without signing in; when signed in, capture in the built-in browser with "📷 Capture view".

**Reusing results:** "⌬ Add to graph …" – into an existing or new graph.

**Discarded suggestions:** Targets that do not come from your data points or the case (e.g. a website guessed by the AI) are discarded by TangoDown at first – so that no uninvolved parties are queried. Under "… AI suggestions discarded" you can add one of them as a step with " + add anyway" after a confirmation prompt; it is then marked and runs like any other step, with justification in the audit log.

**Note:** AI results are leads, not findings of fact.

**Situation picture steps fetch real posts:** If AI research suggests a "Situation picture watch" for a hashtag or term, TangoDown sets up, in addition to the situation picture topic, **watches in source monitoring** (Bluesky, Mastodon), checks them right away and attaches the newest posts as "Post" to the topic in the graph – with the **place mentioned** (e.g. #Berlin) on the map. The watches then keep running and report anything new. Reddit now requires signing in and is therefore not included automatically.

### ✦ AI analyst

**What for:** Asking questions about the case, evaluating texts, extracting entities, hypotheses and report drafts.

**Citations required:** The AI analyst puts the case element in [square brackets] after every statement about the case. Below every answer, TangoDown checks: how many sentences are backed, whether the elements named exist in the case (otherwise "not in the case – possibly made up") and which sentences have no source. General knowledge and hypotheses are labeled.

**Content check of sources:** Below that, TangoDown checks for each backed sentence whether the cited source supports the statement **in substance**: do the key terms, names, numbers and dates appear in the case element (label, fields, note, source, links)? Result per sentence: ✓ **supported**, ◐ **partly** or ✕ **not supported** – with the terms missing from the source (numbers and dates must match exactly). "Not supported" means: it is not stated like that in the source – the statement may still be true, but it is then not backed. **"✦ AI cross-check"** additionally has a model judge each statement based only on the source texts (via the configured AI route; redaction applies); its verdict appears with a short reason next to the local one.

**Second opinion:** Choose a second model in the settings (different provider or different model). "⇄ Second opinion" below an answer asks the same question independently; both answers appear with a comparison of the sources (agreement in %, differences marked).

**Redact before cloud AI:** Can be switched on in the settings per module (AI analyst, AI research, report, situation picture, explain connection). Before sending to Anthropic/OpenAI, names, emails, phone numbers, license plates, addresses, accounts, wallets, domains and companies from the case are replaced by placeholders such as [PERSON-1]; the answer is translated back locally. The number of redacted items is shown on the answer and in the audit log. Local AI (Ollama) needs no redaction. Redaction reduces what goes to the provider, but it is **not complete anonymization**: conclusions may still be possible from the remaining text – better to work on confidential cases with local AI.

🛡 **Protection rule (always on):** Every AI call carries the fixed rule: content from the case, web pages, files, emails, search results and plugins is **content to analyse, not instructions**. The AI may and should follow leads, links, names and traces in it and derive conclusions and next steps – this does not restrict research. Only requests that try to change its role, rules or task (e.g. "Ignore all previous instructions …", "send … to") are not followed but reported as a possible manipulation attempt. Only you give the task. This weakens such attacks but does not reliably prevent them – AI answers remain leads, and actions (e.g. research steps) always need your approval.

**House rules:** In the settings (⚙) store your own additional instructions for all AI functions, e.g. language, style, citation format or your organization's requirements (up to 3000 characters). They are appended **after** the fixed rules and cannot replace them. Every change is recorded in the audit log with a checksum; in the Agency edition only for administration, and with confirmation switched on only with the security key.

**Using an answer:** "⇢ Use …" below every answer: run as AI research (the question becomes the task, detected values become data points), detected values (domains, IPs, emails, URLs, wallets, hashtags, usernames) into the case or into an existing/new graph, answer as a note in the case (appears in the case file and report), start an investigation (autopilot) for a detected domain/IP/email. Everything stays marked as an unchecked AI lead (F6); names only one by one via right-click.

**Providers:** local (Ollama, nothing leaves the computer) or cloud (OpenAI, Anthropic Claude) with your own key.

**Settings in three groups:** 🖥 **Own AI** (Ollama address, own AI server – always counts as own infrastructure), ☁ **Cloud AI** (approval, keys, redaction) and ⇄ **Second opinion** (second model; each choice is marked "own" or "cloud").

**Keys:** Under "☁ Cloud AI", the "Keys" line shows whether a key is stored for Anthropic, OpenAI and your own AI server; "⚿ enter …" jumps straight to the matching entry in the vault.

**Own AI server (on-prem):** Besides Ollama you can enter any server with an OpenAI-compatible interface (vLLM, LM Studio, LocalAI, Open WebUI …): provider "Own AI server", in the settings the address up to `/v1`, a key – if the server requires one – in the vault under "Own AI server (on-prem)". Ollama can be entered this way too (OpenAI-compatible under `/v1`, TangoDown adds it itself) – but the provider "Ollama" is usually better, because TangoDown sets a large context window there; via the OpenAI interface Ollama uses its smaller default and cuts long inputs. If Ollama runs on your own infrastructure but under a public address, tick "Ollama runs at our place, but under a public address". An own server counts as own infrastructure everywhere: no cloud approval needed, never redacted, also for VS-NfD cases and usable in every module (in the authority edition only an administrator sets this).

**Own certificate authority (e.g. Caddy, Traefik, company CA):** If your own AI reports "certificate is not recognised", TangoDown shows the issuer and SHA-256 fingerprint. "📄 Load root certificate …" (recommended) takes the CA's `root.crt` – TangoDown then checks every connection to your own AI against this CA itself (chain, name, validity), even when the server certificate is renewed automatically. "✓ Trust this certificate" pins only exactly this server certificate (compare the fingerprint with the server first). Both work for any address you enter (name or IP), apply only to your own AI – not to the browser, research or Windows – and can be removed again under "Trusted" with ✕.

⚙ **Expert settings** (AI analyst → settings, collapsed): context window (Ollama), max. answer length, temperature, time limit per request, max. input length and extra parameters (JSON) for your own server. Empty = default; "↺ All to default" resets. Typical cases: the answer stops with "answer length reached" → increase the answer length; long cases get cut off → increase context window and input length (roughly 1 token ≈ 4 characters); a slow server hangs → set a time limit.

**Redaction** only affects cloud AI and is off by default – otherwise the AI lacks exactly the details that matter. Turn it on only where data must not leave the organisation in plain text.

## ✦ AI second opinion in modules

**What for:** Have your AI server cross-read tool results – as a second view, not a replacement. The AI names inconsistencies, gaps and assessments; it can be wrong, so check every note yourself.

**Where:** Company search (analyse website), e-mail analysis, PCAP and log analysis, Shodan, Chain-Trace, SOCMINT (usernames), name variants, file forensics, domain tools, subdomains and vehicle matching – each with the **"✦ AI second opinion"** button at the result. Cyber intelligence has its own AI assessment.

**How it works:**

1. Click "✦ AI second opinion": TangoDown shows **which server** receives the request (🖥 own server, e.g. Ollama, or ☁ cloud AI) and **which data** – only this module's result, without the rest of the case.
2. "Send and check". Cloud AI only if allowed (AI analyst → settings); for VS-NfD cases only local. If "redact before cloud AI" is on for "AI second opinion in modules", names and identifiers from the case are replaced first. If a second model is set up, you can use it instead.
3. The answer appears next to your result: **confirmed**, **differs**, **addition**, **note** – each with confidence (high/medium/low) – plus what you should check yourself. Nothing is overwritten. In the company search, suggested values (e.g. company, register number) can be ticked and applied.

Every second opinion is recorded in the audit log (server, model, checksum). Copy passes it on as text.

### ⟲ AI tasks (recurring)

**What for:** Have the AI check something regularly and report **only when there is something new** – e.g. **"Report when a new balance sheet of Muster GmbH appears in the company register"**, "Report changes to management or registered office", "Report when the legal notice changes" or "Report posts from monitoring that name a specific threat".

**Setting up:** "+ New" (or choose a template) → **What should be reported?** → **Source**: a web page (register extract, announcements, legal notice …), the hits of a watch from source monitoring, or the case data → interval (from 30 minutes, default daily) → purpose → Save.

**The three sources in detail:**

- **Website (changes):** TangoDown loads the given page as text (no images) at every interval, compares it with the last state and only asks the AI when it changed – with the difference.
- **Hits from source monitoring:** the new hits of the watches you created in the 📡 **Source monitoring** area (e.g. keyword/hashtag on Bluesky or Mastodon, an account, an RSS feed, a web search) – one specific watch or all. The AI only reads what was added since the last run. If there is no watch yet, the link below the selection takes you there.
- **Case data (on changes):** the whole case as it is in the graph – all elements with their details and notes and all links. The AI is asked as soon as something in the case changes (new entry in the case log); no outgoing query.

**Switches:** "Alarm on report" (bell, Windows notification, webhooks), "Second model instead of main model" (the second model set in the AI analyst, e.g. a cheap local one), "active" (off = task paused).

**How it works:** The first run saves the **initial situation** and has the AI describe it once (one AI request, without an alert). After that TangoDown reads the source **itself** at every interval and compares it with the last state – the AI is not asked for this. **Only when the source has changed** is a request sent to the AI; if the source is unchanged there is no AI request and no report.

**Costs:** Every AI request – the first one, each one after a change and every "⟳ Run now" – costs money with a cloud provider like any other request (at its prices); with a local model (Ollama) there are no provider costs. If a source changes often (e.g. pages with changing ads or clocks, or the "case data" source, where every change in

the case counts), correspondingly many requests arise – then choose a longer interval. How often the AI was asked is shown in the task's history. The AI gets the changes ("+ new line", "− removed line") and must name a **verbatim supporting passage** from the source; without one, a report does not count.

**Results:** per run "Message", "nothing wanted" or "Initial situation" with summary, supporting passages, model and checksum; "▦ Add to report" and "⧉ copy". A report triggers an **alert** (bell, Windows notification, outgoing webhooks for alerts).

**Limits:** Cloud AI only if approved in the AI analyst; "Redact before cloud AI" also exists per module for "AI tasks"; VS-NfD (German classified – restricted) cases only with local AI. Tasks only run while the case is open, over the "SOCMINT" network route; in the Agency edition the order needs the data categories "ki" (and "web" for web pages). A blocked task pauses itself. Every report is a **lead, not a finding of fact**.

### ⌖ Net intel

**What for:** IP, domain, email or URL: DNS, Whois/RDAP, location, ASN, hoster, reverse DNS, VPN/proxy/Tor detection.

**How to use:** Enter a value, Enter. Add results to the case with a click. Each source with status and response time.

**IP location as a place:** "IP2Geo" records country, region, city, provider and accuracy as properties on the IP and sets its geo position. In addition it creates the city as a **place element** (e.g. "Sampletown, Region, DE"), linked with **"Location (estimated, ~25 km)"** – identical cities become one element. This shows in the graph when several IPs, mails or accounts point to the same place. The place is an estimate based on the IP address, not a confirmed address; this is also noted on the place.

**Open ports & services (Shodan):** For every IPv4 (including the IPs of a domain), Net intel shows open ports, detected software, tags (e.g. "cloud", "vpn") and known vulnerabilities (CVE). Without a key via the free Shodan InternetDB; with a Shodan key (Vault & connectors → Shodan) via the full host query with software versions, operating system and data date. Also by right-clicking an IP or domain → "Open ports & services", in "All network transforms", in the Investigation autopilot and in AI research. The values are stored as properties on the IP (open ports, services, known vulnerabilities); hostnames are linked as domains. This is data from Shodan's internet scans – not your own check of the system; vulnerabilities are derived from versions and not confirmed.

**Shodan search (with key):** Right-click a company, organization or hoster → "Shodan: systems of the organization", a domain → "Shodan: systems of the domain" (incl. subdomains). Systems found come into the case as IP elements with ports, software, vulnerabilities and **location** – they appear in the graph and, with location, on the geo map ("◍ On the map" jumps there). The search uses query credits of your Shodan account (search filters need a paid plan).

### ⌘ Subdomains

**What for:** Which subdomains does a domain have (e.g. vpn., dev., intranet.) – and which of them are reachable or orphaned?

**How to use:** Enter a domain – or right-click a domain in the graph → **"Find subdomains"**. Choose sources, **"⌘ Find subdomains"** → TangoDown shows which services will receive the domain → **"✓ Approve and search"** (in the audit log).

**Passive (green):** certificate logs (crt.sh), HackerTarget, AlienVault OTX, Anubis, urlscan.io, Shodan DNS (own key, uses query credits), SecurityTrails (own key) – public databases; the target domain notices nothing.

**Active (orange, only with a mandate/authorization): "Check word list"** tries common names via DNS; **"Check web servers"** contacts the names found (status, page title). TangoDown detects wildcard DNS ("*.domain") and filters out false hits.

**Word list: "✎ Word list"** – add or delete names (one name per line, without the domain), **"⇩ Add from file"**, **"⇪ Export"**, **"↺ Default"** restores the bundled list.

**Result:** per subdomain IP addresses or CNAME, source(s), optional web server response; filters **Resolves / No resolution / ⚠ Possible takeover** (CNAME points to a service such as GitHub Pages, Azure or S3, but the target no longer exists there – a hint, not proof). **"→ To graph"** attaches the active subdomains (at most 40 at once) to the domain, **"⌖"** checks a name in Net intel. In the Investigation autopilot there is the optional step "Subdomains (passive)"; in the report the searches are listed under "Queries and sources".

**Open:** Clicking a name found or **"↗"** in the row opens the page (https) – either in the TangoDown browser or in the system browser (or copy the link); "⌖" checks the name in Net intel.

**Progress:** During the search a box below the sources shows per source "running" (spinner), "✓ done" with count or "⚠" with reason, plus the names found so far, the elapsed time and a counter for the word list or checking.

### 🛡 Domain tools

**What for:** What is behind a domain or IP – and which other sites is it connected to?

**In the graph (like a transform):** Right-click a domain or IP → expand the **"Domain tools"** section → choose a tool or **"▶ Run all in this section"**. The findings appear as new elements **around the element you clicked**, linked to it and briefly highlighted; the view brings them into the picture. From each new element you can continue via right-click – this way you uncover the surroundings step by step. Check results without new elements (spoofing protection, archive, blocklists) are stored as properties on the element; "Details" in the message opens the detailed view. Undo works as with any transform. **Also on email addresses** (spoofing protection, lookalikes and blocklists of the sender domain) and on elements with a web address (technology, tracking IDs, certificate, archive of the page).

**The tools:**

- **≈ Lookalike domains:** typo, character and ending variants (e.g. for beispielbank.example: beispie1bank.example, beispielbank.example with a Cyrillic a). Only registered variants are shown; marked with mail server = usable for phishing mails. New domains with the link "Lookalike".
- **◎ Tracking IDs:** Google Analytics, Tag Manager, AdSense, Meta Pixel & co. from the home page. If the website sends a **bot check** instead of its content, TangoDown reports this (not "no IDs") and offers "🌐 Open in browser" – there **"⛏ Findings"** reads the tracking IDs from the displayed page. The check is not bypassed. The same ID on two sites = very likely the same operator. Each ID becomes its own element; right-click it → **"Search tracking ID in all cases"** or **"Other websites with this ID (web)"**.
- **⇄ Reverse IP:** which other domains are on the same IP (link "same IP"). A **domain** works instead of an IP: TangoDown first determines its IPv4 address and uses the first one (others are listed); in the graph the IP sits between the domain and the hits. With large hosters these are often thousands of unrelated sites – then the conclusion is weak.
- **⏳ DNS history:** which IPs the domain used to be on, with time period. Sources: **AlienVault OTX** and **VirusTotal** (each with a free key) and **SecurityTrails** (with an account) – all in the vault. OTX no longer allows

anonymous queries; without a key a note appears instead of just "no history", with "⚿ Open vault". Below the result you see which sources were asked.

- ✉ **Spoofing protection:** SPF, DMARC, MTA-STS, BIMI and common DKIM selectors with a rating of **protected / harder / spoofable** – can mails be forged in the domain's name?
- 🔒 **TLS certificate:** issuer, validity and all other names in the certificate (linked as domains with "same certificate"). Needs a direct connection; blocked in tunnel/proxy mode because the server would otherwise see your own IP – then use the certificate logs in the subdomain finder.
- ⚙ **Web technology & favicon hash:** CMS, server, libraries; the favicon hash becomes its own element with a link to the Shodan search for sites with the same icon (often copies of a scam site).
- **Archive timeline:** since when the Internet Archive has known the page and how often it was saved – as bars per year, with links to archive copies.
- ⛔ **Blocklists:** Spamhaus, SpamCop, Barracuda (IP) or Spamhaus DBL and SURBL (domain).

**Module:** Everything is also collected in the "Domain tools" module (search: "Domain-Werkzeuge"): choose a tool, enter a value, **Verify**; **" + Add as element"** adds the result just like the right-click. **Console:** `dt <werkzeug> <domain|ip> [--graph]`, e.g. `dt mailsec example.org`.

**Traceable:** Every query goes over the configured network route, may need a justification like all network queries, is stored in the case with SHA-256 and is in the audit log. Statements are leads from public data, not proof of guilt.

### ◎ Cyber intelligence

**What for:** Check an IP or domain against several threat intel / OSINT services at the same time and compare the results – passively, TangoDown scans nothing itself, it only reads what the services have already recorded.

**Sources:** Shodan (without a key the free InternetDB, with your own Shodan key the full host API: services with versions, organization, operating system, data timestamp), GreyNoise (scanner/noise detection), AbuseIPDB (abuse reports), VirusTotal (reputation), urlscan.io (website scans), Netlas (hosts/services/certificates), Censys (hosts/services), **AlienVault OTX** (threat pulses), **Criminal IP** (risk rating of IPs), **ONYPHE** (services, blocklists), **LeakIX** (open databases, misconfigurations), **ThreatFox** and **URLhaus** from abuse.ch (malware indicators and URLs, one shared auth key "abusech"). Each source has its own key under "Vault & connectors"; individual sources can be switched on/off. A 🔑 on a source means: no key stored yet.

**Free without a key: RDAP** (registration of the domain or network owner of the IP: registrar, registration and expiry date, name servers, abuse contact), **RIPEstat** (prefix, ASN with operator, abuse contact – worldwide), **Tor relay** (the Tor Project's Onionoo: is the IP a Tor relay or exit node?), **crt.sh** (certificates and the names/subdomains in them), plus Shodan InternetDB and urlscan.io (search). These sources are marked "· free". For a **domain**, TangoDown queries the IP sources with the resolved IPv4 address (marked "via IP …"). ✦ **AI assessment** evaluates the result (overview, anomalies, exculpatory points, next steps, every statement with a source [Q1] …) – only the target and source results go to the AI provider, no case data; the result is a hint and can be added to the report.

**Saving quotas:** Results are **cached for 24 hours** (the source then shows "from cache"); "query fresh" bypasses that. The number on the source shows today's queries, the tooltip the free quota according to the provider.

**Workflow:** Enter IP/domain → "◎ Query". At the top the combined assessment (ASN, country, open ports, abuse reports, risk, "Internet scanners", "common service"), below it one card per source with summary and fields. **Contradictions** between sources (e.g. different ASN/country) are marked. " + Add as element" creates the target with the combined details (or adds to it), attaches one rating per source as a note and links any **CVEs** found as vulnerability elements. Also by right-clicking an IP or domain.

**Important:** A scanner hint, an abuse report or a reported vulnerability is a **lead, not proof** of a compromise. Mind the services' free quotas (e.g. GreyNoise Community, VirusTotal 500/day – non-commercial).

### ⊞ Shodan

**What for:** Passive query of Shodan's scan database – TangoDown sends nothing to the target systems, it only reads what Shodan has already scanned. For attack surfaces, open services and vulnerabilities.

**Query types:** Search (free Shodan filters, also via the "Organization/Domain/Network/Product/CVE" picker), Statistics (count + top lists only, uses no credits), Host (all banners/ports/certificates of an IP), DNS (resolve/reverse), CVE (vulnerability details from Shodan's CVEDB – no key), Ports.

**Adding:** "→ Systems into case" creates one IP per hit with ports, software, location (→ geo map) and hostnames; "→ incl. CVEs" additionally adds the vulnerabilities as their own **CVE elements**. In the CVE search, each CVE individually " + Add as element". Facets of the statistics are clickable (they become a search).

