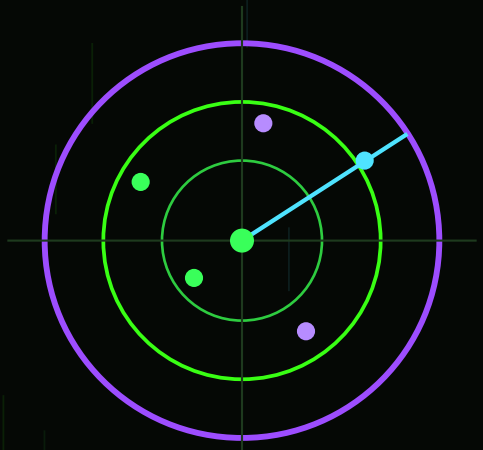


OSINT

LIVE CONNECTIONS VIEWER

What the board is telling you, what the verdicts mean,
and what to do about each one — in plain words.

HOW IT WORKS

USER MANUAL · OCTOBER 2026

777 SOFTWARE

FREE — AND IT STAYS FREE

1 — WHAT OSINT IS

Every program on your computer that touches the internet — your browser, your mail, your updates, your games — holds connections: live lines between your machine and addresses out on the internet. Most people never see them. OSINT shows them to you, live — every connection your computer is holding right now, in plain rows, refreshed every few seconds as connections come and go.

Seeing the lines is only half of it. For each outside address on the board, OSINT checks public safety lists and lookup services — the same public records security people use — and gives you a plain answer: is this connection known safe, carrying no bad reports, suspicious, or known bad? Every answer shows its homework: what each check said, and how long ago it said it.

Think of it as a window with a reference librarian standing next to it. The librarian looks addresses up in public books and shows you the pages. The decision stays yours.

> OSINT is a viewer and an advisor — nothing more. It never blocks a connection, never closes one, never changes anything on your computer or your network. It does not scan, ping, or probe the other end. It reads the connection list your computer already keeps, reads public records about the addresses on it, and tells you what it found. If a connection needs stopping, that is done by closing the program making it — §3 tells you, in plain words, when that is worth doing.

OSINT runs on the machine you install it on, and it shows that machine's connections — open it on your laptop, you see your laptop's lines. There is one window, one board, and one job: help you make a good decision about whether a connection is safe.

2 — READING THE BOARD

The board is a table. Each row is one connection. Here is what every column means, left to right:

Column	What it means, in plain words
STATE	What the connection is doing right now. ESTABLISHED means the line is open and talking. LISTEN means a program is waiting for someone to connect to it. TIME_WAIT and similar states are a connection finishing up and closing. UDP rows are a kind of connection that has no “open line” state — that is normal.
LOCAL	Your end of the line: your computer's address and the number (port) your side is using. This is you.
REMOTE	The other end of the line: the outside address and port your computer is talking to. This is who the checks are about.

Column	What it means, in plain words
TAG	A label from simple local rules. LOCAL_LAN = an address on your own home network. LOOPBACK = your computer talking to itself. SAFE_... = a name you wrote into your own tag file (it ships empty — a SAFE_ label exists only if you write one). EXTERNAL_NODE_... = everybody else: a stranger, with a short code so the same stranger carries the same tag every time. A tag is your label — it never hides a warning (§3).
HOST	The name of the remote address, when one is published. If no name can be found, you see a plain —. OSINT never guesses a name.
VERDICT	The safe-or-not answer for that address, in plain words — the subject of §3. Rows on your own network and listening rows show —: private addresses are never sent anywhere and never judged, because there is no public record to judge them by.

The board's habits

- It breathes. The board re-reads your connections every 5 seconds, and the header shows the countdown to the next refresh. New connections appear; closed ones fall off. Refresh now re-reads at once; Pause holds the board still so you can read.
- The footer counts. The line at the bottom tells you how many connections there are, how many are external, how the checks are doing, and how old the downloaded safety lists are — so stale information is always labeled stale.
- Listeners sit at the bottom, dimmed. They are connections-in-waiting — programs ready to accept a connection — part of the full picture, kept out of the way.
- In the standard order, danger floats. The board's own order puts KNOWN BAD first, then SUSPICIOUS, then the still-being-checked rows, then NO BAD REPORTS and KNOWN SAFE — the rows that deserve your eyes get them first. (§5 shows how to re-order the board yourself.)

