

The Shadow Files

Том 2

Атрибуція

YEHOR SELIN

Зміст

Перш ніж почати	3
Одна зачіпка ніколи не була метою	5
Як влаштований другий том	7
Місток із першого тому	9
Приватне — не значить закрите	13
Павутина нікнеймів	31
Telegram зблизька	44
Обличчя й фотографії	62
Витоки, оброблені чисто	76
Граф особи	93
Як змусити сигнали погодитися	111
Боротьба з власною певністю	130
Повна атрибуція	143
Що ти вмієш тепер	163
Додаток	166

Перш ніж почати

Це другий том The Shadow Files — практичного курсу з розвідки за відкритими джерелами, OSINT. Він продовжується прямо з першого тому. Якщо ти не читав основи — цикл, драбину впевненості, захист самого себе — прочитай їх спершу. Ця книга бере їх як задане.

Тут усе вигадане

Кожне ім'я, нікнейм, електронна адреса, номер телефону, фотографія та кейс у цій книзі — цілком вигадані. Кожен із них створено, щоб навчити методу, — а не щоб описати реальну людину. Будь-яка схожість із реальною особою, акаунтом чи подією — чистий збіг.

Оскільки кожна деталь вигадана, приклади показано повністю — повні, звичайні на вигляд дані замість затертих символів, — щоб ти бачив точно, як справжній слід поводить ся крізь платформи, і ніщо з цього не торкалося реальної людини.

Правило в один рядок

Лише відкриті джерела. Нічого, що вимагає логіна чи пароля. Поважай приватність людей і закон. Це вся рамка, і вона не слабшає, коли росте твоя майстерність.

Дві речі варто тримати в голові. Знай закон там, де працюєш,
— клієнт, який наймає тебе розслідувати когось, це не те
саме, що закон, який дозволяє збирати все про всіх довкола
нього. І більшість шкоди в цьому ремеслі завдають людям,
які ніколи не були суб'єктом, тож бери лише те, що
відповідає на твоє питання, і на цьому спиняйся.

*Професіонал — не той, хто може знайти
найбільше. Це той, хто знає, де зупинитися.*

Одна зачіпка ніколи не була метою

Що змінюється у другому томі

У першому томі ти навчився тягнути одну нитку. Ти брав єдину зачіпку — нікнейм, електронну адресу, номер — і крок за кроком доходив нею до людини. Це фундамент, і все тут стоїть на ньому.

Але справжні люди не живуть на одній платформі. Вони розкидані — фотографія тут, коментар там, старий акаунт, про який забули, родич, який їх позначив, злита електронна адреса, що зв'язує два імені. Одна нитка — це те, з чого ти починаєш. Це майже ніколи не те, чим ти закінчуєш.

Другий том — про закінчення. Він про те, як брати нитки з багатьох місць і сплітати їх в одну впевнену особистість — і робити це під справжнім тиском: приватні профілі, двійники, видалений контент і твоє власне бажання мати рацію.

Для кого ця книга

Для тебе, якщо в тебе є фундамент і ти хочеш перейти від *пошуку зачіпки до побудови справи*. Тобі не треба бути технарем. Тобі потрібне мислення з першого тому й терпіння вести людину крізь пів десятка платформ, не втрачаючи дисципліни. А якщо технічне слово колись соб'є тебе з пантелику — наприкінці є глосарій, зазирни до нього будь-коли.

Що ти вмітимеш наприкінці

Вести одну людину крізь соцмережі й месенджери. Читати, що фотографія й обличчя можуть і чого не можуть тобі сказати. Використовувати дані витоків, щоб з'єднувати ідентифікатори — ніколи щоб вляматися. Малювати карту зв'язків і давати їй вести тебе. І, найважче з усього, вирішувати, *наскільки ти впевнений*.

Чим цей том не є

Це не інструкція до інструментів і не все ремесло. Відновлення видалених акаунтів, геолокація й інфраструктура чекають на третій том; світ професіонала — автоматизація, дью-ділідженс і контррозслідування — чекає своєї черги після того. Тут ми добре опановуємо одне: атрибуцію крізь платформи.

Одна зачіпка відчиняє двері. Ця книга — про кімнати за ними.

Як влаштований другий ТОМ

Серія, ця книга і як побудовано кожен розділ.

The Shadow Files — це серія з чотирьох томів. Кожен піднімає тебе на рівень вище, і кожен бере як задане лише те, чого навчив попередній.

- Том 1 — Фундамент. Мислення, правила й твої перші справжні навички.
- Том 2 — Атрибуція крізь платформи. Ведення однієї людини крізь соцмережі, месенджери, фотографії й витоки — в єдину, впевнену особистість. *(Ця книга.)*
- Том 3 — Складні цілі. Видалені акаунти, геолокація, інфраструктура й трюки, що заскочують людей зненацька.
- Том 4 — Професіонал. Корпоративна робота, звіти, контррозслідування й перетворення навички на ремесло.

Про межу: ми все ще шукаємо людей, не сервери, домени чи фізичні локації — це теж справжній OSINT, але інший набір інструментів для іншого дня.