**Key:** Search and statistics need a Shodan key with a suitable plan (Vault → Shodan); CVE details and the simple IP query (Net intel) work without. Also by right-clicking a company/domain → "Shodan: systems of the …".

### 🚀 OSINT tools

**What for:** A curated collection of freely accessible OSINT web services (search, people, email, domain/DNS, vulnerabilities/CVE, image/geo, air, sea and rail traffic, social, Twitch, fact checking and AI detection, files/malware by checksum only, companies and registers, finance and sanctions, tools such as CyberChef and translators, genealogy, crypto, tool collections) plus your own favorites. Services that upload data or images are marked in the note.

**How to use:** Enter a search value at the top – services with "⌕" put it straight into their search. A click opens the service in the **built-in browser** (session in memory only, network route "Browser & web capture"). Right-click: open externally, copy address, add to favorites. **Your own links** via " + Link" (name, address, category; write `{q}` in the address where the search value goes) – they stay on this computer and can be changed or removed at any time. **External tools via right-click:** In the graph, right-clicking an element offers the section **"↗ External tools (opens website)"** – matching the type: for places with coordinates Google Earth, OpenStreetMap, Mapillary, KartaView, Copernicus, Yandex, Wikimapia, SunCalc, ShadowMap, PeakFinder, FIRMS and OpenRailwayMap; for domains Netcraft, host.io, BuiltWith, whoxy, urlscan, VirusTotal, Wayback; for IPs IP2Proxy, AbuseIPDB, ZoomEye, Censys; for phone numbers reverse lookup; for emails HIBP and IntelX; for usernames WhatsMyName, IDCrawl, Steam, Twitch statistics; for persons and companies WebMii, Forebears, OpenCorporates, Companies House, OpenSanctions; for CVEs NVD and Exploit-DB; for photos with an image address the reverse image search (Google Lens, Yandex, TinEye, Bing – with a prompt first, because the service fetches the image itself). These entries only open the website with the value in the built-in browser; TangoDown does not query anything itself. **Check IBAN:** for bank accounts, "€ Check IBAN (checksum, local)" checks the check digits on this computer and records the result on the element – a valid checksum says nothing about whether the account exists.

**Two fields:** on the left **"⌕ Search term for ⌕ links"** – inserted into services with ⌕ when opening (these are then highlighted), it does not filter; on the right **"⧩ Filter services"** – shows only matching services (name, address, description).

**Open in …:** selectable at the top right: **TangoDown browser**, **system browser** or **Tor Browser**; also individually via right-click on a link.

**Own tabs:** " + Tab" creates a named tab (e.g. "Persons", "Company Example"). Links go in via right-click "Into tab …" or by **dragging onto the tab**; inside the tab, re-order by dragging, remove via right-click or move to another tab. Right-click on the tab: rename, move left/right, create copy, **open all links**, delete. Tabs stay saved on this computer; the last open tab is there again next time.

**External links:** The linked pages belong to third parties. Their operators alone are responsible for their content, availability and handling of data – TangoDown accepts no liability for them and does not adopt their content. Whatever you enter there goes to the respective provider.

## ₿ Chain-Trace

⇄ **Chain switch via bridges:** Known bridges and routers on Ethereum are labeled, e.g. Optimism, Base, Arbitrum, Polygon, Across, Stargate, Hop, Wormhole, zkSync, Synapse, Celer and the THORChain router. If the address has dealt with one of them, the trace shows the **"⇄ Chain switch via bridges"** block with buttons such as **"⛓ Optimism"**: they follow the same address on the target chain, because with Ethereum-like chains many use the same address on both sides. Swaps via THORChain, such as BTC → ETH, are shown in the "Currency switch" block. Labels are leads, not findings of fact.

**What for:** Tracing crypto addresses and transactions (Bitcoin, Ethereum/EVM, Tron, Solana, XRP, Litecoin, Dogecoin, Bitcoin Cash): counterparties, flow of money, swaps across chains, sanctions lists.

**How to use:** Enter an address; flow view, plain-language explanation, add to the graph. For Bitcoin addresses, **" 🔎 Bitcoin Discovery"** leads to the search for public match locations.

**Lines in the flow view:** A line combines all payments between two addresses (amount = sum, with several it shows "· N Tx"). **Click on the line** lists each transaction individually with date, amount and fee; clicking one offers "Trace transaction", "Open in explorer" and copying. Note: in the transaction list of the details view, the amount of an outgoing payment is shown **including the network fee** (balance change of the address); wallets such as Exodus show amount and fee separately.

**Reset view:** ↺ (next to ◎ at the top left of the flow view) clears the highlight, hides the "traced" marks of earlier queries and shows the focus centred at 100 % – like the first visit; the queries themselves stay in the history. A click on an empty spot in the diagram and **Esc** do the same; hidden marks stay hidden in the case, only addresses you trace afterwards are marked. With several currencies, "Simply explained" shows a table (in/out per currency).

**"Simply explained" and transaction list:** newest first (in the explanation switchable to "oldest first"). A **click on an entry** marks the transaction: in the flow view its lines light up (the others fade) and the view jumps there; in the details view it is opened in the transaction list and scrolled to. Clicking again removes the marking.

## 🔎 Bitcoin Discovery 🧪

**What for:** Finding out **where** a Bitcoin address is mentioned publicly – in forums, on GitHub, on websites and donation pages, in archives – and which accounts mention it. From this come **possible identities**, never an "owner".

**Important:** A match location only shows that the address appears there. It does not prove who controls the wallet. A label (e.g. "Exchange X") is not a confirmed identity, and a payment to a service is not proof of identity. TangoDown therefore phrases it like this, for example: "The Bitcoin address is mentioned on the public GitHub profile XY. Control of the wallet by the profile owner has not been proven."

**How to use:**

1. Enter the address – or take it from Chain-Trace, the website analysis ("Contact" tab) or by right-clicking a Bitcoin address in the graph.
2. **Choose sources** (Hacker News, GitHub, Reddit, Brave Search, WalletExplorer, Arkham, Internet Archive, the case's Chain-Trace). Sources with 🔑 need your own key in the vault (`github` optional for code search, `brave`, `arkham`).
3. **"🔎 Find occurrences"** → TangoDown shows which services will receive the address → **"✓ Approve and search"**. Without approval nothing goes out; every search is in the audit log.

⌕ **Search the web (no key):** Below the sources there are buttons for **DuckDuckGo, Startpage, Bing, Google** and **Forums** (Bitcointalk and Reddit via DuckDuckGo). A click searches the **exact address in quotation marks** and opens the results page in the **built-in browser** – over the network route "Browser & web capture" (Tor/proxy, if set). The first time per address TangoDown asks for approval; every search is in the audit log. In the results you add hits with **"⛏ Findings"** or capture pages with **"☝ Capture page"**. Good to know: over Tor, Google often shows a check ("I'm not a robot") – then use DuckDuckGo, Startpage or Bing. Search engines do not find everything; missing hits say nothing about the owner.

**Result in six sections:** Public match locations · Possible identities · Organizations & services · Wallet labels · Cross-references (other addresses in the same text) · Sources & evidence (which source ran, which failed, checksum).

**Per possible identity:** name/account, profile link, where the address was found, why a connection is suspected (**self-declared** / **mentioned by third parties** / **technical assumption**), evidence **for and against** (e.g. several accounts name the same address as their own, warnings such as "scam") and a **review status** (unchecked, plausible, doubtful, rejected, manually confirmed – every change is in the audit log).

**Continuing:** "→ To graph" creates the account as a possible identity (classification F6 = cannot be judged; after "manually confirmed" C3) and links it to the address. "@ Check in SOCMINT" searches for the same username on other platforms, "☝ Capture finding" captures the page as evidence, "✦ To AI analyst" has it evaluated (the AI names leads, not an identity as fact), "▦ Add to report" – the report also has the section **"Bitcoin Discovery / Identity OSINT"**. In the Investigation autopilot, Bitcoin Discovery is an **optional step** (off by default).

**Exact hits only:** Only exactly this address counts – truncated or similar addresses are discarded, duplicate match locations are merged.

## @ SOCMINT

Ⓝ **Name variants (NAMINT):** Right-click a person → "Name variants (NAMINT)" (or module overview, Ctrl+K, in the browser under ⋯). From first, middle and last name (optionally a number such as the year of birth and own email domains) you get spellings, username patterns (f.lastname, firstname_l …, umlauts as "ae" and "a") and email candidates at common providers – **all locally**. Selections can be added as elements (marked "derived, unverified", linked to the person). Nothing goes out until you click: **"🖼 Check avatars"** asks Gravatar (only the checksum of the address) and GitHub, **"@ Check in SOCMINT"** checks a name on many platforms, the **search links** open in the TangoDown browser. Idea after NAMINT (seintpl, MIT licence), rewritten.

**Account IDs (name ↔ fixed ID):** Usernames change, an account's ID stays. Right-click a username or an account → section "Account IDs": **GitHub** and **Reddit** without a key, **YouTube**, **Twitch**, **VK** with a free key in the vault, **Discord** (ID → name with a bot token; without a token at least the creation time from the ID), **Telegram** (channels/groups with a bot token), **X** (ID → profile link and creation time from the ID). If the value is a number, the current name is looked up instead. The result is stored on the element: konto_id, current name, display name, creation date, when and how it was determined; if the name differs, TangoDown points out a possible

rename. For **TikTok, Instagram, Facebook, X, YouTube, GitHub, VK**, **"⛏ Findings"** in the browser reads the ID from the profile page currently displayed (e.g. TikTok profile data, X profile banner) – only what the page itself delivers, also in the signed-in platform session.

**+ WhatsMyName:** Below the search field you can additionally switch on the check rules of **WhatsMyName** (about 600 more sites; data: WhatsMyName, WebBreacher and contributors, CC BY-SA 4.0). Sites with bot protection or login requirement are left out. **"⇩ Load WhatsMyName" or "⟳ Update data"** fetches the current rules from GitHub at any time (via the network route); the date of the data is shown next to it.

**What for:** Checking usernames on public profile pages – without signing in, with a counter-check against false hits – and uncovering companies via their own website.

**Two tabs:**

- **@ Person / username:** Check a username (or first and last name → variants) on more than 40 platforms (including Reddit, Hacker News, Lemmy, Mastodon on several – including German – servers, Bluesky, TikTok, Instagram, X, Telegram, YouTube, Twitch, LinkedIn, Xing). The same name does not mean the same person: hits start with C3. For people with the same name, use the name search per platform. If you type in a company name, TangoDown offers to switch to "Company / website".
  - **Unclear, or checked manually yourself?** For entries "unclear" or "manual", look at the profile with "↗ open" and, if it matches, **"✓ confirm as hit"** – the entry then counts as a hit ("HIT ✓") and is added with "→ Add hits to graph" with the remark "manually confirmed (profile checked personally)". "↺ undo" removes the confirmation (anything already added stays in the case).
- ▣ **Company / website:** Enter the company name and website (if the website is missing, TangoDown suggests one from the case or from the name) → "🕸 Analyze website". The crawler reads public pages of the website at a throttled rate (legal notice, contact, about us, team, careers first), respects robots.txt, does not follow outside redirects and does not fill in forms. If the website builds its content only via JavaScript (a pure web app), TangoDown renders the pages in a hidden, isolated browser window (same network route, no downloads, no pop-ups) and analyses the finished content – the result line then says so. Result in sub-tabs:
  - ◎ **Linked profiles** – social media profiles that the website itself links to (LinkedIn, Xing, Facebook, Instagram, X, YouTube, TikTok, kununu, GitHub, Bluesky, Mastodon …). These are official profiles and are added with B2; per profile open, capture or check the username everywhere.
  - **§ Legal notice** – company with legal form, management/representation, registry court and number, VAT ID, address, with source page.
  - 🖂 **Contacts** – email addresses, phone numbers and linked outside domains, each with the page where they were found.
  - ⌕ **Company sites & variants** – short forms of the company name (e.g. "beispielsoftwaregmbh", "beispiel-software-gmbh", "beispielgmbh"): check as a username or open as a company page on LinkedIn, Xing, kununu, Facebook, Instagram, X, YouTube, TikTok, GitHub; plus searches in the commercial and company register, at North Data, Indeed and a web search across all profiles.
  - 🕸 **Pages** – all pages visited, with status.

" + Add as element" creates the company, domain, profiles, management people, address, emails and phone numbers, linked; "⌬ To graph …" adds everything to an existing or new graph. Every analysis is in the audit log with a checksum and can be found again via the universal search.

**Note:** Many platforms only show company pages when signed in – then use the **Platform accounts** (next section).

### ⚇ Platform accounts (signed-in research)

**What for:** Research on platforms that show hardly anything without signing in (Instagram, X/Twitter, Facebook, TikTok, LinkedIn, Telegram Web). Each platform has its **own, persistent** browser session: sign in once, then research in the **browser** in this signed-in session. The module is only there for **signing in**.

**How to use:** Module **"⚇ Platform accounts"**. Per platform "↗ Sign in" (opens the login page in its persistent session) – after logging in, the sign-in is kept; the status shows "✓ signed in" – for TikTok with the **username the platform reports for the sign-in** ("✓ signed in as @name"; TangoDown asks the signed-in session, nothing is guessed). Then: **"🌐 Open in browser"** (home page in the built-in browser, tab with 🔑), **"◆ My profile"** (TikTok: your own profile with the name read), **"↗ Login window"** (e.g. to switch accounts) and **"Sign out"** (deletes the platform's cookies and session). Other people's profiles, hashtags and searches you simply open in the browser – in a 🔑 tab you see them signed in.

🔐 **Store credentials (all platforms):** Per platform "🔐 Store credentials" – username (or email/phone) and password are stored **encrypted in the vault** and never get back into the interface. When you open the sign-in ("↗ Sign in (fills in)") or the platform asks for a new sign-in in the login window, TangoDown enters the data **only on the platform's own sign-in page** (even if the page asks for username and password one after the other). You confirm submitting, the captcha and the two-factor code yourself. Storing, changing and removing are in the audit log. Note: platform passwords in the vault are an additional risk if someone gets access to your vault – protect the vault and data folder well (master password, security key).

**Why you sometimes have to sign in again:** TangoDown does not store a password but – like a browser – the **sign-in session** (cookies). It is saved immediately after signing in, every minute and on exit. You still have to sign in again when the platform ends the session itself: after some time, with a new IP address (different network, VPN, proxy), on suspicion of automation or when you sign out on another device. Portable: the session is in the data folder and is bound to this PC (Windows protection) – sign in again once on another PC.

**Deliberate exception:** These sessions run **directly** (not over Tor) and **keep cookies** – unlike the ephemeral research browser. Reason: signed-in accounts are usually blocked or hit with captchas over Tor. Credentials are managed by the respective platform; TangoDown only stores the cookies protected by the operating system. In air-gap mode the accounts are blocked. Every opening/sign-out is in the audit log of the open case. **Only lawful, open research** – do not bypass access restrictions.

**Instagram & co.:** This makes Instagram profiles, hashtags and search researchable while signed in. For **videos/reels**, video evidence capture (browser "🎞 Video" or Video center) uses yt-dlp; **automatic** hashtag tracking/alerts only exist for open sources (Mastodon, news), not for Instagram/X/TikTok/Facebook – watch these here manually in the signed-in session.

### ⌕ Browser

**Separate session per case:** The cookies, logins and history of a case are kept apart from all other cases, and only in memory. That way, research in case A leaves no traces that could stand out in case B. When you switch cases, the tabs reload in the session of the new case. Logged-in platform accounts (🔑) stay separate, persistent sessions as usual.

**What for:** View web pages without leaving the app.

**How to use:** Enter an address or a search term (DuckDuckGo). "📸 Capture page" adds the page currently shown as an evidence item (image, content, checksums); "◆ Domain" adds the domain to the case; 🧹 clears cookies, storage and cache.

**Convenience:** Multiple tabs (Ctrl+T, middle mouse button closes), **mute sound per tab** (🔊/🔇 on the tab as soon as it plays sound, or in the toolbar or Ctrl+M – applies to this tab only), bookmarks (Ctrl+D), **View source** (Ctrl+U, with search and copy), find in page (Ctrl+F), zoom (Ctrl +/−/0), developer tools (F12), switch user agent (desktop/mobile – mobile pages often show more without login), optionally open links from TangoDown here instead of in the system browser (always here in tunnel mode). All via "⋯".

**Protection:** Own session in memory only – nothing is saved after you quit. The browser follows the network route "Browser & web capture" – the same route as for page capture, so a capture shows what you saw (tunnel, kill switch, air gap). Device permissions (camera, microphone, location) are blocked, pop-ups open in the same window. Every page visit is recorded in the log of the open case. If the browser runs over Tor, 🔄 next to the network route button ("Tor") requests a new Tor identity (new visible IP) and reloads the page – also in the menu of the route button. There, under **" 🌍 Choose exit country ..."**, you pick by flag which country the connection exits from (or "Automatic", "EU countries"); this applies until restart, permanently and with exclusions under "Connection & cover".

🧅 **.onion addresses (Tor services):** .onion pages can only be reached over Tor.

- **Browser runs over Tor** (Connection & Cover set to "Tor", exit confirmed as Tor): TangoDown shows a notice before loading. The page then runs over Tor, but the built-in browser is **not the Tor Browser**: JavaScript runs, and protection against recognition is weaker than in the Tor Browser. **"Open here"** loads the page (with "☝ Capture page", "⛏ Findings", case log), **"Open here, don't ask again"** applies until restart.
- **Browser does not run over Tor:** TangoDown does not load the page. You can **" 🧅 Open in Tor Browser"**, **"⇌ Set network route to Tor"** or copy the address. Logged-in 🔑 tabs never run over Tor.
- **" 🧅 Open in Tor Browser"** (also under "⋯" for any page) starts your installed **Tor Browser** with the address; if it is already running, a new tab is added. TangoDown looks for it on the desktop, under Downloads and under Program Files; if it is somewhere else: "⋯ → Choose Tor Browser ..." (the file `firefox.exe` in the folder `Tor Browser\Browser`). What happens in the Tor Browser is outside TangoDown: it is not captured and not in the case log – only the note that the address was opened there. If the Tor Browser is missing, the address is on the clipboard; you can download it under "Connection & cloaking".
- **For unknown or risky .onion pages** the Tor Browser is the better choice. Use the built-in browser when you want to capture the page or take over findings.

☝ **Capture page ▾ :**

- **" 📷 Capture view – as displayed"** captures exactly the content of the tab as a full-page image and MHTML with SHA-256: including logged-in content, expanded comments, posts loaded later. If streaming mode is on, the tab is covered during capture. The backup itself contains the real content.
- **"☝ Reload independently and capture"** loads the address in a fresh session and additionally records the server IP, status and headers.

⛏ **Findings:** collects email addresses, phone numbers, social profiles, crypto addresses, IP addresses and linked external domains from the page. You check what should be added. **" + Add selected as elements"** creates the findings and attaches them to the page's domain with "found on". If the case has several graphs, TangoDown first asks **which graph** they go into: main graph only, a new graph or an existing one (the currently open one is marked). Existing items are reused. Everything runs locally; nothing is queried. **What surrounds the link comes along:** every finding from a link carries the visible **link text** (e.g. "Telegram group Example City"), the **section** (nearest heading) and the **context** (list item or paragraph around the link) as properties. The link text also appears in the finding's name. Telegram links with "+" or "joinchat" are marked as an **invite link (group/private channel)** – that is not a username.

🛡 **Self-check:** The 🛡 button (next to ⋯) shows what every website learns about this browser – measured in the current tab, without any outgoing request: identifier (must contain neither "Electron" nor "TangoDown"), browser brands, automation flag, time zone and language (do they match the cover profile?), WebRTC addresses, canvas and WebGL fingerprint, screen, cores, plugins and cookies. Anything notable is marked ⚠ with an explanation. "🌍 Check exit IP" shows the IP the other side sees; "↗ EFF Cover Your Tracks" and "↗ BrowserLeaks" open detailed external tests (data then goes to those sites).

🖥 **Disguise the operating system:** Under ⋯ → "Operating system" (or in the self-check via **"⚙ Change"**) the browser presents itself as **Windows, macOS or Linux**. Identifier, client hints (with the "Google Chrome" brand), `navigator.platform` and the reported graphics card then match; the Chrome version stays the real one. Applies after reload. Fonts, screen size and subtle rendering differences still give hints – the disguise makes attribution harder, it does not prevent it. A fixed custom identifier takes precedence; choosing a system sets it back to default.