3 — THE VERDICTS

A verdict is the worst honest reading of everything the checks said about an address — never an average, never a guess. There are four verdicts and three honest “not a verdict” states:

Verdict	What it means
✓ KNOWN SAFE	The address is positively identified as a known, legitimate service — for example, it sits in a public set of known-benign services — and nothing bad was found in any check. “No bad news” alone can never earn this; identification earns it.

Verdict	What it means
· NO BAD REPORTS	The checks ran, and none of the public lists have anything bad to say about this address. Read it exactly as written: it means nobody has reported it — it is not a promise that it is safe. This is where most ordinary addresses land.
⚠ SUSPICIOUS	Nobody has proven this address bad, but something about it doesn't look right: people have reported it misbehaving, a scanner or two flags it, it has been seen scanning the internet, or it exposes known flaws while nobody can name who it is. Worth a closer look — the detail pane (§4) shows exactly what raised the flag.
KNOWN BAD	The address is on a public list of known-bad addresses — for example, a list of active botnet control servers — or several strong checks agree it is malicious. Treat the connection as dangerous until you know exactly why it is there.
... CHECKING	The lookups for this address are still running. The board keeps refreshing; the answer fills in underneath. Wait a few seconds.
NOT CHECKED	No check has run on this address yet — it just appeared, or a free allowance is spent. The pane says which. It is a statement about the checks, not about the address.
LOOKUP FAILED	The checks could not be completed — a service didn't answer, or there is no connection to ask with. This address is unknown, not cleared. If you are offline, the board says OFFLINE — CACHED ONLY and every verdict comes from the downloaded lists and saved lookups, with their ages shown.

What to do about each one

- KNOWN BAD — stop and look. If you don't know exactly why your computer is talking to that address, close the program you think made the connection, run your normal antivirus scan, and don't send anything sensitive until you've sorted it out. OSINT can't block it for you — closing the program is the block.
- SUSPICIOUS — no panic, one closer look. Open the detail pane and read what raised the flag. If you don't recognize what you were doing when the connection appeared, close the apps you weren't using and watch whether it comes back.
- NO BAD REPORTS — nothing to do. Keep the normal rule: if you recognize the service — your browser, your updates, your mail — this is ordinary internet traffic.
- KNOWN SAFE — nothing to do. This is the kind of connection your computer makes all day: DNS, updates, big public services.

- CHECKING / NOT CHECKED / LOOKUP FAILED — no advice yet, because the checks aren't done or didn't answer. An unknown connection isn't a bad one. Use the WHO IS THIS? section of the pane in the meantime, and check again when the lookups complete.

> The honest rules, so you can hold us to them: no report is a promise — a clean check means “nobody has reported it,” never “proven safe.” A lookup that fails says FAILED, out loud; OSINT never smooths a failure into a clean answer. If two checks disagree, the verdict follows the worse reading and the pane shows both statements. And every fact carries its age, so you always know how fresh an answer is.

One more separation the board keeps: a tag (§2) is your own label — “I know this one.” A verdict is what public records say. If a list flags an address you tagged SAFE_, the row shows both, verdict first. A label never hides a warning.

4 — PICKING A CONNECTION

Click a row on the board and it becomes your pick — highlighted in a deep green that stays readable even when the window doesn't have focus. The pick is always exactly one connection, and it follows the connection, not its place on the list: refreshes, re-sorting, scrolling, and pausing can never slide the highlight onto a different connection. If your picked connection closes, the pane says so in plain words — “This connection has closed — pick another row above” — instead of quietly showing you a different one.

The detail pane

Under the board, the detail pane tells the story of your picked connection in three fixed sections:

- WHO IS THIS? — the published name (or an honest “no name published”), the network that owns the address, roughly where it is, its registry country (the paperwork country — the pane says plainly that this is not proof of location), and any tag of yours that matches.
- WHAT THE CHECKS SAID — every source, one line each: the known-bad lists, what the address exposes, each keyed check you have turned on — what it said, and when it was checked. A source that failed says so on its own line.
- WHAT SHOULD I DO? — the guidance for this verdict, in plain words (§3 has the same texts).

The pane describes the address, not the program using it — checks know about addresses, and the pane never pretends they know more.