Усередині цього тому

1. Приватне — не значить закрите 2. Павутина нікнеймів 3. Telegram зблизька 4. Обличчя й фотографії 5. Витоки, оброблені чисто 6. Граф особи 7. Як змусити сигнали узгодитися 8. Боротьба з власною впевненістю 9. Повна атрибуція

Як побудовано кожен розділ

Той самий ритм, що й у першому томі, щоб ти завжди знав, де перебуваєш:

- Ідея — простими словами, без жаргону.
- Метод — як професіонал насправді думає й працює, крок за кроком.
- Розібраний кейс — коротке, вигадане розслідування, за яким ти можеш стежити, із залишеними глухими кутами.
- Вправа — щось безпечне й законне, що ти робиш сам.
- Підсумок — кілька речей, які варто запам'ятати.

Одна обіцянка про інструменти

Як і раніше: спершу метод, інструменти потім. Деяких названих тут інструментів може вже не бути, коли ти це читатимеш, а їхнє місце займуть нові. Це нормально. Мислення не змінюється. Опануй метод — і будь-який інструмент буде просто швидшим способом зробити те, що ти вже розумієш.

Місток із першого тому

Фундамент на одну сторінку, перш ніж іти глибше.

Перш ніж рушити кудись нове, дай мені швидко повернути тобі в руки фундамент. Якщо щось із цього здається незнайомим — це твій знак повернутися до першого тому, перш ніж іти далі тут. Усе в цій книзі спирається на ці чотири речі.

Цикл

Кожне розслідування, хоч би яке велике, — це ті самі три рухи, прогнані по колу.

Слід → півот → атрибуція.

ЦИКЛ



одна зачіпка, кружляй колом, поки не вкаже на людину

Три рухи йдуть як цикл — атрибуція живить наступний слід.

Слід — це відбиток, який людина лишила на видноті. Півот — це перетворення того відбитка на наступний. Атрибуція — це коли достатньо відбитків шикуються, щоб вказати на одну реальну особистість. Ти починаєш з однієї зачіпки й ганяєш цикл, поки картина не проясниться. Другий том не замінює цей цикл. Він ганяє його одразу крізь багато платформ.

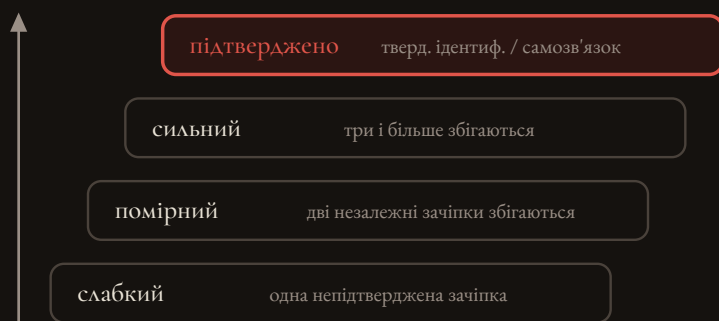
Драбина впевненості

Оскільки збіг — це не факт, ми завжди кажемо, *наскільки* ми впевнені, чотирма фіксованими словами:

- **слабкий** — одна непідтверджена зачіпка. Наведення, ніколи не висновок.
- **помірний** — дві незалежні зачіпки узгоджуються.
- **сильний** — кілька незалежних сигналів, які разом важко пояснити будь-якою суперницькою гіпотезою. Зазвичай це означає три чи більше. Але два важкі, діагностичні (скажімо, побайтово ідентичний файл аватара плюс підтверджений самозв'язок) можуть дійти до сильного, а три слабкі, поширені — не дотягнути. Кількість — це орієнтир; наскільки важко пояснити збіг геть інакше — ось справжня перевірка.

- підтверджено — жорсткий унікальний ідентифікатор або справжній самозв'язок, незалежно закріплений так, що будь-хто міг би перевірити наново.

ДРАБИНА ВПЕВНЕНOSTI



Чотири щаблі, на які ти піднімаєшся лише на незалежних сигналах: слабкий, помірний, сильний, підтверджено.

Ці чотири слова ти зустрінеш у двох місцях: коли оцінюєш силу *окремого сигналу* і коли оцінюєш свій *загальний висновок*. Ті самі слова, зв'язані правилом вище — самотній сильний сигнал ще не є сильним висновком.

Цю драбину ти використовуватимеш у другому томі жорсткіше, ніж будь-де, бо атрибуція криз платформ — це саме те місце, де завзяті початківці перетворюють купу *слабких* на хибне *підтверджено*.

Той самий нік — не той самий чоловік

Одне речення, яке треба винести з першого тому: збіг імені, ніка чи обличчя — це наведення, а не доказ. Двоє незнайомців можуть мати однаковий нікнейм. Звичайне обличчя може ввести в оману. Ти підтверджуєш незалежними сигналами — контентом, датами, зв'язками — а не самим збігом.

Лінія і де зупинитися

Лише відкриті джерела. Жодного входу в акаунти, жодного вдавання когось іншого, жодного обходу замка. І правило понад будь-яку техніку: той, хто знає, де зупинитися, а не той, хто знаходить найбільше. Методи попереду роблять легким продовжувати — тож бери лише те, що відповідає на твоє питання, і на цьому спиняйся. Перш ніж зробити перший півот, зумій сказати одним простим реченням, чому саме *цю* людину треба перевіряти й заради якого легітимного питання. Якщо не можеш — у тебе цікавість, а не справа.

Фундамент у руках? Добре. Ходімо вшир.