✂ **Save snippet:** The ✂ button offers two ways: **"Area of this page"** – drag a frame over the displayed page (Esc cancels) – and **"Screen snippet (whole computer)"**: TangoDown hides briefly, the still image appears on **every connected screen**, and you drag a frame there (double-click = whole screen, Esc = cancel) and so also capture content from other programs. The screen snippet is available anywhere with **Ctrl+Shift+X**. Every snippet is stored as a PNG document in "Files & Documents" (SHA-256, origin, time, type); afterwards a **preview window with the snippet** appears at the bottom right with the buttons "◈ Add to graph as element", "▦ To report", "▤ Show in files" and "✓ Done" (Esc closes; the snippet stays in the files). A case must be open.

**Selection into the case:** Select text → right-click → **"◆ … into the graph …"**. TangoDown detects the type (person, email, phone, username, address, domain, crypto …) and suggests it; other types can be chosen. "◆ Link target into the case" adds a link, e.g. a profile. More entries in the same right-click menu: **"▦ Selection into the report"** (as a quote with page title, address and retrieval time), **"✎ Selection as note element"** (full text plus source as properties, linked to the page's domain), **"⌕ search in all cases"**, **"🔎 search the web"** (new tab) and **"⧉ copy with source"**.

🏛 **Archives:** earlier versions of the page in the Wayback Machine (all, oldest, newest) and at archive.today, plus all archived addresses of the domain. "Archive in Wayback now" asks first, because this tells archive.org about the address.

🕘 **History:** pages of this session with time. It is kept in memory only, can be copied and can be cleared. With a case open, visits are recorded in the case log anyway.

**Protection (⋯ → Protection):**

- **Block ads and trackers:** On by default. Built-in list of common ad, analytics and tracking services; the info line shows "🛡 n trackers blocked".
- **Cloaking profile:** Language, locale and time zone to match a country; "Automatic" follows the exit country of your connection (VPN/Tor/proxy). That way the browser does not give away where you really are through time zone or language. WebRTC always runs through the proxy only.
- **Fingerprint protection:** On by default. Websites often recognize browsers by the "fingerprint" of drawing surfaces (canvas) and graphics card (WebGL). TangoDown adds invisible noise when these are read, which changes at every program start, and reports a common graphics card as well as 8 cores and 8 GB of memory. This makes the browser harder to recognize. Takes effect from the next tab or after reloading.
- **Downloads – four modes** (choose under ⋯ → "Downloads" or at the top of the download list):
  - **Into quarantine** (default): files are renamed ( `.quarantaene` ) and stored in the data folder, never opened, only hashed (SHA-256, in the audit log). "⧈ Analyze in sandbox" takes you straight to

transferring the file into a sandbox VM.

  - **Normally into a folder:** like in any browser – into the Windows "Downloads" folder or a folder of your own ("change" in the list). Files with the same name are not overwritten but saved as "name (2).ext". SHA-256, origin and location are recorded in the case log.
  - **Ask every time:** Windows shows "Save as" for every download. Cancel = no download.
  - **Blocked:** downloads are rejected, with a notice. In offline mode (air gap) downloads are always blocked.

- ↓ **Download list** (↓ button in the browser bar, **Ctrl+J**, also via Ctrl+K "browser downloads"): running downloads with progress and a counter on the button, "✕ Cancel"; finished ones with "Open", "📁 Show in folder", "⧉ SHA-256" and "⧉ URL". TangoDown never opens **programs and scripts** (e.g. .exe, .msi, .bat, .ps1, .js, macro documents) or quarantine files – use "Show in folder" or "⧈ Analyze in sandbox" instead. "Remove from the list" and "Clear list" only remove the entry, not the file.

**Enlarge, pop out:** The browser area can be enlarged, shrunk or moved into its own window – open tabs and loaded pages are kept.

**Session per tab:** The selector next to the address bar switches between **"🕶 without login"** (temporary, in memory only) and a **logged-in platform account** ("🔑 TikTok (logged in)" ...). "🌐 Open in browser" and "◆ My profile" from "Platform accounts" open right here in a 🔑 tab – with address bar, back/forward, "⏢ Capture page", "▱ Video", "▣ As webcam" and "★ Pool". Caution: in a 🔑 tab you act with your own account.

**Right-click in the page:** Back/Forward/Reload, **Copy link**, open link in new tab, **"▣ Put on monitoring wall"** (e.g. a TikTok live from the live search – it lands on the most recently used wall), copy page address, copy/paste. The same menu exists in the login window of the platform accounts (there also Alt+←/→, mouse side buttons, F5, Ctrl+L copies the address).

### ⏢ Evidence capture

**Switch quickly:** "⇄ ⎘ Files & documents" at the top of evidence capture and "⇄ ⏢ Evidence capture" at the top of Files & documents jump straight to the other module.

**What for:** Capture web pages as evidence: screenshot, page content, server response, timestamp, SHA-256.

**One place for everything:** This is where you **capture**. Everything captured in the case – web pages, videos, images and your own files – is also listed in one place in **"Case files & documents"** ("Kind" filter). It is always **the same entry**: "⎘ In case files & documents" jumps there, and removing it works everywhere.

**Typical:** Document imprints, profile pages and posts in a traceable way.

**Remove:** In the list on the left, a ✕ appears when you hover. Faulty captures can only be removed with a reason; URL, time and both checksums remain in the audit log as a record. In cases with the four-eyes principle, only with approval.

**To the item:** The button with the item name (e.g. "◎ muster-gmbh.example") brings the main window to the front and shows the item in the Properties panel and in the graph – even from a separate window.

🕸 **Mirror website (several pages):** Below the address field, expand "▸ 🕸 Mirror website ...". Enter the **start page** at the top, then choose:

- **Depth:** 0 = only the start page, 1 = plus all pages linked there, 2 or 3 = two or three clicks away.
- **at most ... pages** (up to 200) and **pause** between two requests (1–10 s, spares the server).
- **only path** (optional, e.g. `/team/`): only pages below this path.
- **respect robots.txt** (default): areas the operator has blocked for automated requests are left out. Switching it

off asks first.

- **Purpose** (required, recorded in the audit log).

Each page is captured like a single capture – full-page image, MHTML, SHA-256, server IP and headers – via the same network route "Browser & web capture". **Never opened** are links to other websites, files (PDF, images, archives, videos …) and links that could trigger something (log out, delete, order, shopping cart). Progress is shown in the box; "■ Cancel" stops after the current page. Mirrored pages carry a in the list. At the end TangoDown puts a **page list** (address, time, HTTP status, both checksums, found on) as a text file into **"Files & documents"**; its SHA-256 is recorded in the audit log together with start, limits and purpose.

**Limits:** Only pages reachable without logging in are captured (separate session without cookies). Capture logged-in content one by one in the built-in browser with " Capture view". Whether and to what extent a website may be mirrored is your responsibility (purpose, the website's terms of use, copyright).

### Case files & documents

**What for:** Documents for the case with versions and checksums, encrypted within the case.

**Notes are not lost:** a started note is saved automatically when you switch to another document or close the area or window; Ctrl+Enter saves immediately.

**Category and delivery channel:** ▾ shows all suggestions – the configured ones and all that already occur in this case (e.g. "Bildschirmausschnitt (Windows)"). A value you type yourself is remembered as a **new entry**; the existing ones are kept.

**Everything in one place:** Besides your own files, links, videos and recordings, the list also shows **web page captures** (from evidence capture) and **images/stills** (stored at the element). The **"Kind"** filter narrows it to one sort; a click shows the screenshot or image with checksums, "Check integrity" and " In evidence capture". Web page captures and images are immutable; removes them from the whole case (web pages with a reason).

### File forensics

**What for:** Examine files without running them: checksums, metadata (author, camera, GPS), file type spoofing, embedded text and addresses.

## Matching

### Vehicle matching

**What for:** Classify license plates and vehicle identification numbers (VIN).

**How to use:**

- Enter a license plate (e.g. PI-AB 000): country and **registration district** are detected locally, plus E and H plates and special plates (Bundeswehr, THW, Federal Police ...). Without a hyphen, TangoDown shows possible readings.
- Enter a VIN (17 characters): check digit, manufacturer, region, model year.
- **Custom databases** are queried automatically as well. Hits appear in red; create, change or delete entries right here.
- Open registers with a reason: RDW (Netherlands), NHTSA (VIN). Further authorized interfaces (e.g. DVLA UK or agency APIs) via Vault & connectors.
- "Into the case" creates the vehicle as an entity.

**Important:** TangoDown does not query owner data – owner information is reserved for authorized bodies.

### ⌕ Universal search

**What for:** Search all cases you have access to and your own custom databases at once – read-only, without opening the cases.

**How to use:** Enter a term, press Enter. Several words = all must appear. The search covers names, all fields, notes, sources, links, captured web pages, documents and earlier queries; license plates and phone numbers also without separators. Hits are grouped by case; a click jumps exactly to the match location: entities are jumped to in the graph and flash, links are highlighted, evidence captures and network queries open with exactly that entry, documents in "Case files & documents"; other queries open their module (another case: switch after confirmation). Filters at the top hide kinds.

**Also via:** Ctrl+K → "Search all cases: ..." and right-click on any entity.

**Log:** Every search is recorded in the audit log of the open case and in the app log.

### ⛨ Registers & databases

**What for:** Query non-public registers and databases your organization is authorized for – agencies' specialist systems, internal databases, client systems. TangoDown provides the connection; your organization provides the access (certificate, account, network) and the authorization.

**Queries:** Choose a source, enter a search value, give the **legal basis** (remembered per source) and a **reason** → "⛨ Query". Or right-click a matching item (e.g. vehicle → "Vehicle register: ...") – then the value is prefilled and the result can be attached directly to that item. The result shows the configured fields and all rows; "→ Apply fields" or "→ Row" writes the details to the item with source, legal basis and checksum.

**Protection:** Every query only within a case, with legal basis, reason and case number in the audit log; the complete result is stored in the case with SHA-256. In the Agency edition, the order must cover the data category "Registers & protected databases" and the role must be Investigation or Lead; per source, a **four-eyes approval** can be switched on for every query (second person: Lead). Air-gap mode: only sources in your own network.

**Setup:** Administrators set up sources under "+ Set up source" (guide with examples in the developer manual). For querying, you only need the configured source; "Test connection" checks reachability without querying personal data.

## 🗃 Custom databases

**What for:** Cross-case, encrypted lists that you maintain yourself – license plate watch lists, known persons with photo, addresses, phone numbers, email addresses, any values.

**Persons:** Last name and first name are entered separately and stored as "Last name, First name". The search finds persons in any spelling ("Max Muster" = "Muster, Max").

**Owner & address for a license plate:** When you enter or edit a license plate (also directly in vehicle matching), there is the section "◆ Owner & address": person or company, date of birth, address, phone, email, "Owner since" and source. When you save, linked entries are created in "Vehicle owner" and "Addresses" (vehicle → owner → lives at/registered office); existing persons and addresses are reused. Only details from lawful sources – TangoDown does not query owner registers.

**Custom fields:** "+ Custom field" adds another field for all entries of the database (also for the owner). While you type, each field suggests the values that already occur there.

**How to use:**

- "+ New database", choose the kind. Define fields freely (⋯ Database → Fields).
- Create entries, change them with a click or delete them; add an image (for persons, facial features are stored for face matching).
- **Links** between entries – also across databases: vehicle → owner → address.
- Import and export CSV. **"Import CSV (only fill in)"** keeps existing values and only fills empty fields; afterwards you see the differences in a list and take them over selectively. **"... and overwrite values"** replaces differing values (with a list of what was replaced). Fields not in the CSV always stay. On export, values that Excel would execute as a formula (= + - @ at the start) are written as text.
- Every change is recorded in the **change log**.

**Searchable for image search:** At the top of each database there is the switch **"☺ searchable for image search"** (also under ⋯ Database). Only marked databases are included in the face / image search. Person databases are marked by default, all others only once you switch them on. When you switch it on, TangoDown detects the faces in the images already stored (locally; with several faces the largest one); next to it you see how many images have a recognisable face. Switching it off removes the database again – the images are kept. Every change is recorded in the change log.

**Custom kinds:** "+ New database → + Create custom kind ...": name (e.g. "Serial numbers"), symbol, label of the key value, **match rule** – *case-insensitive*, *exactly equal*, *digits only* (12-34/56 = 123456) or *without spaces and special characters* (AB-12 3 = ab123) –, default fields and the **element type** an entry gets with "Into the case". The kind then appears in the "+ New database" menu; edit or delete it via "Edit / delete custom kinds ..." (existing databases stay unchanged).

**+ Into the case:** On an opened entry, the button adds the entry with its fields and note as an element to the open case (type per kind, e.g. license plate → vehicle, address → place).

**Queried automatically:** in vehicle matching, in face matching, in the investigation autopilot and via right-click "Search own databases".

## ☺ Face matching

**Off by default:** Facial features are biometric data (Art. 9 GDPR). Face matching must therefore be **switched on deliberately** – in the section itself or under "Help & info" → "Features & updates" (where you can also switch it off again). When off, all face functions are blocked; stored references stay in the case until you delete them.

**What for:** Local matching of faces – e.g. searching for missing persons or checking whether a person appears in other images.

**Face / image search on an element:** If an element in the graph has an image, the right-click menu offers **"☺ Face / image search …"** directly. The element's images are checked against the case's face inventory (references) and against all own databases marked as **"searchable for image search"** (see Custom databases). Everything runs locally; as usual a reason is required, and every search is recorded in the audit log. A match indicates similarity, not identification – always check it yourself.

**How to proceed:**

1. **Create references** – known persons with photos: take them from case images, search for a person and add a reference image, or load the demo set. The **demo set** ships with the program: six public figures with three clear portraits each as reference and one or two photos from a different occasion as test images – public-domain photos from Wikimedia Commons; sources and authors are in the note of each demo person. It loads without internet in a few seconds; only once per case, missing persons are added. **"🌐 Search more persons online"** in the demo menu additionally fetches further public-domain photos from Wikimedia Commons; many images are checked and only those with exactly one large, clear frontal face are taken – group photos briefly appear while browsing with "multiple faces – skipped", but are never learned. At the end the demo log names the compute engine and the time per photo – if it says "CPU", graphics acceleration is missing and everything takes much longer.
2. Enter a **reason**.
3. **Check image (image → name):** drag in an unknown photo; all faces are marked and shown with similarity in percent. Green ("strong candidate") appears only if the best candidate reaches at least 70 % and is clearly (15 points) ahead of the second; per person, the average of the two best reference images counts. Small or blurry faces are never rated as a strong candidate. It remains a hint, not an identification.
4. **Search person (name → images):** where else does this person appear in the case images?

**New person:** Type the name into the "Search person" field – if the person does not exist yet, the button next to it reads "+ Create “name”" and takes the name. If it already exists, it is selected instead of created twice. Without a name, an input field opens right away. **Rename:** double-click the name in the list or ⋯ → "✎ Rename"; Enter saves, Esc cancels.

**Manage persons and images:** Drag an image onto another person = **move** (with Ctrl: copy). ✕ on the image (on hover) or right-click: "Remove reference" (image stays in the case) or "Delete reference and image". ⋯ on the person or right-click: show in graph/Properties, remove all references, or delete the person together with references and images. If names exist more than once (e.g. demo set loaded twice), "🧹 Remove duplicates" appears – per name, the person with the most references is kept.

**Save query image in the case:** creates the checked image as an item "Query image …" (photo) in the case – with image, checksum and reason, linked to the best hit as a hint ("similar 73 % – no identification"). "⌬ Show in graph" takes you straight there; it is stored encrypted in the case container.

**Tips:** several reference images per person from different angles; click images to view them large; "Show checked images" shows the search run live.

🎞 **Film view:** With the switch "Film view while matching", the compared images flash by in very quick succession like in a film – for "Image → name" the reference images next to the query image, for "Name → images" the case images next to the person searched for. The run then slows down and stops on the most similar image (green: similarity of 50 % or more with a well-detected face, yellow: uncertain, red: no match). This is display only: result, percentages and audit entry are the same as without the film. Click or Esc closes at any time; switch it off with the same switch. If "reduce motion" is set in the system, the film view starts switched off.

**Reference image by dragging:** Drag an image (file or directly from the browser) onto a person in the reference list – or select a person and drag onto "+ Add reference image". The image is stored in the case and added as a reference if there is exactly one face on it.

**Import / share (building up extensive reference persons):**

- **Import folder:** one subfolder per person ("Alex Beispiel" with any number of photos) – or images directly in the folder with the name in the file name ("Alex_Beispiel_2.jpg", "Alex Beispiel (3).jpg" → Alex Beispiel). Existing persons with the same name are extended, otherwise new ones are created.
- **Export:** all reference persons of the case (names, notes, images) as a `.tdfaces` package – AES-256 encrypted with a password. A reason is mandatory and is recorded in the audit log. Share the password separately (e.g. by phone).
- **Import package:** open `.tdfaces` from colleagues, enter the password. Facial features are **not** included but recalculated here from the images – feature data from others is not trusted.
- Face images are specially protected data (GDPR Art. 9): only import and share them with a legal basis.

**Important:** The result is a similarity score as a hint, not an identification. **83 % similarity does not mean an 83 % probability that it is the same person** – light, angle, age and image quality distort the score, and people who look alike do get mixed up. Confirm every hit with other evidence. Face images are specially protected (biometric) data: use them only with a sound legal basis and only within the scope of the assignment. Images and features do not leave the computer.

## Situation & map

### 📰 Message center

**What for:** Public reports from RSS/Atom feeds in one place – on police/operations, politics, crime, violence, disaster/situation and military. Read-only via the configured network route (Tor/proxy).

**How to use:** "↻ Refresh" fetches the reports from the active sources. Filter by keyword and source at the top, below that by **category** (the category is detected automatically per report from title/text). Clicking a report opens it in the built-in browser; "📰 Into the case" creates it as an **event** (with time, source, category, link, summary); right-click for more.

**Sources:** "⚙ Sources" shows the feeds – switch them on/off, remove them, or add your own RSS/Atom addresses (with category) via "+ Add feed". Defaults include Presseportal (police/emergency services) and tagesschau; more are prepared and can be switched off.

**Important:** Reports are hints from third-party sources – check them before adding. Feeds can be temporarily unreachable (then "⚙ Sources" shows the error).

### 🌍 Geo-Intel

**More maps and specialist layers:** Under "Map" additionally **basemap.de** (Germany, BKG), **basemap.at** and **basemap.at aerial** (Austria), **swisstopo** and **SWISSIMAGE** (Switzerland), the **NASA daily image** (VIIRS, with date selection – e.g. smoke, flooding, snow; approx. 375 m per pixel) and **night lights (Black Marble)**. Under "Specialist layers": 🚆 **Rail infrastructure** (OpenRailwayMap), 🔥 **Fires** (NASA FIRMS, last 24 h, free MAP_KEY in the vault) and 🛢 **Possible oil slicks** (SkyTruth Cerulean, 30 days, machine-detected from radar images – a hint, not a finding; click opens the source). Fires and oil slicks are queried for the visible section and refreshed after moving; every query is recorded in the audit log. The attribution of the selected map is shown at the bottom right.

**Collapse the sidebar:** The sections of the right-hand sidebar (map, special layers, layers, live situation, social posts, time slider) collapse and expand with a click on the heading. When collapsed, the current choice is shown next to it (e.g. the selected map). TangoDown remembers the state.

**What for:** The case on the map – plus tools for situation maps.

**Multiple situation maps:** Via **"◍ Main map ▾ "** (next to the search) you create further situation maps, e.g. "Operation North" and "Observation Harbor". Each map has **its own map symbols, arrows and geofences**, its own extent and its own tab – can be popped out as a window, even all at once ("Each situation map in its own window", e.g. for multiple monitors). For each map you choose which **case items** it shows: **all**, **none** (pure situation map) or **only selected** (select the item in the graph, then in the menu "… on this map"). The **main map** shows everything as before; existing cases do not change. Geofence alerts apply regardless of which map the geofence is drawn on. Deleting a map removes its symbols, arrows and geofences (case items remain) – all in the audit log.

**Several items at once:** Shift- or Ctrl-click adds symbols and arrows to the selection, Ctrl + drag draws a frame around several. Dragging a selected symbol moves all of them; Del deletes all (with confirmation); right-click opens the menu for the selection (color for all, zoom in, remove); Esc clears the selection.