The check buttons

Under the pane sit the buttons. Each one acts on your pick only:

Button	What it does
Check with GreyNoise	Asks GreyNoise about your picked address: is it background internet noise — the scanning that washes over everybody — or rarer than that? Works with no key, inside a small free daily allowance; when the day's allowance is spent, the pane says so in plain words and every other check keeps working.
Check with VirusTotal	Asks dozens of security scanners to vote on your picked address, and shows the count in the open. Needs your own free VirusTotal key (§6) — with no key saved, the pane tells you it is OFF instead of failing quietly.
Check with URLhaus	Asks abuse.ch's URLhaus: has this host served malware links? Quiet when there is nothing to say; a ⚠ warning line when there is. Needs your own free abuse.ch Auth-Key (§6).
Copy IP	Copies your picked connection's address to your clipboard, so you can use it in your own tools.

> The rule the whole app is built on: the checks run only on the connection you have actually selected — the same one the detail pane is showing — and only when you click that check's own button. Nothing selected, or your pick has closed, means no lookup goes out at all; the app tells you to pick a connection first. Checks work on outside connections — pick a row on your own home network and the pane answers: “Pick an outside connection first.”

Two honest exceptions, both in the open: AbuseIPDB has no button — once you save its key, it joins the checks by itself for the outside addresses on your board, and its line appears in WHAT THE CHECKS SAID with the others. And Settings carries one optional switch — Auto-check SUSPICIOUS rows with GreyNoise — which is off unless you turn it on; it exists because the free GreyNoise allowance is small, and spending it should be your choice. Those are the only things that can happen without a click, and both are yours to control.

5 — SORT + FILTER: YOUR ORDER, YOUR CUT

Sorting — click a column name

- Click STATE, LOCAL, REMOTE, TAG, HOST or VERDICT at the top of the board and the whole board re-orders by that column. An arrow on the column name shows which column is in charge and which way it runs. Click the same name again to flip the direction.
- VERDICT sorts by danger, not alphabet: the first click puts KNOWN BAD at the top, then SUSPICIOUS, then the still-working classes (CHECKING… / LOOKUP FAILED / NOT CHECKED), then NO BAD REPORTS, then KNOWN SAFE. Rows with no verdict at all — listening sockets and your own network — always stay at the bottom: no verdict is not a danger level.

- Addresses sort by their real numbers, then by port — so 9.9.9.9 comes before 10.77.0.10, the way addresses actually count, not the way they spell.
- Your sort survives the refreshes. New connections slot into the order you chose instead of knocking it over.

Filtering — the FILTER row

- Pick a verdict — for example SUSPICIOUS — and the board shows only rows carrying that verdict.
- Type in the Text box and the board shows only rows whose HOST, LOCAL address, REMOTE address or TAG contains your text. Capitals don't matter.
- The counter tells you the truth: “showing X of Y.”
- Clear wipes the filter. Your sort stays.

> A filter changes only what you SEE. Every connection is still checked exactly as before; filtering never sends anything anywhere. And if you filter away the connection you had picked, the detail pane says so in plain words — “this connection is hidden by your filter right now — it is still the connection the check buttons will use.” The buttons never drift to a row you didn't choose.

Sorting and filtering are for this session only: restart the app and the board comes back whole, in its standard order. Nothing about them is saved, sent, or shared.

6 — SETTINGS + KEYS

The Settings button (bottom bar) opens the Settings window. It holds four optional key fields, two switches, and a cache button — nothing else. A key is a short secret line of text a service gives you, free, so the app can ask it questions in your name. Every key is off until you add your own.

Key (Settings field)	What it turns on
AbuseIPDB key	The best “has this address been reported misbehaving?” score — an abuse confidence score out of 100, with the number of reports. Once saved, this check runs by itself (§4) — there is no button.
VirusTotal key	The Check with VirusTotal button: dozens of scanners vote on an address. Honest catch, in VirusTotal's own warning: any address queried through their API is added to the VirusTotal dataset and made accessible to their community. The same warning sits in Settings, next to the field.
abuse.ch Auth-Key	The Check with URLhaus button: has this host served malware links?

Key (Settings field)	What it turns on
GreyNoise key	GreyNoise works without a key. A key only raises the tiny free allowance a little (free keys run to about 50 lookups a week). GreyNoise gives keys to work-email accounts; a personal-email account gets none — that is their rule, and the keyless button is the product's answer.