РОЗДІЛ ПЕРШИЙ

Приватне — не значить закрите

Замкнений профіль — це стіна, яку ти обходиш, а не двері, які ти висаджуєш.

Ти клікаєш на профіль. Завантажується аватар.
Завантажується ім'я. А далі нічого — ні дописів, ні друзів, ні фотографій. Замок там, де мало б бути життя. Більшість людей тут зупиняється. Вони пишуть у нотатках «приватний, глухий кут» і йдуть далі.

Я розумію чому. Замкнений профіль здається зачиненими дверима, а зачинені двері заведено поважати. Людина за

ними — хтось: мати, інженер, вдівець, дитина, що намагається спокійно рости, — потяглася до налаштування й думала, що на цьому все. Тримайся цієї думки, читаючи цей розділ. Робота нижче — не про те, щоб їх здолати; вона про те, щоб помічати, що світ довкола них уже сказав уголос.

*Приватність контролює те, що публікують вони.
Вона майже ніколи не контролює те, що зробили всі
інші.*

Замкнений акаунт обмежує твій прямий погляд на одну сторінку. Він не обмежує друга, який позначив їх на весіллі. Він не обмежує групу, до якої вони приєдналися 2019 року і яка досі показує учасників. Він не обмежує архів, що зробив знімок сторінки, перш ніж вона стала приватною. І часто — хоч уже не завжди — він не ховає фото профілю, яке багато платформ лишають видимим, щоб акаунт узагалі можна було знайти.

Одну річ закріпи в голові, перш ніж почнемо. Робота цього розділу вузька: ти вже *підозрюєш* особистість — ім'я, обличчя, твердження — і хочеш знати, чи належить замкнений профіль тій людині. Ти тут, щоб підтвердити збіг, використовуючи відкритих людей і записи довкола цілі. Це відрізняється від виявлення особистості, якої ти ще не маєш. Знайти приховану *другу* людину — невідомого родича, псевдонім, якого тобі ніхто не давав — це робота шостого

розділу, який обходить сімейне кільце, а не кільце друзів.

Ідея: перелічуй відкрите кільце, а не закритий центр

Уяви ціль як крапку. Довкола тієї крапки — кільце інших людей та інших записів: друзі, ті, хто позначає, коментатори, співучасники груп, старі кешовані сторінки. Центр темний. Кільце освітлене.

ШАРИ ДОСТУПУ



центр закритий —
кільця навколо
відкриті навстіж.

Йди всередину від
того, що лишили
відкритим.

Замкнений центр, оточений шарами, що лишаються відкритими: публічні дописи, друзі друзів, кеші й архіви та старі копії з витоків. Ти читаєш кільця, а не центр.

Твоя робота — не вламатися в центр. Твоя робота — обійти кільце й прочитати все, що кільце лишило повернутим назовні, а тоді зібрати ці фрагменти в картину центру.

Це повністю переосмислює «приватне». Приватний профіль — це не відсутність інформації. Це інформація, яку *витіснили* — виштовхнули зі сторінки самої цілі на сторінки інших людей, в архіви, у кеші. Ти просто збираєш її з іншої адреси.

Є сім поширених шарів витоку. Вивчи їх як чекліст — але спершу прочитай наступний розділ, бо деякі з них сильно занепали з середини 2010-х, і ти маєш знати, який рух ще живий, перш ніж по нього тягнутися.

- **Спільні зв'язки та «люди, яких ви можете знати».** Платформи пропонують зв'язки. Ці пропозиції картографують граф цілі, навіть коли список друзів прихований. (Цей сигнал працює в обидва боки — зваж на попередження нижче.)
- **Позначки й згадки від інших.** Приватний користувач, позначений у публічному дописі друга, повністю видимий — на сторінці друга.
- **Коментарі.** Ціль коментує публічні сторінки, публічні новинні дописи, публічні групи. Ці коментарі несуть її ім'я, а часто й фото.
- **Членство в групах і сторінках.** Списки учасників, списки відвідувачів подій і «вподобання» часто переживають налаштування приватності, бо живуть на боці групи.

- Кешовані й архівовані копії. Кеші пошуковиків і вебархіви можуть тримати версію сторінки з часів до того, як її замкнули.
- Фото профілю й банер. Часто публічні, щоб акаунт лишався знаходжуваним, — але тепер це залежить від платформи, і деякі сервіси розмивають чи закривають його. Коли воно *відкрите*, це чисте обличчя для реверс-пошуку й нитка до альтернативного акаунта під іншим ім'ям.
- Перетин друзів-друзів (FOAF). Ціль закрита, але деякі її друзі відкриті. Хтось, хто повторюється в кількох таких відкритих списках — і збігається з обличчям та ім'ям — дуже ймовірно всередині кластера цілі. (Переглядається вручну; див. Крок 6.)

Зверни увагу, чого не вимагає жоден із них: жодного входу в акаунт цілі, жодного вгадування пароля, жодного обману. Ти читаєш те, що інші люди опублікували на видноті. У цьому вся гра.

Що досі працює у 2026-му, а що тихо померло

Старіші OSINT-посібники — зокрема й частини першого видання цієї книги — спиралися на жменю розумних платформних трюків. Кілька з них уже не працюють так, як колись, і ніщо не старить слідчого швидше, ніж упевнене виконання руху, який платформа закрила роки тому. Тож вивчи *ідею* під кожним трюком. Прийом може вмерти; причина, чому він працював, — зазвичай ні. Тоді знайди поточний еквівалент для платформи перед тобою.