**How to use:**

- Map style: dark, light, street, satellite. Show and hide layers.
- **Search:** finds places (OpenStreetMap) and your **own objects** – labeled symbols, arrows, geofences, geolocated entities.
- **Move/geolocate entities:** You can **drag any entity point with the mouse to the right spot** – the new geoposition is saved (in the audit log). Right-clicking the point also offers **"Enter coordinates …"** (latitude/longitude in decimal, in degrees/minutes/seconds or as a map link) and "Remove geoposition". This also lets you fine-tune a webcam that was geolocated automatically from its address.
- Draw **geofences:** right-click the map → **"Geofence: drag circle"** (press in the center, drag outward), **"Draw rectangle"** or **"Freehand drawing"**, then give it a name – or "Geofence here (circle with radius)" with a radius in meters/kilometers. Alert as soon as an entity is geolocated there. **Edit:** right-click the geofence → **"Move / resize"**: the ✣ handle in the center moves it, the ⤡ handle on the edge changes the size (for freehand, every corner point), the size is shown live next to it; right-click the area → **Save** or Cancel. In the same menu: color, rename, label, circle ↔ rectangle, situation alert, remove.
- **Select and move symbols:** A click selects a symbol (handles for size and rotation), dragging moves it – the position is saved immediately. **Ctrl + drag a frame** selects several, **Shift/Ctrl + click** adds single ones; selected symbols are dragged together, right-click offers color and remove for all. Esc clears the selection.
- **Situation map:** Place symbols (police, military, air, sea, emergency services (BOS), vehicles, your own images), symbol search, rotate, size, colored outline, label; draw and bend **arrows**. Symbols scale with the map scale (can be switched off).
- **Live situation:** Aircraft (adsb.lol, OpenSky, ADS-B Exchange) and ships (Digitraffic – free, only Finnish waters and the northern Baltic from about 56° north; AISStream – worldwide, free key) in the current extent; a click shows details, "Add to case as sighting". **" ⚡ Add sighting to case"** creates the ship or aircraft as a "vehicle" element with all identifiers (MMSI, IMO, call sign, ship type or ICAO, registration, model) – the same

element on later sightings – and the sighting as an event with time, position, speed, course, altitude and destination, linked; "◈ Show in graph" jumps there.

- **World clock layer:** night side, sun position, local times with legend.
- Export the **map as an image** with title, timestamp and legend.
- Right-click an object: "Zoom in".

📡 **Social posts on the map:** Switch on in Geo-Intel under "Social posts": hits from **source monitoring** that carry a location appear on the map with the symbol of their source (time range selectable, "new only"). **Solid border** = exact coordinates (in the post or as a map link from Google Maps, OpenStreetMap, Apple Maps, Telegram location), **dashed circle** = only a place name in the text (approximate – written about, not necessarily from there). Click a symbol: text, author, time, "↗ open", **" + Add as element"** (post with location + account) and "◉ Monitoring".

⏱ **Time slider:** Switch on in Geo-Intel under "Time slider": the map shows only items **up to the chosen day** – or only a window (this day only, last 7 or 30 days). The date comes from time properties (e.g. "Date", "published", "seen"), otherwise from the date the item was created in the case. ◀ / ▶| steps day by day, ▶ plays back the timeline. Social posts follow the slider by their publication time.

## 📣 Social search (the easy way)

🗏 **Social deck:** Watch social media in **columns side by side** – like TweetDeck, but read-only. At the top you add columns: **# Search / hashtag** (terms and hashtags, platforms and period selectable), **@ Account** (Bluesky handle, Mastodon name@server, public Telegram channel, Reddit name, YouTube @handle with key), 📍 **Place** (posts mentioning the place) and 📈 **Trends** (Bluesky, Mastodon, Google search trends per country; " + #" turns a trend into a search column). Each column refreshes at the set interval (2–60 minutes) and marks new posts; "⟳ Refresh all" queries immediately. Per post: ↗ open in the TangoDown browser, + add as element (post with account), 🖷 capture the page as evidence, ▦ to the report, ⧉ copy; clicking the author turns them into an account column. Columns can be moved, changed and removed and apply per case. Only what is publicly accessible without sign-in is read; every query is recorded in the audit log. **Network route:** The switch at the top (e.g. "direct" or "Tor") shows which route the deck uses for its queries and changes it for the deck. If a service refuses (e.g. HTTP 403 – some services block certain addresses or requests without sign-in, Reddit almost always), the reason appears below the column header instead of a silently empty column; another route may help.

**Trends column – country:** The country selection (e.g. DE · Germany, AT, CH, US) applies **to Google Trends only**. Bluesky and Mastodon have no country filter; their trends are worldwide (mostly English) and marked "worldwide". Google trends of the selected country come first. ↗ opens the news item Google names for the search term, otherwise Google News – Google's trends detail page often blocks new sessions with "429 Too Many Requests". To see only the country, untick Bluesky and Mastodon in the column.

**What for:** "What is being written publicly about #beispiel, #stadtname … right now – and where?" Find posts, filter them on the map, open them, capture them as evidence.

**How it works:**

1. Enter terms or hashtags separated by commas (e.g. `#beispiel, #beispieltag, Stadtname, Demo Stadtname`), choose a time range (6 h to 7 days) and sources: **Bluesky** (keywords and hashtags), **Mastodon** (hashtags only), **Reddit**, **Lemmy**, **Hacker News** and 📰 **News** (Google News and worldwide press via GDELT) – all without login and on by default; plus **YouTube** (videos, with your own key "youtube") and **X** (with your own access "x"). If a source fails (e.g. Reddit sometimes blocks requests without login), the others still deliver; the

reason is shown as a notice. The same sources are used by "Fetch recent posts" in the graph, the AI web search and the AI research.

2. Optionally **"Germany only"** (default): posts in German or with a German place/"Germany" in the text – the reason is shown on the post. Platforms do not publish a location; a place that is mentioned is the topic, not necessarily where the person is.
3. Optionally **"Only these places"** (e.g. "Hamburg" or districts, squares, buildings such as "Altona, Jungfernstieg"): the list and map then show **only posts from these places** (" 📍 Only posts from Hamburg · show all places"). Unknown places are looked up once via OpenStreetMap. Different spellings of the same city ("hamburg"/"Hamburg", "Cologne"/"Köln", "Munich"/"München") are merged into one place.
4. **"⌕ Search".** Posts on the left, on the right the map with the cities/places mentioned (dot size = count; a click filters the list).

**Filter:** by term, platform, place, " 📍 with location only" and free text – list and map always show the same. "✕ Clear filter" resets.

**Per post:** "↗ Open" (system browser), "⌕ in browser" (built-in browser), **"☝ Capture as evidence"** (screenshot + MHTML + SHA-256 of the original post, under evidence capture), **" + Add as element"** (post with place, account, topic – linked), "⧉" copy, "◍ Map".

**Livestreams:** "Livestreams" tab – with your own YouTube key ("youtube"), the YouTube lives currently running as cards ("↗ View", "☝ Capture", "→ Add to case as livestream" for monitoring walls and recording); always available: **live searches** on YouTube, TikTok, Twitch, X, Facebook and Instagram (open in the built-in browser).

**Web:** "Web" tab – searches on **Google** (recent, news, videos), Bing News, DuckDuckGo as well as Telegram/Instagram via Google with one click; with your own **Brave Search** key ("brave"), web hits directly in the list. Google itself is not read automatically (terms of use).

**Keep watching:** adds the terms as watches to source monitoring (every 15 minutes, alert on anything new; geolocated hits also in Geo-Intel under "Social posts").

**Framework:** Every search is recorded with a checksum in the audit log, via the "SOCMINT" network route; in the Agency edition, the order needs the data category "social".

### ◷ World clock

**What for:** Local time in every country, day/night, office hours, daylight saving time – and convert timestamps into any zone.

**Legend:** light dot = day, yellow = twilight, dark = night, green ring = usual office hours (Mon–Fri 8 am–6 pm), ☼ = daylight saving time.

### 📡 Source monitoring

**What for:** Watch open sources continuously – similar to "tweetmonitor": reports as soon as a keyword or hashtag appears, an account or channel publishes something, or a website changes. Unlike the situation picture (trends, frequencies), monitoring shows the **individual posts**.

**Sources:** Bluesky, Mastodon (hashtag or account name@instance), Reddit (keyword, u/user, r/subreddit), Hacker News, public Telegram channels (web preview), GitHub (keyword or user activity), RSS/Atom feeds (also a YouTube channel via the channel ID "UC…") and **website change** (reports changed text with the new and removed lines).

**How to use:** "+ New" → source, kind (keyword/account/address), value, name, optionally "Only with term" and "Exclude", interval (5 minutes to 1 day), purpose → **"Save and verify"**. The **first run saves the baseline** (visible, but not as new and without an alert); after that, TangoDown only reports what is newly added.

**Hits:** on the left, the number of unread hits per watch; on the right, the stream – new hits marked. Per hit: ↗ **open**, → **Into the case** (post + account, linked), **Capture** (evidence capture with checksum), **copy**. "✓ All read" resets the marking; "⟳ Check now" checks immediately, "⏸ Pause" stops.

**With your own access (social API connectors):** Additional sources via the official interfaces – only if you have access there and store it in the **Vault**:

- **X / Twitter (API v2):** search query of the last 7 days or posts of an account – Vault "x" = bearer token of your developer access (without a paid access tier, X returns hardly anything).
- **YouTube (Data API):** new videos for a keyword or channel (channel ID "UC…") – Vault "youtube" = API key (free daily quota).
- **Bluesky (logged in):** reliable keyword search – Vault "bluesky" = `handle:app-passwort` (an **app password**, never the main password).
- **Mastodon (token):** full-text search on your instance – Vault "mastodon" = `instanz.social|token` (token with read rights only).
- **Rocket.Chat (your own server):** messages of a room (`#raum`) or a search term across all rooms of your account – Vault "rocketchat" = `https://server|Benutzer-ID|Token` (personal access token). **Only rooms your account is a member of, and only with authorization** (e.g. your own work chat).

If the access is missing, TangoDown queries nothing. Provider errors (quota exhausted, access tier insufficient) are shown in plain language on the watch. Facebook and Instagram are not included: their interfaces deliver public posts only to apps reviewed by Meta.

**Places and map:** Every hit is **geolocated** where possible: coordinates or map links in the post, otherwise a place name from the watch's **own place list** ("Places for the map" – one place per line, e.g. "Elbphilharmonie" or "Lager Nord; 53.55, 9.99"; names without coordinates are looked up once via OpenStreetMap when saving) and – can be switched off – larger cities. The hit then shows 📍 place, "◍ Map" and **"📍 Geolocate"** or "Change location" (enter coordinates, a map link or a place name). Geo-Intel shows geolocated hits under "Social posts".

**Alert:** on new hits, a message in the bell and – depending on the setting under "Notifications" – a Windows notification. Optionally, new hits go to the **outgoing webhooks**.

**Framework:** Watches belong to the case and only run while the case is open – via the "SOCMINT" network route, with air gap/kill switch and (Agency edition) order and data category. Creating, changing, deleting and every round with new hits are recorded in the audit log. A blocked watch (e.g. order expired) pauses itself and reports this once.

## ↗ Outgoing webhooks

**What for:** Automatically send new hits from source monitoring and alerts to your own systems – e.g. into a team channel (Rocket.Chat, Mattermost, Slack, Microsoft Teams, Discord) or to automations (Zapier "Catch Hook", Make, n8n, your own services).

**Setup:** In the target system, create an "incoming webhook" and copy the address. In TangoDown **"+ Webhook"** → name, **format** (General/JSON, Rocket.Chat, Mattermost, Slack, Teams, Discord), address, choose events → Save → **"Test message"**.

**Events:** "New hits in source monitoring" (only for watches with "send new hits to outgoing webhooks") and "Alerts" (watchlist, geofence, situation picture, monitoring).

**Data-minimizing:** The default is a **short message** (title, count, link). Texts of hits and alert details are only sent with **"Include content"** – only for trusted targets.

**Security:** The address works like a password: it is stored **encrypted in the Vault** and is not shown again (only the server name). Optionally with a **signing key** – then every message carries the header `x-tangodown-signature: sha256=…` (HMAC-SHA256 over the content), which the recipient can use to verify authenticity. Only https:// (http only in your own network). Sent via the "Connector" network route; with air gap or kill switch, nothing is sent. Every sending is recorded with target, event and status in the audit log of the case. Setup for administrators only.

## ◉ Situation picture

**List and map together:** a click on a signal on the left flies the map to the country and marks it with a pulsing ring; the detail opens on the right. A click on a circle shows the evidence with the period: per post platform, time, term and text, per event category, place, time and news site – **"↗ Open source"** or **"↗ Open article"** shows the original (TangoDown or system browser). A click on a situation picture alert also jumps straight to the country.

**What are the tabs for?** *Signals* = automatically detected anomalies (sudden increase) to check · *Watch* = terms whose frequency in the live stream is counted continuously (trend per hour and country – the basis of the map) · *Radar* = which hashtags are gaining overall right now · *Hashtag* = one-off search for posts on a hashtag (Mastodon). The situation picture shows **trends and frequencies**; to find **individual posts**, filter them on the map and capture them, use 📣 **Social search**.

**What for:** Watch worldwide events and social media activity; anomalies are reported as signals and can be turned into an investigation graph.

**Sources of the watch:** Bluesky (live stream), Mastodon (hashtags), Reddit, Lemmy, Hacker News and news (Google News, GDELT) – the last four are queried every 5 minutes per term; the first fetch does not count, so no artificial increase occurs.

**Area (🎯 only … / 🌐 worldwide):** If your watches have countries (e.g. all "DE"), the situation picture shows signals and map points **only for these countries** – reports about, say, Syria or North Korea from the worldwide event data (GDELT) are hidden ("n signal(s) from other countries hidden · show worldwide") and trigger **no alerts**. At the top right you can switch to "🌐 worldwide". A watch without countries counts as worldwide and lifts the filter.

**Hashtag search ("# Hashtag" tab):** Enter a hashtag (e.g. `#osint`) – TangoDown fetches public posts from several Mastodon servers, without login. Shown are the count, a timeline per hour (last 24 hours), related hashtags (a click searches further) and the posts with time, account and link. Every search is recorded in the audit log. Bluesky no longer allows anonymous search; there the watch runs via the open live stream.

**Hashtag search – cities and filters:** The hashtag search detects **cities** mentioned in the posts – also as a hashtag in any spelling (#Köln, #koeln, #koln, "# köln") – and shows them on the map as **turquoise dots** with a count; clicking a dot lists the posts with link. This is the **place mentioned**, not necessarily the location of the person (Mastodon and Bluesky do not publish a location). The chips 📍 **Cities**, ⌖ **Countries** (DE, FR …) and 🗣 **Language** are **filters**: clicking filters the post list and map, several can be combined, "✕ Clear filter" resets.

## ⚑ Alerts & watchlist

**My alerts – set up, view, change, delete in one place:** At the top of the module, **"+ New alert"** → what should be watched: **hashtag / term** (e.g. `#hamburg` – new public posts on the chosen platforms), **place / area** (e.g. "Berlin" – "⌕ Find place", choose a radius; alert on situation events in the area and when case elements are

located there, optionally also on posts naming the place), **domain**, **crypto address** or **username**. Add a justification – done. Below, **all** alert rules are listed, wherever they were created (source monitoring, geofences, watchlist, situation picture): ↗ shows where the rule lives or what it found, ⏸/▶ pauses, ✎ changes the interval or radius, 🗑 deletes (previous alerts remain in the case). Whatever arrives is listed below under "Received alerts" – with its source; a click takes you to the event.

**Which alerts do I want?** The orange number at the bottom of the status bar ("⚑ n ALERTS") counts unread alerts. In the "⚑ Alerts & watchlist" module, under **"Which alerts do I want?"**, you set for each source: **On the alert itself:** at the right of every row its source is shown (e.g. "Situation picture signals") – a click on it jumps to the matching row here with on · silent · off. "⋯" on the row opens the same menu as a right-click: silence, switch off or "Where to configure what is watched".

- **Mode:**
  - **on:** The alert counts in orange at the bottom.
  - **silent:** The alert only appears in the list and is not counted.
  - **off:** No alert is created at all.
- **Windows notification:** Notification at the bottom right, only in "on" mode.

**The sources and where you set what they watch** ("↗ Where to configure" jumps there):

- **Watchlist:** Domains, crypto addresses and usernames. Add or remove them at the bottom of this module.
- **Geofences:** An item enters an area, or there is situation activity in the area. On the map, right-click the area.
- **Situation picture signals:** an unusually high number of events in your area. In the situation picture, choose the area (e.g. DE only), sources and observations. Most orange alerts often come from here.
- **Source monitoring:** new matches from your observations. Turn "report" on or off per observation.
- **AI tasks:** relevant changes. Turn "report" on or off per task.

The setting applies to this computer, so it is available **even without an open case**; changes are recorded in the audit log of the open case. **Right-click an alert:** go to the event, mark as read, copy text, **silence or turn off alerts from this source**, "↗ Where to configure what is watched". "mark all as read" sets the number to zero.

**Area monitoring:** Right-click a geofence → "◉ Situation alert for this area …" and enter a threshold. As soon as the situation picture (GDELT) reports that many events – unrest, violence, tensions – within the area, an alert with location and source is created (at most once per hour per area). The situation picture must be running for this. A hint, not a finding – check the source.

**Purpose:** Watch domains (DNS changes), wallets (new transactions) and usernames (new profiles); geofence alerts. Windows notifications can be turned off per source; a click jumps to the event.

## ★ Camera pool

**Purpose:** All cameras and live streams across cases in one place – collected once, can be added to any case and any monitoring wall.

**Where:** Sidebar "Situation" → "★ Camera pool", Ctrl+K "Camera pool", or the "★ Camera pool" tab in the "Webcams" module.

## ◉ Webcams & video · ▣ Monitoring walls

**Purpose:** Show public cameras and live streams for places, save still images; your own cameras in the Video Center; several sources on monitoring walls for the operations center.

★ **Camera pool:** Top-level area for all cameras and live streams – stored across cases and permanently, usable even without an open case. Every webcam created in a case goes into it automatically, as do a case's webcams when the case is opened. From the pool: "◉ To case" brings the camera into the open case, "▦ Wall" puts it on a monitoring wall. Name, place, tags and note via ✎ or right-click; filter with substring search. Your own cameras from the Video Center are included too (credentials stay in the Vault). You can also fill the pool from the wall (right-click → "★ Add to camera pool") and from the browser ("★ Pool"). Public addresses only, no credentials.

**Removing with confirmation:** ✕ on a tile asks first ("remove from the wall?"); afterwards **"↶ Restore"** in the message brings the tile back. The case and the camera pool keep their entries. In the **camera pool**, "Remove from pool" also asks first and offers **"↶ Restore"** – otherwise the camera would be gone without a known link.

**Live page into the case:** " + Add as element" and "★ Add to camera pool" take the **address the tile is actually showing right now** (e.g. `tiktok.com/@name/live` instead of the general live overview, which shows a different stream each time). In addition, a **still image** of the moment is attached to the item (encrypted, SHA-256), along with the time ("seen") and the source address. When opened later, a live account shows whatever is running at that time – the still image documents what you saw; "🎞" saves the stream itself.

**A tile's menu:** Right-click the tile or its name at the top left – or the **"⋯"** button in the button bar. With YouTube and other embedded players, a right-click *in the video* goes to the provider; so use "⋯" or the name there.

**Each wall its own window:** "⧉ Separate window" in a wall's bar (or right-click the wall tab → "As separate window") puts **exactly this wall** into its own window with its own taskbar entry – even from a window that already holds several walls as tabs. **Rename:** ✎ next to the wall name, double-click the name, or right-click the tab → "✎ Rename wall …" – the new name shows immediately in the tab, the window bar and the taskbar. In a separate window with several tabs: right-click → "⧉ Move this tab to a separate window". "⧉ All as windows" (next to " + Wall") spreads all walls across separate windows, e.g. for several screens. If a wall is running in its own window, the "Monitoring walls" overview does not play it again (no duplicate sound/stream) – "⤴ Go there" brings that window to the front. The ✕ **of a wall window** (also "Webcams & video") **closes the area completely** – stream and sound stop immediately; the wall itself is kept and can be reopened at any time. **"⇲ Back to main window"** instead brings the area back without closing it.