How keys live, and the switches

- Save Settings saves EVERYTHING — all four keys and both switches, exactly as you left them, permanently, until you change them. They are still there when you open the app again.
- Your keys live in one file on your computer only: `osint_settings.json`, next to the program, locked so only your own user account can read it (permissions 0600). The file is never uploaded, never printed in any log, and never part of any download. A key is sent only to its own service, when you run its check.
- Live lookups ON — turn it off and the app works in offline mode: the board still shows your live connections, and verdicts come from the downloaded lists and saved lookups only, with their ages shown.
- Auto-check SUSPICIOUS rows with GreyNoise — off by default (§4). Turn it on only if you want the app to spend the small free GreyNoise allowance by itself, on suspicious rows only.
- Clear Intel Cache (in the app) empties the downloaded lists and saved lookups for real; the next lookups simply fetch fresh copies.
- Removing a key: clear its field and press Save Settings. That check turns back off. (GreyNoise simply returns to its keyless allowance.)

> Getting the keys, step by step: the companion guide OSINT — Getting Your Keys (`OSINT-Getting-Your-Keys.pdf`) ships with this program and walks each free signup — where to go, which email link to click, where the key is shown, and how to paste it into the fields above. Every key in it is free; if a page ever asks you for a card, you are on the wrong plan.

7 — PRIVACY: THE WHOLE TRUTH

OSINT has no accounts, no telemetry, no analytics, no update checks, no crash reporting — and no server of ours for anything to phone home to. There is nothing to sign up for with 777 Software, and nothing about you is collected, because there is nowhere for it to go.

To give a verdict, the app does ask outside services about addresses — the outside addresses already on your board. It asks about an address, never about you. Here is the complete list of what leaves your computer:

Where it goes	What is sent
Public safety-list hosts (abuse.ch Feodo Tracker + SSLBL, the CISA exploited-flaws catalog)	Nothing about your connections. The app downloads the public lists whole, like downloading a newspaper. Those checks then happen on your own machine.
Shodan InternetDB · Team Cymru · ipapi.co	The outside address being checked — once, then the answer is saved on your machine (a day for the first two, a week for rough location) instead of asking again.
GreyNoise · AbuseIPDB · VirusTotal · URLhaus	The outside address being checked — plus your own key for that service, to that service only. GreyNoise, AbuseIPDB and VirusTotal/URLhaus run only as §4 and §6 describe.
Your normal DNS resolver	The outside address, to turn it into a name (the HOST column) and to look up which network owns it.

- Never sent, anywhere: addresses on your own network, your computer's own addresses, your connection list as a set, which programs you have open, your tag file and your own SAFE_ names, and your keys (except to their own service, over an encrypted connection).
- Everything the app keeps, it keeps at home: the downloaded lists, the saved lookup answers, your settings and keys — all in files next to the program, on your machine, yours. The lookup cache is capped at about 10 MB.
- Nothing queues up to send later. Go offline and the app keeps working from what it has saved, honestly labeled. Come back online and lookups simply resume for addresses still on the board.

8 — THE LIMITS, SAID STRAIGHT

A tool you can trust tells you what it cannot do. Here is OSINT's list, complete:

- OSINT advises; it does not protect. It cannot block, close, or slow a connection, and it is not a firewall, an antivirus, or a substitute for either. Your protection is still your firewall, your antivirus, and your own judgment — OSINT feeds the judgment.
- A clean verdict is not a guarantee. NO BAD REPORTS means nobody has reported the address — a brand-new bad address has no reports yet either. KNOWN SAFE requires positive identification, and even that is identification, not a promise about tomorrow.
- It shows connections, not culprits. The board shows the lines your computer holds; it does not promise to name which program holds each one, and a connection that opens and closes between refreshes can pass unseen — every connection viewer shares that limit, and the 5-second refresh keeps the gap small.
- The checks know addresses, not intentions. Public records describe what an address has been seen doing and who owns it. They cannot tell you why your program connected to it —

that part is yours to recognize.

- Free services have free limits. Allowances run out, services go quiet, lists age. When any of that happens, OSINT says so in plain words instead of dressing a gap up as an answer — but the gap is real while it lasts.

> When in doubt, disconnect first and read later. If a connection worries you and you can't name why it's there: close the program you think made it (or disconnect the machine), then read the pane at your leisure. You can always reconnect. Reading is free; un-sending something is not.

> That's the whole of it. One board, honest verdicts, checks that fire only when you say so, keys that live on your own machine, and limits stated in the open. Open OSINT, look at who your machine is talking to, and decide with your eyes open. That's what it's for.

OSINT — Live Connections Viewer · 777 Software. This manual ships with the program, alongside OSINT — Getting Your Keys. The services named here are run by their own people; their pages may rearrange over time, but the shape of this app — one board, honest answers, nothing phoning home — does not change.