Три рухи занепали особливо:

- Витягування числового ID з коду розлогіненої сторінки. Роками ти міг відкрити сирий HTML профілю, шукати `id` чи `profile_id` і прочитати постійний числовий ID прямо зі сторінки. На головних платформах це тепер здебільшого закрито — сторінка є JavaScript-оболонкою, і ID більше не лежить у коді. Принцип тримається: кожен акаунт досі має стабільний числовий ID за своїм ніком, і той ID досі переживає перейменування. Ти просто маєш дістатися до нього крізь те, що платформа відкриває сьогодні — редирект share-лінка, вбудову, офіційний lookup — а не грабунком view-source. Стався до «переглянь код і прочитай id» як до ілюстрації ідеї, а не кроку, на який можна розраховувати.
- URL спільних друзів на два числові ID. Колись був URL, якому ти міг вручити два числові ID й отримати

назад людей, яких вони ділять. Facebook Graph Search, що живив більшість цього, прибрали 2019 року, і той ендпоінт спільних друзів пішов разом із ним на головних платформах. Принцип тримається: спільні зв'язки досі картографують прихований граф, і деякі платформи досі показують спільних в інтерфейсі. Але охайного URL «встав два ID» більше нема — не вчи його й не спирайся на нього як на живий крок.

- **Скрапінг і перетин списків друзів (FOAF).** Класичний рух — автоматично витягнути повні списки друзів кількох друзів і перетнути їх. Дві проблеми у 2026-му. Перша: списки друзів тепер приховувані за замовчуванням і часто приховані, тож витягати нерідко нема чого. Друга — і це важить усюди в цій книзі — автоматизований скрапінг списків друзів порушує умови надання послуг платформи. Ми цього не робимо. Принцип тримається: ціль знову з'являється всередині відомого кластера відкритих людей. Але ти доходиш до неї *ручним, відкритим переглядом* списків, які люди самі обрали лишити публічними, а не скриптовим збором.

Коли улюблений трюк перестає працювати, зазвичай зрушила стіна, а не ти. Кільце досі там. Іди знайди поточні двері в нього.

Перш ніж дивитися: не засвіти себе

Ось помилка, яку роблять навіть досвідчені люди, і вона достатньо нова для другого тому, щоб заслужити власний знак «стоп». Коли ти переглядаєш ціль, залогінений у дослідницький чи «сок»-акаунт — чисту, окрему особистість, яку ти тримаєш лише для розслідувань, ніколи не свій справжній профіль, — ти не невидимий. Механізм «людей, яких ви можете знати» двонапрямлений — ті самі сигнали, що виносять ціль тобі, можуть винести *твій сок-акаунт цілі*. Багаторазове відкриття чийогось профілю, дозвіл застосунку читати твої контакти чи спільна з ними мережа можуть виштовхнути твій слідчий акаунт у *їхні* пропозиції. Це попереджає їх, спалює акаунт, а в чутливій справі може скомпрометувати все завдання.

Тож налаштуйся, перш ніж дивитися. Використовуй чисту, обжиту дослідницьку особистість, не пов'язану з твоїми контактами, адресною книгою телефону чи справжніми акаунтами. Вимкни синхронізацію контактів. Віддавай перевагу розлогіненим та архівним переглядам усюди, де вони досі повертають потрібне. Припускай, що будь-що, зроблене залогіненим, може відлунати назад людині, за якою ти стежиш, і дій відповідно.

Метод, крок за кроком

Крок 1 — Зафіксуй якір. Перш за все розв'яжи одну річ, яка не змінюється: стабільний числовий ID за красивим ім'ям. Красиві ніки змінюються; числові ID постійні, і кожна наступна техніка відштовхується від цього якоря. Як зазначено вище, ти рідко можеш просто прочитати його з коду сторінки — дістанься до нього крізь те, що платформа відкриває сьогодні. Хоч би який маршрут ти обрав, запиши ID. Він переживе те, що ціль перейменує себе наступного тижня.

Спробуй (2026). Обери один конкретний маршрут, щоб перетворити ім'я на число. У Telegram перешли одне з повідомлень акаунта боту-ID (резолверу типу @username_to_id — наприклад, @username_to_id_bot або @usinfobot) і прочитай числовий ID користувача. В Instagram відкрий розлогінений share-лінк на кшталт `instagram.com/<handle>/` у чистому браузері й прочитай числовий id з URL сторінки чи URL опублікованого допису; на Facebook чи X вбудова одного з дописів профілю відкриває те саме число тим самим шляхом. На більшості платформ публічний вебпошук «username to ID» робить ту саму роботу з розлогіненого стану. Хоч би що ти використав, ти шукаєш те саме: число, що живе під ім'ям. Застереження: конкретний бот, ендпоінт чи сайт-пошук, названий вище, цілком може бути мертвим до того, як ти це

читаєш, — форма лишається (знайди число під ім'ям), конкретні двері — ні.