**Reload:** Every tile in "Webcams & video" has **"↻"** – reloads the live page or YouTube, or fetches the image immediately; in monitoring walls, likewise "↻" in the button bar. Live pages show "running in the tile" instead of a permanent "loading …".

**Sound with several cameras (Webcams & video):** at the top, " 🔊 Sound: one" (turning one on mutes the others) or **" 🔊 multiple"** – then each tile has its own sound switch and several can be heard at the same time; " 🔇 Mute all" turns all of them off. Your choice is remembered. (In monitoring walls, each tile has its own sound anyway.)

**Live pages:** TikTok, Facebook, Twitch, Instagram, Kick, X and others run as a web page in the tile – in an isolated session without sign-in, sound only on click.

**Checking and geolocating the pool:** "⟳ Check streams" shows for each camera ✓ running, ✕ unavailable or ⊘ only on the platform (YouTube: embedding blocked by the owner); "running only" hides the rest. "◍ Map" shows the geolocated cameras, "◍ Locate … without position" looks up the place or name via OpenStreetMap. "Near" an item or a geofence of the case plus a radius filters and sorts by distance. Situation alerts for an area also list matching pool cameras.

**Prepared live cam searches:** If places come from AI research, they appear at the top with "▶ YouTube live" and "⌕ Web search". The search opens the embedded browser; if there is a matching live stream, "▣ As webcam" adds it to the case with one click.

**Stream with a place → automatically on the map:** When creating a public webcam ("◉ Public webcams" tab, "＋ Webcam" button) and when taking over a live stream from the browser ("▣ As webcam"), you can enter an **address or a place**. The address is looked up via OpenStreetMap and the camera immediately appears at that spot in Geo-Intel – as a geolocated entity that can be shown, filtered and linked on the situation map like any other. If a camera has no position yet, the tile shows **"◍ Geolocate"**: it takes the camera's address or place field (or asks for it), looks it up and sets the map position; if there are several matches, you choose. If the camera is already geolocated, **"◍"** goes straight to its spot on the map. You can add or change the address at any time in the Properties panel ("Address / place (for the map)" field). The camera pool geolocates its entries the same way ("◍ Locate … without position") and takes the position into the case.

🎞 **Video evidence capture (download & recording):** Public videos can be saved for evidence capture – as a finished video (**VOD download** including sound) or as a **recording** of a running live stream (YouTube, TikTok, Facebook, Twitch and many more).

- **By link:** In the **Video Center** ("▦ Video Center" tab), **paste the video link** at the top and click "🎞 Load video" → download, record, or load the sound only.
- **From the browser:** On a video or live page, the **"🎞 Video"** button → download the VOD, record the live stream, or sound only.
- **From a live tile:** On YouTube/live tiles (Public webcams), the **"● Recording"** button.
- **From a monitoring wall:** on every tile with a web address, the **"🎞"** button (or menu → "🎞 Save video"): **record live stream**, **download video** or **sound only** – encrypted into the case (Case files & documents) with SHA-256 and an audit entry. **"●"** on the tile starts the recording directly. While it runs, the tile shows a red **"● REC 0:18"** at the top left with the running time and **"■ Stop & save"**, plus a red frame – even without the mouse over it.
- **Requirement:** the free programs **yt-dlp** and (for recordings, picture+sound and RTSP cameras) **ffmpeg**. **Set up with one click:** If they are missing, TangoDown asks briefly after startup ("↓ Set up now" / "Later" / "Don't ask again"); also available at any time under "Webcams & video → ⚙ Video tools" or "⚙ ffmpeg" with **"↓ Set up … automatically"** and later **"⟳ Update …"**. Downloads come only from the official project releases on GitHub (yt-dlp: approx. 18 MB; ffmpeg builds of the yt-dlp project: approx. 200 MB); before storing them, TangoDown checks the **SHA-256 checksum** against the official checksum list – if it does not match, nothing is installed. At the very first start yt-dlp unpacks itself and is checked by the virus scanner – this can take up to a minute (especially in virtual machines); TangoDown waits that long. If the old file is still locked, TangoDown places the new one next to it. Stored in the data folder (`TangoDown-Daten\tools`, also in portable mode, without admin rights); the setup is recorded in the audit log. Alternatively, you can still choose your own programs ("📁 Choose …").
- **Recording until stop:** A livestream recording starts **immediately** and runs until you press **"■ Stop & save"** in the message at the bottom right (safety net: at most 6 hours). The **purpose** is asked while recording is already running; if it is still missing at the end, saving waits for it – leaving it empty discards the recording (recorded in the audit log). For cases without mandatory details the question is skipped. It is saved **encrypted in "Case files & documents"** – with **SHA-256**, source URL, time, purpose and account (visible under "Details recorded when saving") and an entry in the audit log. "⎘ Open recording" in the message jumps straight there.
- **● REC – record immediately:** The red **"● REC"** button in the browser bar (or **Ctrl+Shift+R**) starts without asking first; the same button then shows **"■ Stop"** and ends the recording. A running recording is marked with ● on the tab. The button shows what it records (**"● REC · Tab"** or **"● REC · Stream"**); the arrow **" ▾ "** next to it (or right-clicking REC) sets it: the **tab** (default) or **only the livestream**.
- **Tab recording (picture, sound, chat):** records the browser tab as it is shown – video, **chat, reactions, gifts** and the **tab's sound**, on any page (TikTok, YouTube, Twitch …). Only this one tab is recorded, not the screen

and no other windows. Result: a WebM file in "Case files & documents". **Keep working while recording:** in other browser tabs this works without restriction – the recorded tab keeps running in the background. 🔇 mutes it while the recording keeps the sound. If the whole browser area is covered by another tab (e.g. "Case files"), the sound continues but the picture stands still until the browser is visible again – a message points this out. To work in other areas meanwhile, pop the browser out into its own window **before** recording (drag the tab out of the window) or place it next to the other areas. Any page can be recorded this way, not only videos. Sound is recorded unprocessed; picture quality matches the display. **Only the stream** (without chat, in original quality) is available via "🎞 Video → Record livestream".

- **Running live instead of a finished video:** "Download video" only works for finished videos. On a running TikTok live page TangoDown records instead automatically; for other platforms the error message offers "⏺ Record now".
- **Into the graph:** In "Case files & documents", **"◈ Add to graph as element"** takes over a record as an element – recordings as type **"Video"** (source, platform, account, time, SHA-256, purpose), images as "Photo", otherwise as "Note". The element refers to the record; if the case already has an account with the same name (e.g. @sampleaccount), it is connected to it. A second click shows the existing element ("◈ Show in graph").
- **Setup:** In the Video Center under **"⚙ Video tools"**, enter the path to **yt-dlp** (e.g. "winget install yt-dlp"); for merging picture and sound and for recordings, also **ffmpeg** ("⚙ ffmpeg"). Both are standalone programs and are not bundled. Download/recording runs over the **cameras' network route** (Direct/tunnel). **Public content only** for evidence capture; platform terms of service and copyright are your responsibility.

## Tools

**Editing tiles:** ✎ on the tile (or right-click) → name or **change address** – without creating the tile again.

**Live on TikTok, Twitch, Kick …:** A tile with such a live address (e.g. `https://www.tiktok.com/@name/live`) first fetches the **direct stream address** and plays the stream without the web page (TikTok directly via the public live interface, others via yt-dlp from the video tools). If the account is **not live right now**, the tile says so ("↻ Reload" once it is running again). If the direct route does not work, the tile shows the web page. **Signed-in accounts:** If you are signed in to the platform under "Platform accounts", the tile loads the page in that session (marked "🔑 signed in") – can be turned off per tile via right-click "Show without login".

### 🌐 Remote cameras via VPN

**Purpose:** Include your own cameras at another location via an encrypted tunnel (holiday home, company, relatives) – as if they were on your own network. The camera stays invisible to the internet; only your devices in the VPN can reach it. After that, it works in the Video Center with all functions (live image, sound, pan/zoom, still images, monitoring walls). **Why not via the Reolink UID or the share QR code?** The UID only connects via Reolink's own, undisclosed protocol through the Reolink servers. And a port forward on the router exposes the camera openly to the internet – this is not recommended.

**What you need:** at the remote location, a device that is always running and can do VPN – usually the router itself (e.g. FRITZ!Box), otherwise a small computer (Raspberry Pi, NAS). On this PC, the matching VPN program. Important: The network at the remote location must have a different address range than your own (e.g. 192.168.178.x there, 192.168.0.x here) – otherwise the PC does not know which device is meant.

**Route A – FRITZ!Box at the remote location (WireGuard, easiest):**

1. Sign in to the FRITZ!Box at the remote location: Internet → Permit Access → VPN (WireGuard) → "Add

connection".

2. Choose "Connect a single device", assign a name (e.g. "TangoDown-PC"), finish and download the configuration file (or use the QR code).
3. On this PC, install "WireGuard for Windows" (wireguard.com), "Import tunnel(s) from file" → choose the file → "Activate".
4. In TangoDown: Webcams & video → Video Center → " + Camera" → enter the camera's address in the remote network (e.g. 192.168.178.40; shown in the Reolink app under device information → IP address) → credentials (stored in the Vault) → "Test".

**Route B – Tailscale (any router, with a Raspberry Pi or NAS on site):**

1. On the device at the remote location, install Tailscale and set it up as a "Subnet Router": `tailscale up --advertise-routes=192.168.178.0/24` (address range of the remote network; on Linux, turn on IP forwarding first – see the Tailscale guide "Subnet routers").
2. In the Tailscale admin console (login.tailscale.com), approve the route for this device ("Edit route settings").
3. On this PC, install Tailscale, sign in with the same account and turn on "Use Tailscale subnets".
4. In TangoDown, create the camera with its address in the remote network, as in Route A.

**Route C – other routers:** Many routers (e.g. from Asus, TP-Link, Ubiquiti, OpenWrt) have a built-in WireGuard or OpenVPN server. The steps are as in Route A: turn on the server on the remote router, create access for this PC, import it in the VPN program, create the camera by address.

**Checking:** When the VPN is active, "Test" in the Video Center or the 🪄 assistant must find the camera. If it does not work: check the VPN connection in the VPN program, compare the address ranges (they must not be the same), look up the camera address in the Reolink app.

**TangoDown and network route:** Addresses of private networks and VPNs (including Tailscale 100.64.x.x and *.ts.net) never go through Tor or a proxy and are not blocked by the kill switch – the camera stays reachable even when Tor is turned on for research. The camera's credentials are kept only in the Vault.

### ⌖ Single-target scan (authorized)

**Purpose:** For commissioned assessments (e.g. a pentest, checking your own servers, an assignment from a company), determine the **open ports of a single target** – with service, software identifier (banner/HTTP header) and TLS certificate.

**Only with an assignment:** Required are the **client** (the authorized party, e.g. owner/operator), **assignment/case number**, **valid until** and the confirmation that a **written assignment** exists for exactly this target and this scope. Without an assignment, a port scan may be a criminal offense and may breach the network operator's contracts.

**Limits (deliberate): exactly one target** (one IP or one hostname – no networks, ranges or lists), at most **1024 ports**, only connection setup and banners – **no exploitation of vulnerabilities**. **Never via Tor/proxy** (scans through other people's exit nodes are abusive): use the "Direct" connection route or a VPN. Air gap, VPN requirement and query lock block it.

**Steps:** Target, port selection (presets: common services, web, remote access, email, databases – or your own list such as "22,80,443,8000-8100"), assignment details → "⌖ Start scan". Result: open/closed/filtered, and for each open port the service, software, banner or certificate. **" + Add as element"** creates the IP (and hostname) with the services as "Service / port" items. Start, assignment and result (with SHA-256) are recorded in the audit log; earlier scans of the case remain available.

### ⇄ Remote access

**Purpose:** SSH, SFTP and RDP to your own servers. Credentials only in the encrypted Vault. Transfer files by dragging (also between two servers), dock sessions side by side.

**Symbols:** Each connection you create shows its kind – green "SSH" (console, plus files via SFTP) or blue "RDP" (remote desktop). Plain FTP is deliberately not included: it transfers passwords unencrypted – files are transferred securely via SFTP.

### › Terminal

**Purpose:** TangoDown commands (e.g. netz, chain, fall, audit), PowerShell, Command Prompt and Linux shell (WSL) side by side.

**Usage:** Chain commands with pipes: source | filter | output, e.g. `entities --type domain | where rel~A | graph new "Domains"` or `entities | count typ | chart`. Other outputs: table, JSON, CSV, copy, map (`map`), chart (`chart`). `datei <pfad>` analyzes captures and logs. Save results as a variable (`$d = …`), jobs in the background (`… &`, `jobs`, `cancel`), macros (`macro rec/stop/run`). `explain` shows in advance which query would go out; `doctor` checks case, audit chain, network route, AI and Vault.

**Real terminal:** `pty powershell|cmd|wsl` or "+ Shell" → "… · Terminal" opens a real terminal: full-screen programs such as vim, nano, htop, ssh with password prompt, colors, Ctrl+C cancels. Ctrl+Shift+C/V copies or pastes. Only opening and closing are recorded in the audit log, no input or output.

**Tab completes (as in Windows and Linux):**

- In the **TangoDown console**, Tab completes:
  - commands
  - fixed values (e.g. `shell pow` → `shell powershell`, `bus o` → `on` / `off`)
  - module names for `open` / `pop`, types after `--type` and variables (`$…`)
  - tools for `dt`, macro names
  - field names of the last output for `where` / `select` / `sort` / `count`
  - file paths for `datei` or when you type a path (`C:\…`, `.\…`, `~\…`)
- In the **system shells** (PowerShell, CMD, WSL), Tab completes files, folders and commands in the shell's current folder:
  - **PowerShell** uses its own completion, including for parameters such as `-Recurse`.
  - **WSL** uses bash's completion.
  - **CMD** knows built-in commands and all programs on the search path.

If the match is unique, it is inserted; folders end with `\` or `/`, names with spaces get quotation marks. If there are several, the common beginning is completed and all options are listed below. Tab only suggests and never runs anything. In the **real terminal** ("▣ … · Terminal"), the shell's own Tab completion applies.

**AI command assistant:** `frag which domains do we have?` – the AI (without AI: built-in rules) suggests a command line, which is placed in the input. It only runs when you press Enter.

**Repeat and recording:** `replay [n]` runs the session's last commands again – queries that go out are skipped. `record start` / `record stop` places the session as a text document in the case file; passwords, tokens and keys are redacted first. `history <text>` searches the history.

<!-- term-ref -->

### First steps in the console

New to the console? Type `einstieg` – seven short steps with examples to type in (`einstieg 3` jumps to step 3). `help` shows all commands, `help <befehl>` explains one in detail (e.g. `help where`). If you don't know what something is called: `frag show me all domains` suggests a command line.

**How a command line is built:** `Quelle | Filter | Ausgabe` (source | filter | output). The source delivers rows (like a table), each filter changes them, and the output shows or uses them. Example: `entities --type domain | where rel~A | select label,rel | csv`.

**Conditions for where:** `=` equal, `!=` not equal, `~` contains, `!~` does not contain, `>` `<` `>=` `<=` greater/less. Example: `where label~beispiel`. **Queries that go out** (marked with ⇄ in `help`) need an open case, are approved as in the user interface and are recorded in the audit log. `explain <zeile>` shows beforehand what would happen.

### All commands

#### Sources – produce rows

| Command | What it does |
|---|---|
| `entities [text] [--type domain]` | Entities of the case (full text across label, details, notes) · also: ent, suche, find |
| `links` | Links in the case |
| `evidence` | Evidence captures (web captures) · also: beweise |
| `audit [n]` | Audit log entries |
| `alerts` | Alerts (watchlist, geofence, situation picture) · also: alarme |
| `fall` | Case overview · also: case |
| `netz <ip\|domain\|mail\|url>` | Net intel query · ⇄ queries externally · also: ip, dns, whois |
| `dt <werkzeug> <domain\|ip> [--graph]` | Domain tools: lookalike, tracking, reverseip, dnshistory, mailsec, cert, web, wayback, dnsbl · --graph creates findings linked in the case · ⇄ queries externally · also: domain, domaintools |
| `chain <adresse\|txid> [--chain eth]` | Chain trace (BTC, ETH/EVM, Tron, Solana, XRP …); returns counterparties · ⇄ queries externally · also: btc, krypto |
| `user <benutzername>` | Check a username on platforms · ⇄ queries externally · also: socmint |
| `datei <pfad> · datei beispiel:pcap\|log\|web` | Analyze a capture/log file locally: addresses, domains, accounts with counts; anomalies as a hint · also: pcap, log |
| `plugin [id] <wert> [--type domain]` | Run your own plugin (without a value: list); result as items in the case · also: plugins |
| `vars` | Saved variables |
| `jobs` | Background jobs (started with & at the end) |

#### Actions

| Command | What it does |
|---|---|
| `capture <url>` | Save a web page as evidence (PNG + MHTML, SHA-256) · ⇄ queries externally · also: sichern |

#### Filters – come after a |

| Command | What it does |
|---|---|
| `where <feld><op><wert> (op: = != ~ !~ > < >= <=)` | Filter rows, e.g. where label~muster · where rel=A1 · also: filter, wo |
| `select feld1,feld2` | only these columns · also: felder |
| `sort [-]feld` | sort (- = descending) |
| `head [n]` | first n rows · also: top, erste |
| `tail [n]` | last n rows |
| `uniq feld` | only one row per value |
| `count [feld]` | count (total or per value) · also: anzahl |
| `table` | output as a table (default) · also: tabelle |

### Output and effect – come at the end of a pipeline

| Command | What it does |
|---|---|
| `json` | output as JSON |
| `csv` | output as CSV |
| `list` | one block per row (for long values) · also: liste |
| `chart [feld]` | Bar chart – uses "anzahl" (e.g. after count feld) or counts per value · also: diagramm |
| `map` | show geolocated entities on the situation map · also: karte |
| `copy [--json]` | to the clipboard (table as TSV or JSON) · also: kopieren |
| `graph add \| graph new "Name"` | Entities into the active or a new subgraph |
| `sel [nr]` | Select an entity (Properties, graph, map) · also: auswahl |
| `fokus [nr]` | zoom in on the graph · also: focus |
| `set feld=wert` | Set a detail on all entities of the input (audit per item) · also: tag |
| `verify · evidence \| verify` | Check the audit chain or re-check evidence hashes · also: prüfen |
| `ki <frage> · … \| ki <frage>` | Question to the AI analyst; input rows are sent along as context · ⇄ queries externally |

### Console

| Command | What it does |
|---|---|
| `help [befehl]` | Overview or help on a command (also: hilfe, ?) |
| `einstieg [1-7]` | guided introduction for new users: step by step with examples to try out |
| `explain <pipeline>` | shows what a pipeline would do (which queries go out) – without running it |
| `doctor` | Health check: case, audit chain, network route, AI, Vault |
| `$name = <pipeline>` | Save the result as a variable ($_ = last output); vars lists all |
| `<pipeline> &` | run in the background · jobs · cancel <nr> |

| Command | What it does |
|---|---|
| `macro rec <name> · macro stop · macro run <name> · macro list · macro del <name>` | Record and play back command sequences (without secrets) |
| `open <modul> · pop <modul>` | Open or pop out a module |
| `shell powershell\|cmd\|wsl` | Open a system shell as its own tab (line by line) |
| `pty powershell\|cmd\|wsl` | real terminal: full-screen programs (vim, htop, ssh), colors, Ctrl+C |
| `bus on\|off` | Show/hide the bus log |
| `history [suchtext]` | Command history (searchable) |
| `frag <was du willst> · ?? …` | AI command assistant: suggests a command line – it only runs after Enter |
| `replay [n]` | run the last n commands of this session again – queries that go out are skipped |
| `record start · record stop` | Session recording; passwords/tokens/keys redacted, placed as a document in the case file |
| `clear` | Clear the screen (Ctrl+L) |

**Keys:** ↑/↓ history · Tab completes · Ctrl+L clears · Right-click on rows and values shows matching actions. <!--/term-ref -->

## ⚿ Vault & connectors

**Purpose:** Store API keys and credentials encrypted and test them; connect your own interfaces as connectors – including agency APIs you are authorized to use. Templates for Shodan, AbuseIPDB, DVLA and your own vehicle interfaces.