Крок 2 — Забери зображення. Якщо аватар публічний, витягни версію в повній роздільності — багато платформ досі віддають велике зображення, навіть коли стіна закрита. Збережи його. Ти реверс-шукатимеш його пізніше, бо те саме обличчя під іншим, *незамкненим* ніком — це один із найпоширеніших способів, яким приватний профіль розкривається. Якщо зображення закрите чи розмите, занотуй це й іди далі; не сприймай відсутній аватар як відсутню справу.

Крок 3 — Картографуй спільні зв'язки. Якщо ти вже маєш одного відомого пов'язаного — «орбітний» профіль на кшталт подружжя, колеги, брата чи сестри — пошукай зв'язки, які вони ділять із твоєю ціллю. Деякі платформи досі показують спільних в інтерфейсі; старий URL «встав два ID» — ні. Роби це з належно підготовленого дослідницького акаунта (див. попередження вище) й пам'ятай, що доводить спільний зв'язок: *зв'язок*, а не *особистість*. Тобі все одно доводиться подивитися на людину на тому кінці.

****Крок 4 — Шукай довкола цілі, а не на ній.**** Використай власне поле пошуку платформи з ім'ям цілі плюс контекстні слова: прізвище, роботодавця, місто, «день народження». Це витягує контент зі сторінок *інших людей*, який стрічка самої цілі приховує. Тоді залиш платформу зовсім і пройди

дорками відкритий вебпростір — шукай з операторами на кшталт site:: site:platform.com "їхнє ім'я", числовий ID, будь-яку унікальну фразу з біо.

Крок 5 — Пройди архіви. Згодуй URL профілю вебархіву й кешу пошуковика. Якщо сторінка колись була публічна, знімок може існувати. Іди календарем назад — *старіші* знімки часто багатші, зроблені до того, як людина затягнулася тугіше. Але перевір, що знімок насправді захопив: знімок, зроблений *після* замикання, зберігає лише стіну.

Крок 6 — Переглянь відкритий кластер (FOAF, вручну). Візьми трьох-чотирьох підтверджених друзів, чії власні списки друзів вони лишили публічними. Прочитай ці списки сам і занотуй, хто повторюється. Людина, що з'являється в кількох друзів твоєї цілі й збігається з аватаром та ім'ям, дуже ймовірно всередині кластера твоєї цілі. Лише ручний перегляд — жодного автоматизованого витягання, жодного скриптового перетину. Ця лінія не опційна; автоматизований збір порушує правила платформи й псує роботу.

Крок 7 — Постав кожен фрагмент на драбину. Спільне ім'я з позначки — слабе. Позначка *плюс* збіг обличчя *плюс* спільний зв'язок — сильне. Зваж, тоді вирішуй.

Розібраний кейс, з глухими кутами й усім іншим

Слідча редакція попросила мене підтвердити одну річ, перш ніж запустити матеріал. Чоловік, який називав себе Rui Costa, дав під запис коментар іншому виданню, представившись прорабом і речником з безпеки на проблемному будівельному проєкті, — і повністю приватний акаунт Instagram, нік r.costa.builds, аватар чоловіка на будмайданчику, без видимих дописів чи підписників, ходив по руках як доказ, що він справді там працює. Чи належав той замкнений акаунт тому самому Rui Costa, якого газета збиралася цитувати як авторитет? Вигадані імена, справжній метод. Та сама людина чи збіг?

Спершу якір — і одразу в мертвий трюк. За звичкою я поліз у код розлогіненої сторінки, щоб зняти числовий ID. Нічого. Сторінка була JavaScript-оболонкою.

```
Код розлогіненої сторінки
-----
view-source: r.costa.builds
пошук "profile_id" ... 0 збігів
пошук "user_id"    ... 0 збігів
сторінка = JS-оболонка, ID нема
-----
2026: цей трюк тут закрито
```

Старий трюк із числовим ID, мертвий одразу.

Тож я зробив те, чого вимагає принцип: перестав оплакувати трюк і дістався до стабільного ID через редирект share-лінка. Якір закріплено, просто крізь інші двері.

Аватар. Зображення було публічним, тож я витягнув фото в повній роздільності й прогнав його крізь два реверс-рушії зображень і один face-рушій.

```
Реверс зображення + пошук обличчя
-----
QUERY  r_costa_avatar.jpg
рушій A  0 візуальних збігів
рушій B  1 збіг
  - stockphotos "man at job site"
face-рушій 1 кандидат 68%
  - linkedin "Rui Costa", будівельник
-----
сток-хіт = типовий, кинь його
```

Одна сток-настка, одна тонка зачіпка обличчя.

Збіг зі сток-фото був типовим зображенням «чоловік на будмайданчику», перевикористаним усюди — спільне стокове фото не пов'язує нікого. Слабкий, відхилено. Face-кандидат, LinkedIn «Rui Costa», зазначений як будівельник, був тонким, але справжнім — 68% збіг обличчя, лише обличчя, без збігу ідентичного файлу. Я його відклав.

Глухий кут архіву. Приватний профіль мав чистий красивий URL, тож я перевінив вебархів на старішу, публічну версію. Було два знімки — багатонадійно, поки я їх не відкрив.

Пошук у вебархіві

URL `instagram/r.costa.builds`

знімків знайдено: 2

2020-08-02 захоплено

2023-01-19 захоплено

відкриваю 2020-08-02 ...

збережено стіну входу

відкриваю 2023-01-19 ...

збережено стіну входу

обидва = шлюз входу платформи

Два знімки, обидва стіни. Нічого.

Обидва знімки захопили лише шлюз входу платформи, а не публічну версію сторінки. Поширений провал — архів зберігає те, що було видно в момент захоплення, а тут це була стіна. Глухий кут. Занотуй, іди далі. Не кожен шар віддає результат; це нормально, а прогін, де кожен шар віддає результат, — це прогін, якому варто не довіряти.

Що насправді втрималося. Дві нитки вижили. Перша: LinkedIn «Rui Costa» — те саме обличчя, що й аватар, на око, 68% за рушієм — зазначав точно того підрядника, якого коментар назвав його роботодавцем. Друга: пошук імені цілі плюс той роботодавець виніс публічний допис у Facebook від друга, «Tiago M.», який позначив якогось Rui Costa на будмайданчику 2023 року, на тому самому проєкті, що описував матеріал. Це був контент, витіснений начисто з приватного профілю на сторінку друга.

Де це лишає драбину. Вишикуй їх чесно. Зв'язок обличчя — помірний: пристойна схожість, але лише обличчя, на 68%, без збігу ідентичного файлу, щоб прицвяхувати. Публічна позначка теж помірна: вона прив'язує *якогось* Rui Costa до проекту, але не остаточно до *цього* приватного Instagram. Дві помірні нитки, що вказують в один бік, — справжній сигнал, але дві помірні нитки не є однією сильною, і складання їх не підвищує їх.

Тож я відзвітував це як помірний — імовірно та сама людина, але на одну незалежну нитку менше за сильний, і сказав саме так. Я розповів редакції, як виглядала б третя нитка — ідентичний файл аватара деінде, спільний, що міг би поставити акаунти разом, деталь біо, що збігається крізь платформи — і що поки одне з цього не приземлиться, я не поставлю свого імені під сильним, не кажучи вже про підтверджено. Цитату, що тримається на особистості, не запускають на помірному. Редактори отримали чесний щабель, а не лестивий. Ця стриманість — це робота.

Де зупинитися

Той профіль був приватним *навмисно*, і все, що я використав, було опубліковано кимось іншим на видноті. Це лінія, і це справжня лінія. Прочитати публічну позначку друга — це робота з відкритими джерелами. Умовити того друга прийняти фейковий запит, щоб ти побачив приватний список, — ні; це обман, це порушує правила платформи, а в юридичній справі це може отруїти всю справу. Дивися крізь вікна, які лишили відкритими інші люди; не зламуй замка.

І поважай *початковий контекст*. Фото, яке друг виклав на вечірці, було задумане як фото з вечірки, а не як доказ у твоєму файлі. Збирай те, що служить справжньому суспільному інтересу, і коли той інтерес закінчується, зупинися.

Вправа

Зроби це на собі. Розлогінься звідусіль, відкрий чистий браузер і спробуй відновити власний приватний профіль лише з кільця — ніколи з власної сторінки.

- Знайди свій стабільний числовий ID крізь будь-який маршрут, який твоя платформа досі відкриває. Запиши його.
- Реверс-шукай власний аватар, якщо він публічний. Де ще з'являється те обличчя чи файл?

- Пошукай власне ім'я плюс місто в полі пошуку кожної платформи. У що тебе позначали друзі?
- Перевір вебархів на старі публічні версії твого профілю — і перевір, що насправді захопив кожен знімок.
- Прочитай публічні списки трьох друзів вручну. Ти знову з'являєшся в них?

Тоді напиши власний рядок упевненості: чи міг би незнайомец, лише з кільця, дійти до *сильного* на тобі — чи лише до *помірного*? Більшість людей у шоці, як далеко несе кільце. Полагодити власне кільце — найкращий урок приватності з усіх, і найшвидший спосіб зрозуміти метод зсередини.

Підсумок

- Приватність обмежує твій погляд на одну сторінку; вона рідко обмежує те, що *інші* опублікували про ціль.
- Робота цього розділу — підтвердити підозрюваний збіг через відкрите кільце.
- Картографуй відкрите кільце довкола цілі — спільні зв'язки, позначки, коментарі, групи, кеші, архіви, аватар, переглянутий вручну FOAF — а не закритий центр.
- Спершу зафіксуй якір на стабільному числовому ID; він переживає перейменування — навіть попри те, що ти більше не можеш просто прочитати його з коду сторінки на головних платформах.

- Знай, який класичний рух помер: витягання ID з коду сторінки, URL спільних на два ID і скриптовий скрапінг списків друзів закриті чи проти правил. Принцип виживає в кожному; знайди поточний еквівалент.
- Не засвіти себе: перегляд із залогінованого сок-акаунта може винести *тебе* цілі через «людей, яких ви можете знати». Спершу підготуй акаунт.
- Витісна інформація — усе одно відкрита інформація; ти просто збираєш її з адрес інших людей.
- Чекай глухих кутів: мертві трюки, застарілі знімки архіву, типові спільні зображення, збіги того самого імені з іншою людиною. Відхиляй їх уголос.
- Дві помірні нитки не є однією сильною. Приземляйся там, де приземляються докази.
- Читай відкриті вікна, ніколи не зламує замість; поважай початковий контекст; зупиняйся, коли зупиняється суспільний інтерес.