**Other stored credentials:** "Other stored credentials" lists all credentials that other areas keep encrypted in the Vault: Proxmox, SSH/RDP, your own cameras, platform accounts, OpenVPN, registers, local databases. The filter at the top finds them too, e.g. "proxmox". "↗" jumps to the responsible area; for Proxmox, "Edit connection" opens directly.

**Your own connectors:** A connector connects a web service you have access to. Configured connectors appear in the right-click menu of matching items; "Test" shows the response. Setup is described in the developer manual.

**Entering keys:** Always enter the key in the "Key" field – it is stored encrypted and never displayed (only the last four characters).

**Shodan:** No separate connector is needed for Shodan. Net intel queries Shodan itself with every IP and domain query – using the Shodan key stored above under "Data sources", otherwise via the free InternetDB. The "Shodan InternetDB" template only takes IPv4 addresses (e.g. 8.8.8.8) and needs no key; "HTTP 404" there means "nothing known about this IP". The **"Shodan host API"** template uses your own Shodan key (paid account or membership) and returns more: organization, provider, operating system, vulnerabilities, data timestamp. A sample plugin "Shodan host lookup (with your own key)" shows the same as a plugin. Location searches ("all devices in Hamburg") are Shodan search queries across many third-party systems and are deliberately not built in.

**Interface for programs and AI assistants:** Your own programs or AI assistants can – if you turn this on – read and add to the open case. Off by default, only on this PC, only with an access key, every access recorded in the audit log. Setup: developer manual.

### ⇌ Connection & cloaking

**Purpose:** Choose the network route (direct, Tor, proxy), exceptions per module, kill switch, check of the exit IP.

**Exceptions per module:** The route at the top applies to the whole app. Below, each module can deviate: **"As above"** (the normal case) follows the choice above, **"Own IP"** always goes direct for this module – even if Tor is chosen above –, **"Always Tor/proxy"** always goes via Tor or the proxy – even if "Direct" is chosen above. The switch is also available in each module (e.g. the "Tor" button in the browser).

**Indicator at the top right: "○ NOT CLOAKED"** means: direct connection – websites and services see your real IP address (shown next to it; hidden in streaming mode). **" 🧅 TOR"** or **"⇌ PROXY"** shows the address websites see instead; **"⛔ BLOCKED"** means nothing goes out. A click opens this module, the tooltip explains the state.

🧅 **Set up the Tor service (Windows):** Instead of keeping the Tor Browser open, TangoDown can set up Tor itself – under "Tor" → " 🧅 Set up Tor service":

- **Two kinds: as a Windows service** (starts with Windows, also runs without TangoDown; Windows asks **once for admin rights**) or **without admin** (TangoDown starts Tor itself and stops it when closing).
- **Origin and verification:** TangoDown asks the Tor Project for the current version and downloads the **Tor Expert Bundle** (only Tor, no browser, approx. 23 MB) from dist.torproject.org. The download goes **through your own connection** – Tor is not there yet; TangoDown asks first. The **Tor Project's signature** is checked against the pinned fingerprint `EF6E 286D DA85 EA2A 4BA7 DE68 4E2C 6E87 9329 8290`. If it does not match, nothing is installed. For the service, all files are hashed again with admin rights after copying.
- **Location:** Service: program in `C:\Program Files\TangoDown-Tor`, data and log in `C:\ProgramData\TangoDown-Tor`, Windows service "tor". Without admin: in the TangoDown data folder under `tools`.
- **This computer only:** Tor listens exclusively on `127.0.0.1:9050` – other devices on the network cannot use it. If TangoDown runs in a VM, set up Tor in the same VM.
- **Afterwards:** TangoDown waits until Tor is connected, switches the connection to "Tor" (port 9050) and checks the exit. Display: " 🧅 Tor service running" or progress in percent; "■ Stop" / "▶ Start" (for the Windows service with an admin prompt; when stopped it stays set up – if the connection is set to Tor, the kill switch blocks until Tor runs again), "↻ Restart", "↓ Update" (latest version, again with signature check), "✕ Remove" (unregister service, delete Tor files; if the connection is set to Tor, the kill switch then blocks until you choose another route).
- **Bridges**, if Tor is blocked on the network: "Snowflake" or "obfs4" (built into the Tor package) or your own bridge lines from bridges.torproject.org. For the service, changing them asks for admin rights again.
- **If there is already another "tor" service** on the PC, TangoDown does not change it – if it runs on port 9050, "↻ search" is enough.

🔄 **Control Tor** (under "Tor", as soon as the connection is set to Tor; via the control port of the installed Tor service 9051 or the Tor Browser 9151, local only, authentication by cookie file):

- 🔄 **New identity:** Tor builds new paths, TangoDown closes the open connections of all its own sessions (queries, browser, web capture), immediately checks the new visible IP and records it in the case log. Tor

allows this at most every 10 seconds. Also in the status bar ("🔄 New Tor ID", right-click opens the controls) and via Ctrl+K.

- **Current path:** entry → middle → exit with name, IP and country – websites only see the exit.
- **Exit country:** quick choice (automatic, Germany, DACH, EU countries, USA, Netherlands, Switzerland) or your own country codes; plus countries through which Tor should **never** exit. "Permanent" remembers the choice and sets it again after every start of Tor; otherwise it applies until restart. After a change, TangoDown fetches a new identity right away. Note: few countries = few exits – slower and easier to recognise.
- **New identity on every case switch** (switch): research from different cases then does not come from the same Tor exit.

🛡 **OpenVPN:** "+ .ovpn profile" stores your VPN provider's profile file **encrypted in the Vault** (profiles with scripts such as `up` / `down` / `plugin` are rejected for security reasons). "Connect" starts the **installed client** – OpenVPN GUI (Community) or OpenVPN Connect, selectable or automatic; the client asks for the sign-in details itself. "⏏ Disconnect" ends the connection. OpenVPN reroutes the **whole computer**; Tor/proxy can be used in addition.

**VPN requirement:** If it is on, TangoDown checks every 10 seconds whether a VPN adapter is active – **without a tunnel, all outgoing connections are blocked** (like the kill switch; local targets remain reachable), with the reason in the status display. If the VPN drops, blocking starts immediately.

### ◇ Types & symbols

**Purpose:** Your own entity types with fields and symbols, extend built-in types, icon packs.

### ⛓ Audit log

**Purpose:** Every work step is traceable; a later change would be noticed immediately.

🔐 **Audit checkpoints (optional, can be turned off):** When a case is closed, when a report is created and on export, TangoDown sets a **signed audit checkpoint** – a kind of seal on the current state of the log. If the log is changed later, "🔐 Checkpoints" shows it. If you wish, TangoDown also fetches a **timestamp** from an external timestamping service (only a checksum leaves the computer, no case data). Both can be turned off under "🔐 Checkpoints" (administrator). **Cases without logging** (free mode) get no audit checkpoints.

**Important:** An audit checkpoint shows that the log has not changed since that point in time – not that the contents are correct.

### ⓘ Help & info

🩺 **Diagnostic report:** "Help & info → Contact → 🩺 Create diagnostic report" (or Ctrl+K "Diagnose") saves a text file for support. It contains the version, system, the error log of this session and an overview of the settings. Keys, passwords and case data are not included. Your own details such as user, computer name, paths, IP and accounts are always masked, even without streaming mode. Look at the file yourself before sending it.

🧭 **Setup check:** On first start (and at any time via Ctrl+K "Setup check"), a traffic light shows what should be set up: privacy, security keys, network route, automatic backup, streaming terms, video tools, AI, API keys and updates. "↗" jumps straight to each one. Nothing is changed automatically.

**? on every area:** The "?" at the top right of every tab header jumps in the manual to exactly the heading of the active module and briefly highlights it.

⚙ **Features & updates:** Turn face matching on/off; **update address** (https address of the version file `latest.json`, which is created next to the installers during the build); **"⇪ Check for updates"** compares the version and shows the download address and SHA-256; **"✓ Check download"** checks a downloaded file against the checksum (from the version file or a `SHA256SUMS-….txt`) – only start it if it says "Checksum matches". TangoDown never installs anything itself. **Signed:** the version file from tangodown.eu carries the publisher's signature; TangoDown checks it with its built-in key and shows "🔐 Signed by the publisher". If it is missing or does not match, TangoDown warns and offers no download – the website may have been tampered with. If the update address has already been entered by the publisher (it then shows in the field), you don't need to set anything – just "⇪ Check for updates" now and then.

⇪ **Notice about new versions:** At the first start, TangoDown asks once whether it should inform you about new versions. With "Yes" it asks tangodown.eu at start and every 12 hours only for the latest version number – no data about you or your cases; can be turned off under "⚙ Features & updates → Check for updates at start". If a newer version exists, a notice appears at the bottom right: **"⇪ Update now"** downloads the matching file (installer, or for the portable edition the portable file), checks it against the signed checksum and then offers **"▶ Start installer"** or **"▶ Start new version"**; TangoDown closes, the open case is saved. The portable edition is always called `TangoDown-Security-portable.exe`. On update TangoDown replaces the running program file **under its existing name** and restarts (an older file with a version number in its name is renamed once to `TangoDown-Security-portable.exe`) – shortcuts, start menu and taskbar entries stay valid, the old version goes to the recycle bin. "Later" reminds you at the next start, "Skip this version" only at the next newer one. If the checksum does not match or the signature is missing, nothing is started. If the check reports "HTTP 404", no version has been published on the website yet; "temporarily suspended" means the operator has paused updates. **Admin update key:** If you run the website yourself, you can suspend updates for everyone there and still update yourself: create a key in the website admin under "Security & settings" and paste it here under "Admin update key". It is stored encrypted, never shown and only sent to the configured update address.

**Other documents:** In the manual area, the tabs **"🔒 Privacy"** (what stays local, what goes to whom and when, responsibility under the GDPR) and **"⇄ External services"** (each service with its purpose, the data sent and whether a key is needed). Please report security vulnerabilities confidentially to info@tangodown.eu.

**Purpose:** Version, contact and ways to get help. It also shows the transparency note: **designed, directed and tested by Lars Stahl – AI-assisted implementation**. With the developer's photo and LinkedIn profile, "🌐 tangodown.eu" (official website: downloads, news, plugins), "✉ Write email" to **info@tangodown.eu** (for questions and bug reports – please include the version, do not send any case data) and buttons for the manual, terms of use, demo, and Data & migration. Found in the sidebar under "Administration" or with Ctrl+K "Help". Under **"♥ Support the project"** you'll find ways to donate (Bitcoin, Ethereum, USDC via Ethereum/Polygon/Avalanche/BNB Smart Chain or via Solana (separate address each), XRP, PayPal) – copy the address or scan the QR code with your wallet app; voluntary, use remains free of charge.

## § Terms of use & disclaimer

**When:** The terms of use appear on first start (in the Agency edition after the first sign-in per user account) and after every new version. You cannot use TangoDown without agreeing; "Decline and exit" closes the program.

**In short:** TangoDown is a free hobby project with no warranty. Updates can change features, plugins, interfaces and connectors; there is no control over third-party services and interfaces; you are responsible for lawful use and for backing up your data. TangoDown is protected by copyright (© Lars Stahl): free use and passing it on unchanged are allowed – decompiling, reverse engineering (including with AI), modifying, circumventing protection measures and selling are not. Please build extensions via plugins, connectors and the program interface.

**Read again:** at any time in the manual tab "§ Terms of use", under "ⓘ Help & info" or with Ctrl+K "Terms of use".

## ⛨ Administration · ◐ Design

**Sprache · Language:** Under "◐ Design" you switch the interface to **English**, instantly and without a restart. The choice also applies to the unlock window of the portable edition at the next start. Menus, buttons, hints and tooltips are translated. Case data, inputs and reports stay unchanged. **The manual, developer guide, legal texts, shortcut overview and PDF export** then also appear in English; the "?" jumps to the matching place in the English manual. Messages from the background service, native menus (e.g. the right-click in the browser) and the **AI's answers** (AI analyst, AI research, AI web search, assessments) also follow the selected language. AI answers and case data are never rewritten word by word – quotes, names and source texts stay as they are. The English translation was created with AI and may contain errors; TangoDown points this out when you switch. If in doubt, the German text applies.

**Readability of grey text:** Under "◐ Design" the slider **"Readability of grey text"** sets how bright hints, explanations in menus (e.g. on the right of "🖒 Save page") and secondary labels are everywhere – from dark to bright, instantly and also in detached windows. "Default" resets the value.

**Colours:** Under "◐ Design → Colours" you can freely choose **headings** (category and section titles such as "Search & meta"), **text**, **background**, **surfaces**, **lines**, **warning**, **error** and **OK**; quick choice "Headings in accent colour" or "bright". "Default" resets one colour, "↺ All colours to default" all of them. Takes effect immediately, also in own windows, and only on this computer.

**Forgot password (Agency edition):**

- **Normal account:** An administrator sets a new password under "⛨ Administration → Users & roles → Edit" (and resets 2FA if the phone is lost).
- **Administrator access lost:** When the Agency edition is activated, TangoDown shows a **recovery key once** – print it and keep it safe (e.g. in a safe). On the sign-in screen, **"Forgot password?"** → enter the key, admin user name and new password. The account becomes active again, its 2FA is reset, and you immediately get a new key. Administrators can generate a new key at any time under "⛨ Administration → Recovery key".

🔐 **Two-factor sign-in (2FA, optional per account):** "⛨ Administration → Two-factor sign-in → Set up 2FA", scan the QR code with an authenticator app (Microsoft/Google Authenticator, Aegis, 2FAS …), enter the 6-digit code. TangoDown then shows **10 recovery codes** – each works exactly once, in case your phone is missing. At sign-in TangoDown asks for password **and** code. A code cannot be used twice.

**What 2FA protects:** the sign-in – e.g. if someone has picked up your password. The case data itself is encrypted anyway (Windows account or master password).

**What for:** users, roles, four-eyes approvals, report branding; appearance (**Contrast** or **Calm** – also switchable at the top of the title bar), font size, colors.

## ◉ Streaming mode (privacy when presenting)

**What for:** You want to present, stream or record TangoDown or share your screen without showing your own details. In streaming mode certain of your own details are replaced by ▒▒▒ in TangoDown's texts – not in images, maps and videos, and not the case data.

⚠ **Not complete protection – check yourself:** Streaming mode is an **aid**, not a guarantee. It only hides certain of your own details in text (list below) and only as far as it recognizes them. **Much is not hidden** (see "Limits") – above all images, maps, videos and the case data itself. So before every stream, recording or screen share, check

yourself what is visible, and if in doubt only show a demo case with fictitious data.

**What it does not change:** It affects **only the display**. Data, inputs, copying, export, reports, evidence capture and all queries stay unchanged – a report or export therefore contains the real values. If you copy a hidden value, the real value ends up on the clipboard.

**Turn on and off:**

- **Ctrl+Alt+S**, in any window.
- Click **"○ Streaming"** at the bottom of the status bar. When on, it shows **"◉ STREAMING"** in red, so you can always see that the protection is active.
- Ctrl+K → "Turn on streaming mode".

The state is kept after a restart. **What is meant to be hidden automatically** (do not rely on this blindly – the mode does not recognize every representation, spelling or place; always check the view yourself):

- your Windows user and computer name as well as folder paths containing your user name
- your sign-in name in the program
- your IP addresses (network adapters and outgoing internet connection) and the location according to the outgoing IP
- signed-in names and stored users of the platform accounts
- your own servers and remote access, your own cameras
- the details from the report header: organization, address, contact
- optionally all addresses from home or company networks (10.…, 192.168.…, 172.16–31.…)

**Custom terms:** Under "◐ Design → Streaming mode" you can also enter everything else that should not be visible, one term per line: name, street, town, email, phone number, company name. Upper and lower case don't matter; short terms are only hidden as a whole word. The list is stored encrypted. There you can also see how many of your own details were detected per area. Only the count is shown, never the values.

**You choose what is hidden:** Under "◐ Design → Streaming mode" each area has a checkbox, e.g. own IP, location, platform accounts, report header, custom terms. If you uncheck one, that area stays visible, for example if you deliberately want to show the report header. With **"Also obscure labels in the graph"** names in the graph are hidden too. An image of the graph for the report always contains the real names.

**Where it works:**

- in all modules and popped-out windows: texts, tables, tooltips, hints
- in desktop notifications
- if you want, also in web pages: TangoDown browser, walls, video tiles, sign-in windows of the platform accounts

Input fields containing your own details are **blurred**; their content is kept.

**Limits:**

- **Images and graphics are not hidden:** photos, screenshots and evidence-capture images, captured web pages (MHTML), document and PDF previews, map tiles, videos, camera images and monitoring walls (except the optional web-page masking), faces and QR codes.
- **Case data is not hidden:** names, addresses, number plates, accounts etc. of persons and companies **in the case** stay visible – the mode only knows your own details and the terms you enter yourself. Graph labels only if "Also obscure labels in the graph" is on.
- **It does not work outside TangoDown:** windows of other programs, Windows notifications of other programs, the taskbar, file dialogs (Open/Save show folders and file names), browsers outside TangoDown.
- **Only recognized spellings:** differing spellings, abbreviations or typos of a term are not recognized; newly appearing content can be visible for a moment before it is hidden.
- Before streaming, check the view you want to show – ideally with a test recording.
- If your user name is an ordinary word, that word is hidden everywhere it stands on its own.

### ✪ Demo mode

**What for:** Automatic demo run through all modules – for presenting or recording a video.

**Quick version:** "⚡ Quick version: a case step by step" shows a single connected case in about three minutes – lead (license plate) → research with a hit → enrich data → connections in the graph → AI evaluation with evidence → evidence capture → report. Every click is zoomed in and made visible, every result shown large and explained in simple words. Ideal for viewers who don't know TangoDown yet.

**Demo case "From license plate to company":** "🚗 Demo case: from license plate to company" shows an investigation chain in nine explained steps in about six minutes – with visible clicks, right-clicks and chosen actions: **1.** A license plate is checked in Vehicle matching against your own databases – hit with owner; "Into the case with links" adds vehicle and owner. **2.** Right-click the owner in the graph → "Search own databases" → open the hit → "⇢ Into the case with links": the home address is added. **3.** Right-click the address → "Show on map": Geo-Intel. **4.** Right-click the owner → "Search all cases": open the hit in the company directory and add the company together with its domain. **5.** SOCMINT "Company / website" reads the company website: official profiles, legal notice – and under "Contact" a Bitcoin address. **6.** Chain-Trace shows the money flow of this address as a flow diagram and explains the transactions (fictitious data). **7.** After approval, Bitcoin Discovery finds a Reddit account that names the address as its own donation address – a profile the website does not link to; it is added to the graph as a possible identity. **8.** The overall picture in the graph. **9.** The report with preview. All data is made up; the company website is a local replica at the reserved address `muster-logistik.example`, which does not exist on the internet. The demo case is created as a separate case "DEMO-KZ-…".

**Open:** Ctrl+K → "Start demo", or the module "✪ Demo mode" in the bar on the left, or at the top of the manual.

**How to use:**

1. **Demo case:** checkbox "Create demo case with fictitious data" – on start, a separate case "DEMO-…" with made-up people, company, vehicle and events is created (your current case stays unchanged).
2. **Pace:** calm, normal or brisk.
3. **Modules:** click all or individual modules (chips).
4. Check or uncheck **full screen**.
5. **"▶ Start demo"** – the estimated duration is shown on the button. **Personal details are replaced:** user and computer name, paths, public IP, your own servers and cameras. Esc ends, Space pauses (then "⏸ PAUSED" appears clearly at the top; Space again = continue). The demo runs in the main window: each module is

enlarged behind the title card and closed again afterwards – at the end your workspace looks as it did before.

**What the demo shows:** real actions instead of still images – right-click menus in the graph and on the situation map, a transformation (DNS) whose results are pulled up and named in the graph, placing tanks and shrinking them with Alt+mouse wheel, selecting symbols (also with a Ctrl frame) and moving them, drawing an arrow, drawing a geofence, moving it, enlarging it and saving it, zooming and panning the map, changing the map style, searching your own objects, live air traffic, SSH/SFTP on the local demo server, PowerShell, CMD and – if set up – WSL (Linux) side by side, the sandbox with demo VMs. In the Webcams section four public live cameras run (Tallinn, Tokyo, Namibia); the monitoring wall "Demo situation center" shows them at the same time; the wall is removed again afterwards. If no AI is set up, AI research and AI analyst show a sample answer clearly marked as **DEMO-SIMULATION**.