РОЗДІЛ ДРУГИЙ

Павутина нікнеймів

Один нік — це нитка. На цьому рівні ти сплітаєш усю павутину.

У першому томі ти навчився брати нік і перевіряти, чи існує він на інших сайтах. Це базовий рух — неймчекінг.

Корисний, і недостатній. Він вручає тобі список URL, які відповіли, а список URL — це не особистість.

Цей розділ — про наступну висоту. Не «чи існує цей рядок деінде», а «які з цих хітів — *та сама людина*, як саме ця конкретна людина *мутує* свої ніки і де вся їхня павутина згортається в одну захищену особистість».

Нік — це наведення. Людина — це висновок. Робота — це відстань між ними.

Ідея: рядки дешеві, люди дорогі

Перелічування дешеве. Ти можеш прогнати один нік проти семисот сайтів за хвилину й отримати сорок зелених галочок. Це відчувається як прогрес. Це не так — це сорок *гіпотез*, більшість із них хибні. Деякі — заглушки зарезервованих імен. Деякі — не пов'язані люди, яким випадково сподобалося те саме слово. Кілька — твоя ціль.

На цьому рівні ти інвертуєш зусилля. Перелічування — це дешева основа піраміди; дорога вершина — підтвердити, що конкретний хіт — це конкретна людина, за її *контентом*, *датами й фото*, — ніколи за самим рядком.

Три ідеї роблять тут основну роботу.

- Граматика імен. Це стрижнева ідея розділу, тож сповільнись на ній. Людина не обирає ніки навмання. Вона мутує їх послідовним, особистим способом — завжди підкреслення, завжди рік народження в кінці, завжди те саме щасливе число, завжди ті самі лит-заміни, та сама улюблена основа, перекомбінована. Ця звичка — *відбиток пальця, зроблений із виборів*. Двоє людей можуть ділити рядок випадково; майже жодні двоє не ділять цілу граматику випадково. Тож віддача йде у два боки. Назад — збіжна граматика підтверджує, що розкидані акаунти

мають одного автора. Уперед — і це та частина, якої неймчекінг ніколи тобі не дає — щойно ти прочитав граматику, ти можеш *генерувати ніки, яких людина тобі не показувала, і йти їх знаходити*. Ти перестаєш реагувати на зелені галочки інструмента й починаєш передбачати, де живе ціль.

- Пастка однофамільців у масштабі. Поширений нік — це багато людей. shadowwolf — це не людина; це демографія. Що рідкісніший рядок, то вищі шанси, що два хіти мають одного власника. Рідкісність — твій друг; поширеність — це болото.
- Підтвердження через збіжність. Одна зелена галочка слабка. Зелена галочка *плюс* той самий рідкісний аватар *плюс* фраза біо, перевикористана дослівно, *плюс* дати створення, що вкладаються в одне життя, *плюс* той самий соцграф — ось як рядок стає людиною. Драбина першого тому, застосована в масштабі.

Метод, крок за кроком

Крок 1 — Перелічуй широко, більш ніж одним інструментом. Прожени сід-нік крізь щонайменше два еnumератори. Кожен несе *інший* список сайтів, тож їхні результати розходяться — один знаходить форум, який інший ніколи не перевіряє. Два інструменти, більше покриття, а розбіжність між ними — це вже сама по собі інформація.

Ось як виглядає справжній прогін — брудний, не чистий:

```
SEED  nyx_falken
-----
[+] github      200  живий профіль
[+] reddit      200  живий профіль
[+] steam       200  живий профіль
[-] instagram   404  не знайдено
[+] twitter/x   200  живий профіль
[?] tiktok      timeout (повтор)
[?] mastodon    429  ліміт запитів
[+] pinterest   200  РЕЗЕРВ-сторінка
[-] twitch      404  не знайдено
-----
9 перевір  5 живих  2 404  2 невід.
NOTE: pinterest = заглушка, не
      справжній профіль. перевір оком.
```

Що друкує еnumератор нікнеймів

Читай цю коробку так, як читає професіонал. П'ять живих хітів — але «хіт» Pinterest — це заглушка зарезервованого імені, хибнопозитив, який інструмент не відрізняє від справжнього профілю. Таймаут TikTok і ліміт запитів Mastodon — це *невідомі*, а не «ні» — провалена перевірка зазвичай означає, що мережа тебе заблокувала, а не що акаунта нема. Прожени їх пізніше з іншої адреси, перш ніж списувати. Інструмент каже тобі, що URL відповів. Він ніколи не каже, хто за ним стоїть.

Крок 2 — Тріаж кожного хіта оком. Відкрий кожен живий профіль. Це твій суб'єкт, не пов'язана людина чи сквотер? Забери півот-матеріал зі справжніх: відображуване ім'я, біо,

лінковані URL, інші ніки, які вони згадують, аватар. Кожен новий нік, який вони *самі декларують*, — золото; самодекларований зв'язок між двома акаунтами — це майже підтвердження, куди сильніше за будь-який збіг рядків, що ти вивів.

Крок 3 — Прочитай граматику імен. Поклади підтверджені ніки поряд і знайди патерн. Ця людина завжди додає рік народження? Завжди міняє а на 4? Завжди ім'я-підкреслення-іменник? Щойно побачиш граматику — згенеруй варіанти, яких вони *ще не* використовували, і протестуй їх. Ти перестаєш вгадувати навімання й починаєш передбачати.