**Topic demos (in English):** Under "Topic demos" each button starts a short demo on one topic – each with its own demo case ("DEMO-…"). The interface runs in English during the demo and is switched back to your language afterwards.

- ⚑ **Alerts & situation picture:** set up an alert for #hamburg and for Berlin, pause and edit alerts in "My alerts", an incoming area alert with its source, situation picture: clicking a signal flies there, clicking a circle shows the evidence, live sighting of an aircraft or ship into the graph. The situation data is fictional and is fed into the demo case without any outside connection; the alert rules are paused at the end.
- 👤 **From a name to the picture:** a public person (Donald Trump) into the graph, web search and profile search via right-click (e.g. truthsocial.com), the AI adds accounts, companies and offices, a public-domain photo goes onto the element and is matched locally against the face demo set. This demo queries the internet live; if a search returns nothing (e.g. bot protection), it adds publicly known facts – marked as demo.
- ✦ **Working with AI:** the two switches (Where from: case · internet · case + internet; How: answer · plan with approval · recurring) with examples. Without a configured AI, answers clearly marked as **DEMO SIMULATION** appear.
- ▤ **Social Deck:** column for #osint, trends, post into the case, filter, network route.
- ▦ **Video walls & live streams:** webcams, save a still, camera pool, monitoring wall, record a live stream (needs yt-dlp and ffmpeg).
- 🌐 **Built-in browser:** own session and network route, save page, take findings, crypto address, clip/REC/archives, self-check, page source – on a local demo website (127.0.0.1).

## ⧈ Sandbox & VMs

⚠ **Tip – back up first:** Before you connect Proxmox, Hyper-V or VirtualBox to TangoDown or control existing VMs with it, create a **complete backup of your existing VMs** and keep it **outside** the host (another drive, NAS, external storage) – in case of a malfunction in TangoDown or an operating error.

- **Proxmox:** Datacenter or node → **Backup** (vzdump) or Proxmox Backup Server, target outside the host.
- **Hyper-V:** Hyper-V Manager → VM → **Export**.
- **VirtualBox:** File → **Export Appliance** (or copy the VM folder while the VM is powered off).
- **Snapshots alone are not a backup** – they are on the same storage as the VM.
- Set up access only with the permissions you need (e.g. Proxmox **PVEAuditor** for viewing only).
- Before relying on the backup, check once that it can be restored.

**Proxmox shows no VMs?** Proxmox simply returns an empty list to an access without permissions. TangoDown now tells you this directly. This is how you grant the permissions in Proxmox:

1. Datacenter → Permissions → Add → **API Token Permission**, choose the token TangoDown uses (shown under the provider, e.g. `tangodown@pam!sandbox`). Important: If the token has "Privilege Separation" (Proxmox default), **only the token's permissions** count. The user's permissions alone are then not enough.
2. Path **/**, role **PVEAuditor** (view only) or **PVEVMAdmin** (start, snapshots, clone), check "Propagate".
3. In TangoDown, "Refresh".

**Change access:** click **"✎ Access"** on the provider (or right-click → "Edit connection"). There you change the address, token ID and token secret. If the secret is left empty, the existing one is kept.

**What for:** Control analysis and lab VMs in one place – without switching between Proxmox, Hyper-V Manager and VirtualBox.

**+ New VM (VirtualBox):** from an ISO on this PC, e.g. Ubuntu 24.04 Desktop, Debian, Kali or Windows 11. The dialog contains links to the official downloads.

- **Unattended install:** VirtualBox sets up user, password and Guest Additions by itself (Ubuntu, Debian, Windows). Otherwise you install it yourself in the console.
- **Sandbox defaults:** clipboard and drag & drop off, optionally without network, otherwise NAT. Windows 11 gets TPM 2.0.
- Your existing VMs stay untouched; newly created ones count as created by TangoDown and can be discarded.

**+ New VM (Proxmox):** creates a fresh VM.

- **☁ Ready-made image (fast):** Ubuntu 24.04 LTS, Ubuntu 22.04 LTS, Debian 13 or Debian 12. Proxmox downloads the official cloud image itself; before that, TangoDown fetches the checksum from the vendor's site, and Proxmox verifies it while downloading. Cloud-Init sets up user, password and/or SSH key as well as networking via DHCP. The VM is ready after about one minute. An image is downloaded only once and reused afterwards.
- **💿 Install from ISO:** empty disk and an ISO from the Proxmox storage, e.g. Ubuntu Desktop, Kali or Windows. You do the installation in the console (🖥).
- **Settings:** vCPU, RAM, disk size, storage, network bridge, "Network disconnected", snapshot "clean", start afterwards, assign to the case.
- **Requirement for images:** A storage must allow the content **"Import"**. In Proxmox: Datacenter → Storage → local → Edit → add content "Import". The token needs permission to create VMs, e.g. the role PVEAdmin on "/".
- New VMs count as created by TangoDown and can be discarded here again.

**⚙ VM settings:** click the VM → "⚙ Settings …" (or right-click the card).

- **Changeable everywhere:** name, vCPU, RAM and description.
- **Proxmox:** additionally "Start with host", deletion protection and QEMU guest agent. For a running VM, CPU and RAM apply from the next restart.
- **VirtualBox and Hyper-V:** name, CPU and RAM only when the VM is powered off.
- **VirtualBox, also while running:** clipboard and drag & drop (for a sandbox "off"); shared folders can be removed.
- **Everything else** (disks, graphics, USB, network adapters): "↗ Proxmox interface", "↗ VirtualBox Manager" or "↗ Hyper-V Manager".

Every change is recorded in the VM log.

🌐 **Proxmox interface:** right-click the provider → "Open Proxmox interface", either in the TangoDown browser or the system browser. The TangoDown browser accepts the self-signed Proxmox certificate only if it exactly matches the pinned one.

**Transfer a file into the VM (VirtualBox):** The target folder is created if needed. The default is `C:\Users\Public\Analyse`, where every user may write. If access is denied in the guest, TangoDown tells you which folder works instead.

**Add a provider:**

- **Proxmox VE:** for detailed instructions see "Connect Proxmox – step by step". In short: "＋ Proxmox" → address (e.g. `https://pve.lan:8006`), token ID (`benutzer@pve!tokenname`) and token secret. In Proxmox, create a separate user with an API token for this and give it only the role it needs (PVEVMUser for start/stop and console, PVEVMAdmin also for snapshots) – not root@pam. On the first request, TangoDown shows the checksum (SHA-256) of the server certificate – a character string, not a fingerprint sensor. Compare it with Proxmox (Node → System → Certificates → "Fingerprint") and click "Trust". If it changes later, the connection is blocked.
- **Hyper-V / VirtualBox on this PC:** appear as a button if they are installed. Hyper-V requires the group "Hyper-V Administrators".
- **Demo:** made-up VMs to try things out.

**How to use:** Cards show status, CPU, RAM and uptime. ▶ start, ⏻ shut down cleanly, ⏸ pause, 🖥 console (in the app; Hyper-V: vmconnect), 📸 snapshot, ⚑ assign to the open case. Clicking a card shows snapshots (revert, delete) and the history; right-click opens the menu with all actions.

**Analysis VM for the case (clone of a template):** Right-click a clean VM → "Mark as template for analysis VMs" (🧩). Then at the top "♻ Analysis VM for the case": choose a template, a name is suggested (TD-case number-date), checkboxes for linked clone, disconnect network, snapshot "clean" and case assignment. Proxmox makes linked clones only from real Proxmox templates, otherwise full clones; VirtualBox links via the template's current snapshot; Hyper-V cannot clone (yet). Such analysis VMs (♻) can be permanently deleted after the examination with "Discard analysis VM" – TangoDown never deletes other VMs.

**Network:** Every card shows 🔌 "no network" or 🌐 "Network". One click disconnects all network adapters (Proxmox: link_down, VirtualBox: unplug cable, Hyper-V: disconnect from switch) or reconnects them (with confirmation).

**File into the VM (⇪):** Choose a file, enter a target folder – the SHA-256 goes into the log. Only into running VMs. Hyper-V needs the guest services, VirtualBox the Guest Additions and a sign-in in the guest (stored in the Vault on request), Proxmox the QEMU guest agent (small files only, up to 45 KB).

**Analyze in sandbox ( 🧪 ):** In File forensics choose a file → "🧪 Analyze in sandbox". Choose a template (for VirtualBox the guest sign-in) and "▶ Prepare analysis VM": TangoDown clones the template (network disconnected, snapshot "clean", assigned to the case), starts it, copies the file into it (the SHA-256 is compared with forensics) and opens the console. After the examination: "⇩ Result to files" fetches a file from the VM (e.g. a report) with SHA-256 into Case files & documents, "✎ Finding" creates a note in the case and in the report, "✕ Discard VM" deletes the analysis VM. Hyper-V cannot read files from the guest, Proxmox only small ones.

**Security:** A VM is only a sandbox with a blocked or isolated network, without shared folders and without a shared clipboard. Take a snapshot before every analysis and revert afterwards. Every action is recorded in the VM log and, with an open case, in the audit log; Proxmox tokens are stored only in the Vault.

**Console in the app:** 🖥 opens the VM's screen directly in the sandbox area. Proxmox: full-featured (mouse, keyboard, Ctrl+Alt+Del, paste) – the connection uses the API token from the Vault and the confirmed certificate; no Proxmox sign-in in the browser is needed. VirtualBox: live image about every second, typing text and special keys (Enter, Esc, Tab, arrows, Ctrl+Alt+Del); for the mouse use "⧉ Separate window". Hyper-V still opens vmconnect. Inputs are not logged, only the fact that the console was used.

### ⧈ Connect Proxmox – step by step

**What for:** Control analysis VMs on a Proxmox server from TangoDown: start, snapshots, clones for analyses, file in, result out, console in the app. For this, TangoDown uses its own restricted access – never the administrator account.

**In Proxmox (web interface, as administrator):**

1. **Create a user:** Datacenter → Permissions → Users → "Add". User name e.g. `tangodown`, realm "Proxmox VE authentication server" (pve). TangoDown does not need a password.
2. **Create an API token:** Datacenter → Permissions → API Tokens → "Add". User `tangodown@pve`, token ID e.g. `td`. Leave the "Privilege Separation" checkbox checked (the token only gets the permissions you give it). **Copy the displayed secret right away** – Proxmox shows it only once.
3. **Grant permissions:** Datacenter → Permissions → "Add" → "API Token Permission":
   - Path `/vms` (all VMs) or `/vms/<Nummer>` (only specific VMs), token `tangodown@pve!td`.
   - The role **PVEVMUser** is enough for starting, stopping and the console.
   - The role **PVEVMAdmin** is needed for snapshots, clones and disconnecting the network.
   - For clones additionally: path `/storage/<Speicher>` (e.g. `/storage/local-lvm`) with the role **PVEDatastoreUser**.
4. **Note the fingerprint:** Node (e.g. `pve`) → System → Certificates → select the certificate → "View Certificate" → "Fingerprint (SHA-256)". You will compare it in TangoDown in a moment.

**In TangoDown:**

1. Tools → Sandbox & VMs → "+ Proxmox".
2. Enter the address, e.g. `https://192.168.178.10:8006` (always https), token ID `tangodown@pve!td`, paste the token secret → Save. After that, the secret is stored only in the Vault.
3. On the first request, TangoDown shows the **checksum of the server certificate** – compare it with the fingerprint from Proxmox and click "Trust". If the certificate changes later, TangoDown blocks the connection (protection against substituted servers).
4. The VMs appear as cards. For analyses: set up a clean VM (install tools, disconnect the network if needed), shut it down and mark it in TangoDown as "🧩 Template". Every analysis then starts on a copy.

**Common errors:** "API token rejected" → token ID or secret wrong (format `benutzer@pve!tokenid`). "No permission" → role or path from step 3 is missing. "root@pam" is deliberately rejected – use a separate user. Unencrypted http is rejected (except on this PC). Make Proxmox reachable only via VPN or in your own network, never openly on the internet.

## ✉ Email analysis

**What for:** Check suspicious emails (.eml, .msg from Outlook): Who really sent it, which servers did the mail pass through, is the sender genuine – and how do you recognize fraud?

**How to use:** "📂 Analyze email …" or drag the file here (from Outlook: drag the mail to the desktop, then into TangoDown). "✉ Example (phishing)" shows a typical fraud mail.

**Paste headers:** "📋 Paste header …" (or simply Ctrl+V in the area) accepts copied headers or the full source of an e-mail – e.g. from Outlook (File → Properties → Internet headers) or Gmail (⋮ → Show original). It is analysed exactly like a file; headers alone are enough for the delivery path, IPs and SPF/DKIM/DMARC, links and attachments need the full source.

**Result:** sender, recipient, date, Message-ID, reply-to address and Return-Path · authenticity according to the mail server (SPF, DKIM, DMARC) · delivery path from the sender to the mailbox with IP addresses, times and delays · originating IP · anomalies (different reply-to address, display name with a different address, disguised links, risky attachments such as .exe or .pdf.exe, long delays) · all links and attachments with SHA-256 · all headers.

🔍 **Verify authenticity (DNS):** The details "SPF/DKIM/DMARC according to mail server" come from the receiving server and can themselves be forged. This button does its own calculation: the **DKIM signature** is checked cryptographically with the public key of the sender domain (shows whether text or headers were changed after sending), **SPF** is evaluated against the originating IP from the delivery path (with include/redirect, at most 10 lookups), **DMARC** checks whether signature or server match the visible sender domain. Result: **sender confirmed / suspicious / inconclusive**. For this, DNS records of the sender domain are queried (network route, justification if required, audit log). Forwarding and mailing lists can break signatures without anything having been forged.

**Links in detail:** Every link is assessed without opening it – **Punycode** (internationalized names, e.g. "xn--..." is shown readably), **mixed scripts** (Cyrillic "a" in "beispielbank"), **resembles the sender domain** (beispie1bau.example instead of beispielbau.example), **imitates a brand** (e.g. a well-known brand name with "-secure" or "-login" in a foreign domain), **IP address instead of a name**, **disguise with @** (www.beispielbank.example@fremd.example leads to fremd.example) and **short links** (bit.ly & co.). For short links, **"↪ Resolve target"** determines the redirect chain – only the redirects are read; the target page itself is not loaded.

**Attachments in detail (without opening):** Office files with **macros** (including old .doc/.xls), automatic start on opening, externally loaded templates; **PDF** with JavaScript, auto-start action, program launch or embedded files; **ZIP** with content list, executable files inside and **password protection** (virus scanners cannot look inside); **double extensions** (rechnung.pdf.exe), invisible right-to-left characters, **wrong file type** (extension .jpg, content is a program); **forwarded mails** in the attachment are read as well. "▸ Details" shows everything per attachment. **"VirusTotal (Hash)"** looks up the checksum – only the SHA-256 is sent, never the file (your own VirusTotal key under "Vault & connectors"; observe VirusTotal's terms of use).

📬 **Analyze mailbox:** Choose or drag in an **.mbox** (e.g. Thunderbird, Google data export) or **several .eml** files at once. TangoDown reads only the headers and shows **who wrote to whom how often** (with time span and subject excerpts) and all addresses with sent/received; duplicate mails (same Message-ID) count once. **"✉ Communication network into the case"** creates the 80 most frequent addresses as elements and connects them with "writes to (count, time span)" – in the graph you immediately see who is at the center. The name and checksum of the files are recorded in the audit log.

**Into the case:** Sender, reply-to and Return-Path addresses, originating IP and link domains are created as elements and linked to an event for the mail (graph and timeline).

**Protection:** The file is only read; attachments are never opened or executed. Check suspicious attachments in the sandbox. The name and checksum of the mail are recorded in the audit log. Results are leads, not established facts.

### ≡ PCAP and log analysis

**What for:** Analyze network captures (.pcap, .pcapng – e.g. from Wireshark) and log files locally.

**How to use:** "📂 Analyze file ..." or one of the examples. Capture: communication partners (IP addresses), DNS queries, TLS server names, HTTP hosts, connections with packets and bytes; hint at regular contacts at fixed intervals (possible automatic check-in). Logs: web servers (Apache/nginx), SSH/auth.log and general logs – IP addresses, accounts, failed attempts, suspicious requests (.env, .git, wp-login). Clicking a value copies it. "+ Add as elements" creates the file, addresses, domains and conspicuous events as elements – linked in the graph and with a timestamp on the timeline.

**Protection:** The file is only read, never executed or sent. Name and SHA-256 are recorded in the log. Results are leads, not established facts.

## ⚙ Plugins

**What for:** Additional functions for the right-click menu: A plugin receives the value of an element (e.g. a domain) and returns new elements, links or a note. Plugins are written by your IT or a developer (instructions in the developer manual).

**How to use:** In the module "⚙ Plugins" you see all available plugins. New or changed plugins must be enabled with "✓ Review & approve"; "▶ Try it" tests a plugin with a value without writing anything into the case.

**Use:** Approved plugins appear in the right-click menu of matching elements (graph, Properties, tables), in the Terminal and in the Investigation autopilot. Results are linked to the source element; the plugin's name is given as the source.

**Protection:** JavaScript and Python plugins run isolated in the sandbox and cannot access your files, the PC or the credentials. **Exception – local web service:** A plugin of the "http" kind calls a web service on your computer or in your own network (e.g. FastAPI). This service is a separate program outside the TangoDown sandbox – it can do whatever that program is allowed to do on your computer. TangoDown only protects the hand-over: it only receives the value, and its answer is checked as strictly as any plugin answer. Only connect such services from a trustworthy source; the approval points this out. If a plugin needs more – internet access to specific addresses, a stored key or a file you choose yourself – this is stated exactly at approval. Every change to the plugin requires a new approval; every run is recorded in the audit log. Results are leads, not established facts.

**At your own risk:** Installing, approving and using plugins – including from the marketplace – is at your own risk; the plugin's author is responsible for it.

⚠ **Possible risk with keys:** If a plugin asks for a key from the vault (e.g. Shodan), it uses this access **on your behalf** – quota, costs and queries run through your account. TangoDown inserts each key only into requests to the corresponding service (Shodan only to api.shodan.io); the plugin itself never sees it and cannot send it to another server. Still: only approve plugins with key or network access from a trustworthy source. With network access, a plugin can send values from your case to the declared hosts.

**Existing elements:** If a plugin returns an element that already exists in the case (same type and name), TangoDown only fills empty fields. Differing values stay unchanged; a notice "View differences" shows them, and you take them over selectively. The same applies to data import.

**Same names:** If two plugins have the same name, the right-click menu adds the author or ID, and approval shows a warning. Two plugins with the same ID do not both run – the second is shown as faulty.

⟨⟩ **View code:** Every plugin has the "⟨⟩ Code" button: it shows all files (plugin.json, program code, instructions) read-only, with copy and "📂 Open folder". This way everyone can check what a plugin does before approving it, and improve plugins further. In the marketplace on tangodown.eu the code can also be viewed before downloading.

⛔ **Blocked plugins:** The publisher can block plugins in the application if he considers it necessary, e.g. in case of a security problem. TangoDown only loads the block list together with "Check for updates" or the marketplace catalog. A blocked plugin is shown with the reason and can neither be approved nor run.

🛒 **Marketplace:** the "🛒 Marketplace" tab → "⇣ Load catalog from tangodown.eu" shows free plugins with description, guide ("📖") and their permissions in plain words. "⇩ Install" downloads the plugin, checks the **checksum and the publisher's signature** and stores it – it may only run after your approval under "Installed". Unsigned plugins cannot be installed there. Without internet: "📄 Install from file ..." for a `.tdplugin` file (e.g. from the website). When updating, the older version goes to the Recycle Bin.

### ♥ Data source status

**What for:** See at a glance which sources are reachable, which are slow or disrupted, what is blocked (air gap, kill switch) and which keys or providers are missing.

**How to use:** Opening checks immediately; "↻ Check now" repeats. Checked are Net intel (DNS, RDAP), Chain-Trace, live situation (aircraft, ships), Situation picture (GDELT, Mastodon), Wikimedia, RDW, AI and second model, keys in the Vault (only whether stored, never the value), custom connectors, network route and sandbox providers. Each probe is a small status query without case data via the network route of the respective module. Clicking a row opens the module.

### ◧ Workspace templates

**What for:** The right layout for the type of case with one click: license plate case, person research, crypto case, infrastructure & technology, situation center, analysis & report.

**How to use:** At the top "▣ VIEW ▾ " → "◧ Templates" or Ctrl+K → "Template: …". You can then save your own layout as a view as usual.

## Data, migration & portable mode

### 🛟 Automatic backup

**What for:** If the hard drive fails or the PC is lost, all cases are gone without a backup. That is why TangoDown backs up everything once a day, encrypted: cases, vault, settings and custom databases.

**Setup:** "⇄ Data & migration" → " 🛟 Automatic backup":

1. **Choose a target folder**, ideally a second drive, a USB stick or a network drive, not the data folder itself.
2. Set a **backup password** (at least 10 characters). Write it down and keep it separately: without this password, no backup can be opened.
3. Check **"back up automatically every day"**.

**How it works:** The backup runs at startup or as soon as no case is open, at most once every 20 hours. Each backup is test-opened after it is written. The last n days are kept (default 7), plus one backup per week for w weeks (default 4); older ones are removed.

- **" 🛟 Back up now"** backs up immediately. An open case is briefly closed for this and then reopened.
- **If the target is not reachable** (USB stick missing), a notice appears with a jump to the setting.

**Restoring:** Single or all cases selectively via **"↺ Restore …"** (see "Back up & restore" below). Everything at once (including vault and settings, e.g. on a new PC): "⇩ Import migration package" → choose the backup file ( `TangoDown-Sicherung-….tdumzug` ) → backup password.

**⚙ Transfer settings only:** "⚙ Export settings …" creates an encrypted package with appearance, controls, network route, connectors, browser identities, alerts and streaming terms, without cases, vault keys and databases. Meant for a second computer or colleagues. It is imported like a migration package; security-relevant settings are only applied if you explicitly ask for it.

### 🛟 Back up & restore (single or all cases)

**What for:** Bring a case back to an earlier state (e.g. after deleting something by mistake), get single cases out of a backup or back up selected cases separately.

**Open:** Case selection → **"🛟 Back up & restore …"**, in "⇄ Data & migration" → "↺ Restore …" or Ctrl+K "Back up & restore".

**Back up:**

- **"🛟 Back up all cases now"** immediately writes a checked backup of everything (like the automatic backup; target folder and backup password must be set up).
- **"Back up selected cases …"**: tick the cases, enter a password (empty = backup password) and choose where to save. The file contains only these cases including evidence captures, images, documents, videos and audit log – without vault and settings.

**Restore:**

1. Open a backup from the list ("View contents") or any backup or case package (`.tdpack`) via **"📂 Choose file …"**. Without a password entered, the backup password is used.
2. The **preview** shows for each case the file number, title, classification, status and number of elements in the file, and whether the case already exists here and in what state. For case packages also who exported it, when and with which version.
3. Choose for each case:
   - **"import as a copy"** – the case is added as a separate case "… (Sicherung <date>)", the original stays unchanged.
   - **"reset to this state"** – only with a **justification**. The previous state is **not deleted** but stays in the case selection as a separate case "… (Stand vor Wiederherstellung <date>)". If confirmation with a security key is switched on, the YubiKey is required.
   - If the case does not exist here (any more), it is restored.
4. **Custom databases** (backups only): tick which ones to complete – missing entries are added, existing ones stay unchanged.
5. **"↺ Restore selected"**. An open case is closed for this. Afterwards "Open" takes you straight to the case.

**Traceable:** Restoring, resetting and backing up are recorded with file, state and justification in the audit log of the cases concerned. Vault and settings from a backup are never touched here – that is what the migration package is for.

⚠ **Passing on:** Backups and migration packages contain the vault (credentials, API keys) and platform logins. Never pass them on together with the password – the case package is meant for colleagues. Packages are not bound to a computer: anyone who has the file **and** the password can import them. Only import VS-NfD cases on workstations approved for them; the preview points this out.

## ⇄ Where is my data?

In the **"⇄ Data & migration"** module (sidebar "Administration") you see the data folder, the mode and the key protection; "📂 Open" shows the folder in Explorer.

- **Installed version:** `%APPDATA%\TangoDown Security\` – i.e. `C:\Users\<Name>\AppData\Roaming\TangoDown Security\`.
- **Portable version:** folder `TangoDown-Daten` right **next to the portable.exe** (e.g. on the USB stick). If this location is not writable, it uses the normal data folder and tells you so.

That is where your cases, their keys, the stored credentials and API keys, the custom databases, plugins, camera pool, connectors and settings are kept. Everything important is encrypted. Please do not change the folder by hand – to take it with you, use the migration package.

### 🔐 How are the keys protected?

- **Installed – Windows DPAPI:** Windows encrypts the keys with your **Windows user account on this PC**. If the hard drive is stolen or the folder is copied, nothing can be decrypted on another computer. That is why it is **not** enough to simply copy the folder to a new PC.
- **Settings protected:** The settings files (network route, AI, interface, connectors, remote access, cameras, program paths, plugin approvals, SSH host keys, OpenVPN …) are also stored **encrypted and protected against tampering** in the data folder – no longer readable. If one of them was changed, replaced or swapped outside TangoDown, the app does **not** load it, sets it aside as "…manipuliert-…", uses **conservative defaults** (e.g. network route direct, interface off, cloud AI off) and **warns clearly**. Existing settings are converted once on the first start of this version.
- **What stays readable in the data folder – and why:** Since 0.59.2, the subdomain word list, custom map symbols and the **vault as a whole** are also sealed (the names of the services are no longer readable either; the secrets themselves were already encrypted individually). The **deletion log** (`deletions.jsonl`) and **sandbox log** (`vm-log.jsonl`) are encrypted line by line; their hash chain remains verifiable. TangoDown converts existing readable files once on first start. Only `master.json` and `keyring.json` stay readable – that is the lock itself (salt, parameters and **encrypted** keys, no plain text); without them nothing could be unlocked. Cases, custom databases and evidence are encrypted anyway. Folders such as `Cache`, `Local Storage` etc. belong to the built-in Chromium (interface settings, browser cache).
- 🔑 **Security key (YubiKey, FIDO2):** In addition to the master password (portable mode, under "Data & migration") or the account password (Agency edition, under "Administration" → 2FA), a security key can be required. Windows shows its own dialog for this ("Insert and touch the key") – no extra software needed. When unlocking, the list of keys is bound to the encrypted data key: anyone who deletes it from the file does not bypass the key, but can no longer unlock at all. **Key lost:** the recovery key resets the second factor (Agency edition: one-time recovery code or administrator). Ideally set up two keys. Limit: against a targeted attack on the files themselves, a **strong master password** is what protects you most.
- 🔒 **Bind the data key to the YubiKey (stronger, portable mode):** Under "Data & migration" → "Bind data key to YubiKey (stronger)", a secret from the key itself (FIDO2 extension PRF or "hmac-secret") is mixed into the encryption. After that, the data can only be opened with the **master password and a bound key** – even copied files or a modified app do not help without the real key. How it works:
  - **Requirements:** a FIDO2 key with PIN (e.g. YubiKey 5) and a **recovery key** created beforehand – without it the binding cannot be switched on.
  - **Switching on:** enter the master password, "🔒 Bind now". Windows asks twice for PIN and touch; if the key has no PIN yet, you set it during this step. A credential (passkey) for "tangodown.localhost" is stored on the key. The previous "touch only" list is replaced.
  - **Unlocking:** master password, then PIN and touch. A wrong password is reported immediately, before the key is asked.
  - **Bind a second key (recommended):** "+ Bind another key" – first set up the new key (PIN + touch twice), then touch an existing one once. Each key opens on its own (together with the password).
  - **Removing a key:** with the master password. The last key stays – use "Remove binding" for that (password and key needed); afterwards the password is enough again.
  - **Changing the master password** works without the key.
  - **Key lost or PIN blocked:** at start, "Forgot master password?" with the recovery key – this sets a new password and **removes the binding**. Without the recovery key and without a key, the data is **lost for good**.
  - **Keep using the YubiKey elsewhere:** the PIN only applies to the FIDO2 part; OTP, smart card (PIV), OpenPGP and TOTP codes are unaffected. After 8 wrong PIN entries the FIDO2 part locks; resetting it

deletes all passkeys stored there.

- 🔑 **Confirm sensitive steps with the key (optional):** If a security key is set up, you can switch on below that these steps additionally require touching the key: approving a plugin, enabling write access or the on-prem token of the local interface, copying the on-prem configuration and taking over a team sync. This way nobody who sits briefly at your unlocked PC can set up a backdoor unnoticed. Switching it on and off itself requires the key; every confirmation is recorded in the audit log. The key does not check content – whatever comes in via approved plugins or the interface keeps working as usual.
- **Portable – master password:** All keys are protected with your **master password**. This way the data runs on **any** Windows PC – but only with the password. **There is no reset:** if you forget the master password, you can no longer open the data. Ideally store it in a password manager.

### ⇪ Migration package – take everything to a new PC

1. Old PC: **"⇄ Data & migration"** → **"⇪ Create migration package"**, enter a **passphrase** (at least 10 characters) twice and choose the save location. An open case is closed for this.
2. Bring the file `TangoDown-Umzug-<Datum>.tdumzug` to the new PC (USB stick, network drive). Remember or pass on the passphrase separately.
3. New PC: install TangoDown (or start it portably), **"⇩ Import migration package"**, enter the passphrase, choose the package. TangoDown shows the contents (cases, number of keys, size) – only "⇩ Restore now" applies it.
4. **"↻ Restart now"** – done.

**What's included:** all cases with their keys, the whole vault, custom databases, plugins, camera pool, connectors, custom cameras, settings, views, favorites and monitoring walls, users/edition (only on a fresh workstation).

**Also included:** the **sign-ins of the platform accounts** (TikTok, Instagram, X, Facebook, LinkedIn, Telegram) – on the new PC you are signed in right away, as long as nobody is signed in there yet; stored credentials (🔐) come along with the vault. **What's not included:** program paths to **ffmpeg/yt-dlp** (select them again on the new PC or set them up with a click).

**Safe merging:** Existing cases, vault entries and plugins on the target PC are **never overwritten** – only added to. Custom databases are merged. General settings come from the package. **Security-relevant settings** (network routes/proxy, AI providers, REST/MCP interface, connectors, registers, remote access, VMs) come along as long as the checkbox **"Also apply security-relevant settings"** is checked (default). For a package from someone else, uncheck it. **Never applied** are plugin approvals, known server keys (SSH) and consent to the terms of use; these are granted anew on the new PC. The REST/MCP interface is always **off** at first after importing.

**Security:** The package is fully encrypted. A wrong passphrase or a modified file is detected before anything is written. Also suitable as a **backup copy**. Individual cases can still be exported as `.tdpack` in the case overview.

## 🪫 Portable mode (USB stick)

1. Copy the file `TangoDown-Security-<Version>-portable.exe` to the stick and start it **there**.
2. On first start, **"Portable mode"** appears: set a **master password** (at least 8 characters) (twice). If this PC already has data from the installed version, you can check **"Take over existing data from this PC"** – it is moved into the `TangoDown-Daten` folder and re-protected with the master password.
3. On every later start, TangoDown asks for the master password. After wrong entries, the waiting time gets longer.
4. Plug the stick into another Windows PC, start the EXE, enter the master password – all data is there.
5. Change the master password: **"⇄ Data & migration"** → **" 🔑 Change master password"** (takes effect immediately, the data is not re-encrypted).

### 🧯 Recovery key – if you forgot the master password

- During setup, TangoDown shows a recovery key **once** (24 characters, e.g. `ABCD-EFGH-…`). **Write it down or print it** and keep it separate from the stick – only then can you continue.
- Password forgotten: at startup click **"Forgot master password?"**, enter the key and a new password. All data is kept. Afterwards you get a **new** key (the old one is used up).
- For folders set up before this version: generate one with the master password under **"⇄ Data & migration"** → **" 🧯 Recovery key"**. "Regenerate" invalidates the old one.
- **Without the master password and without the key, the data is lost** – this is intentional, otherwise anyone with the stick could get to the data.

**Notes:** Platform account sign-ins stay on the PC where you signed in (Windows protects the browser's sign-in data itself). Do not unplug the stick while the app is running. For agencies: manage storage media according to your office's rules (encrypted stick, loss report).

## Use cases

### Fake shop or fraud domain

1. Start the investigation autopilot with the domain: capture DNS, Whois, hoster, legal notice (Impressum).
2. Approve follow-up steps: IPs of the servers, other domains on the same IP.
3. Evidence capture of the shop pages; trace the wallet from the payment method in Chain-Trace.
4. Check the timeline, create a report.

### Missing person

1. Add photos of the person as references in face matching (or in a custom person database).
2. Check images found (leads, sightings) against the references.
3. Record sightings with place and time – Geo-Intel and the timeline show the route.
4. Put a geofence around likely locations.

### Vehicle from a lead

1. Enter the license plate in vehicle matching: district, custom wanted list.
2. On a match: take the links (owner, address) into the case as well.
3. Record the sighting with time and place; situation map with vehicle symbol and direction of travel.

### Situation picture for an event

1. Create a situation picture watch for terms/hashtags.
2. Geo-Intel: situation map with symbols, arrows, areas; live air and ship traffic; world clock.
3. Export the map as an image and pass it on.

### Crypto money flow

1. Address in Chain-Trace: counterparties, swaps, sanctions lists.
2. Take it into a subgraph; watchlist for new transactions.
3. Report with money flow and sources.

## Principles

- **Never overwrite silently:** If data comes in from outside and the entry already exists, existing values stay. Differences are shown; only what you explicitly select is taken over.
- **Check everything yourself:** Every result – including from queries, matches and analyses – is a lead. Before using it, always verify it at the source yourself and cross-check where possible.
- **Only lawfully accessible, public data.** No signing in to other people's accounts, no bypassing of protective measures.
- **Purpose limitation:** Every query belongs to a case with a purpose; many queries require a justification.
- **A hint is not evidence:** Correlations, similarity scores and AI answers are hints and must be checked.
- **Data minimization:** Keep to retention deadlines; facial images and personal data only within the scope of

the assignment.
- **Traceability:** Audit log, checksums and source references make every step verifiable.

## Keyboard shortcuts

This overview is available as an overlay at any time with **F1** or **Ctrl+#**.

**Everywhere**

- **Ctrl+K** – command palette: modules, functions, elements, manual sections, even with typos
- **F1 / Ctrl+#** – this keyboard shortcut overview
- **Ctrl+Alt+S** – streaming mode on/off (hide your own details)
- **Ctrl+mouse wheel / Ctrl + / Ctrl − / Ctrl+0** – interface larger, smaller, 100 %
- **F11** – full screen of the current window
- **Esc** – cancel, close menu, clear selection, end magnification

**Graph**

- **Large graphs** (from a few hundred elements) briefly show an image of the area without lines and labels while panning and zooming, so everything stays smooth. Small-font labels fade out when zooming out, layout runs without animation.
- **Ctrl+Z** – undo last change, including deletion
- **Double-click** on a line – label it; **right-click** – menu
- **Ctrl+drag** – select several elements with a frame
- **Ctrl+C / Ctrl+V** – copy selected elements / paste into another graph or case

**Situation map**

- **Del** – remove the selected map symbol (with confirmation)
- **Alt+mouse wheel / Shift+mouse wheel** – enlarge / rotate map symbol
- **Ctrl+drag** – select several symbols

**Browser**

- **Ctrl+T / Ctrl+W** – new tab / close tab
- **Ctrl+L** – address bar
- **Ctrl+F** – find in page
- **Ctrl+U** – page source
- **Ctrl+D** – bookmark
- **Ctrl+J** – show downloads
- **Ctrl+P** – capture page
- **F5 / Ctrl+R** – reload
- **F12** – developer tools

**Terminal**

- **Tab** – complete (commands, values, files)
- ↑ **/** ↓ – history
- **Ctrl+L** – clear screen
- **Ctrl+Shift+C / V** – copy / paste in the real terminal
- **Ctrl+C** – cancel in the real terminal

**Demo**

- **Space** – pause / resume
- **Esc** – exit

## Terms & abbreviations

- **ADS-B** (Automatic Dependent Surveillance–Broadcast) – radio signal with which aircraft transmit their position and identification; basis of the live flight data.
- **Admiralty code (A1–F6)** – rating of a piece of information: letter = reliability of the source (A very reliable … F cannot be judged), number = credibility of the information (1 confirmed … 6 cannot be judged).
- **AES-256** (Advanced Encryption Standard, 256 bit) – very strong encryption standard used worldwide; cases and packages are encrypted with it.
- **Air gap** – operation without any connection to the outside; all online queries are blocked.
- **AIS** (Automatic Identification System) – radio system with which ships transmit their position and identification.
- **API** (Application Programming Interface) – interface through which TangoDown queries data from a service; this usually requires an **API key** from the provider.
- **ASN** (Autonomous System Number) – number of a network operator on the internet (e.g. a hoster).
- **Audit log** – log of all actions in the case; later changes stand out.
- **CSV** (Comma-Separated Values) – simple table file, e.g. for custom databases.
- **CVE** (Common Vulnerabilities and Exposures) – worldwide identifier of a security vulnerability, e.g. CVE-2024-3400.
- **CVSS** (Common Vulnerability Scoring System) – severity of a vulnerability from 0 to 10.
- **DMS** (document management system) – here: "Case files & documents" with versions, origin and checksum.
- **DNS** (Domain Name System) – the "phone book" of the internet, translates names into IP addresses.
- **DoH** (DNS over HTTPS) – encrypted DNS queries, so eavesdroppers cannot see which names are looked up.
- **DPAPI** (Data Protection API) – Windows protection feature that binds data to the Windows user account on one PC. Protects against theft, but prevents simply copying to another PC.
- **GDPR** (DSGVO, Datenschutz-Grundverordnung – General Data Protection Regulation) – EU data protection law; basis for purpose limitation, data minimization and retention deadlines.
- **EXIF** – additional data in photos (camera, time, often GPS position).
- **ffmpeg** – free program for converting, merging and recording video and audio.
- **GDELT** (Global Database of Events, Language and Tone) – open, automatically built database of news events worldwide.
- **Geofence** – marked area on the map that triggers an alert when there is activity.
- **HLS** (HTTP Live Streaming) – common format for live streams on the internet.
- **IP address** (Internet Protocol) – address of a device on the internet.
- **KEV** (Known Exploited Vulnerabilities) – list by the US agency CISA of vulnerabilities that are known to be

exploited.

- **Kill switch** – blocks all connections as soon as the tunnel (Tor/proxy) fails, so your own IP does not become visible.
- **MJPEG** (Motion JPEG) – video stream made of single images, typical for simple webcams.
- **ONVIF** – standard through which network cameras can be found and controlled.
- **OSINT** (Open Source Intelligence) – insights from openly accessible sources.
- **Passphrase** – longer password that protects a package (.tdpack, .tdumzug).
- **PCAP** (Packet Capture) – recording of network traffic, e.g. from Wireshark.
- **RDAP** (Registration Data Access Protocol) – modern successor of WHOIS for domain and IP registration data.
- **RDP** (Remote Desktop Protocol) – remote access to a Windows desktop.
- **RTSP** (Real Time Streaming Protocol) – protocol for live camera images.
- **SHA-256** – checksum ("digital fingerprint") of a file; any change produces a completely different value.
- **SOCKS** – proxy protocol through which, e.g., Tor is addressed.
- **SOCMINT** (Social Media Intelligence) – insights from social media.
- **SSH / SFTP** (Secure Shell / SSH File Transfer Protocol) – encrypted remote access to servers and file transfer, respectively.
- **Tor** (The Onion Router) – anonymization network that hides your own IP address.
- **Migration package (.tdumzug)** – encrypted file with all of the application's data for moving to another PC.
- **URL** (Uniform Resource Locator) – internet address, e.g. https://example.org.
- **User agent (browser identity)** – text with which a browser identifies itself to websites.
- **VOD** (Video on Demand) – finished video available on request (as opposed to a live stream).
- **VPN** (Virtual Private Network) – encrypted tunnel into another network.
- **VS-NfD** (Verschlusssache – Nur für den Dienstgebrauch; German classified – restricted) – lowest German classification level; such cases are blocked for cloud AI and can only be queried via the local interface with the on-prem token.
- **yt-dlp** – free program for downloading videos from the internet; basis of video evidence capture.
- **Purpose limitation** – every query belongs to a case with a defined purpose (GDPR principle).