Крок 4 — Зважуй за рідкісністю. Перш ніж довіритися будь-якому крос-платформному збігу, спитай, наскільки рідкісний рядок. Виразне вигадане слово — *nyx_falken* — перенесене крізь чотири платформи — це сильний пріор. Словникове слово — *nightowl* — перенесене крізь чотири платформи — майже нічого не значить, бо тисячі не пов'язаних людей обрали його незалежно. Скоригуй свою впевненість під рідкісність рядка *перш ніж* дивитися на будь-що інше.

Крок 5 — Підтверджуй на контенті, а не на рядку. Це крок, який пропускають аматори. Для кожного кандидата вишикуй *докази, що переживають ім'я*: аватар (той самий файл, або те саме обличчя на різних фото), формулювання

біо, перевикористане слово в слово, дати створення, що вкладаються в одну правдоподібну хронологію, ті самі друзі, що з'являються в різних акаунтах, ті самі тики письма. Коли кілька з них збігаються на одній людині — у тебе є особистість. Коли *єдине* спільне — це нік, у тебе є збіг у костюмі.

Крок 6 — Постав на драбину й зупинися на чесному шаблі. Звітуй той щабель, якого ти насправді досяг.

Спробуй (2026). Прожени один нік крізь Sherlock чи Maigret — або вебчекер типу WhatsMyName — щоб отримати живий крос-платформний список хітів, тоді відкрий кожен хіт і перевір його за контентом, ніколи лише за зеленою галочкою. Списки сайтів і правила виявлення гниють, тож стався до виводу будь-якого одного інструмента як до відправної точки й переперевірай промахи зі свіжої адреси.

Розібраний кейс, із відхиленням двійником

Сідом був один нік зі звіту про шахрайство на маркетплейсі: пух_falken. Наскрізь вигадано, справжній метод. Клієнт хотів єдину особистість за ним або чесне «дійти туди не можу».

Широке перелічування дало мені прогін із коробки вище — GitHub, Reddit, Steam, Twitter/X живі; Instagram і Twitch відсутні; TikTok і Mastodon невідомі; Pinterest — заглушка.

П'ятеро справжніх дверей, а `пух_falken` — вигадане слово, не словниковий термін. Хороший пріор рідкості. Я почав з надією, але з дисципліною.

Тріаж. GitHub був найбагатшим. Біо профілю читалося: *«code by night, ramen by day — falkennest.dev.»* Він сам декларував особистий домен. Акаунт Reddit активно постив у сабреддіті про механічні клавіатури. Steam показував публічний профіль, кіберпанковий аватар. Twitter/X: той самий вигаданий нік, акаунт, зосереджений на артї.

Граматика імен. GitHub, Reddit, Steam і особистий домен усі використовували `пух_falken` чи `falken`. Домен — `falkennest.dev` — додав нову основу, `falkennest`. Я переперелічив цю нову основу свіжим прогоном — попередній прогін завжди тестував лише `пух_falken`, ніколи `falkennest` — і він виявив акаунт Mastodon `@falkennest@fosstodon.org`. Граматика тепер читалася: префікс `пух` або основа `falken(nest)`, малими літерами, іноді підкреслення. Це дало мені передбачити й підтвердити акаунт Mastodon, а не наштовхнутися на нього.

Двійник. `пух_falken` у Twitter/X виглядав як легка п'ята платформа. Я мало не залогоував його як збіг лише за ніком. Тоді я перевінив контент замість рядка.

```
HANDLE   nux_falken   (twitter/x)
-----
ім'я      "Nux | comm status: OPEN"
біо       furry-художниця, she/her, EST
аватар    ориг. арт, БЕЗ реверс-хіту
створ.    2019-06 (розкод. з id)
-----
проти GitHub nux_falken
приєдн.   2022-11 (сторінка, не id)
біо       чол., рамен, клавіатури
домен     falkennest.dev (без лінка)
-----
ВЕРДИКТ   той рядок, інша людина
```

Що виявляє крос-платформна перевірка

Усе розійшлося. Інші займенники, інший самоопис, акаунт, створений на *три роки раніше* за той, що на GitHub, — і зауваж, що дві дати походять із різних джерел: дата Twitter/X розкодована зі snowflake-ID акаунта — числа, у яке математично вбудований час створення акаунта, тож воно розкодовується в точну дату, — тоді як дата GitHub — це просто рядок «Приєднався», надрукований на публічній сторінці профілю, не розкодований із жодного ID, — оригінальний аватар без спільного файлу й жодного лінка назад на falkennest.dev. Той самий рідкісний рядок, двоє не пов'язаних людей — пастка однофамільців у масштабі, що б'є навіть по вигаданих словах, бо друга людина може незалежно вигадати те саме або схопити звільнений нік. Відхилено як ціль. Я залогував акаунт Twitter/X як окрему людину й викреслив його з особистості.

Підтвердження через збіжність. Що насправді трималося до купи: GitHub, Reddit, Steam, домен *falkennest.dev* і акаунт Mastodon. Я хотів жорсткий ідентифікатор із того домену — email, ім'я реєстранта — і не отримав, і варто сказати чому, бо багато старіших туторіалів тут тобі збрешуть. У 2026-му WHOIS-запис *.dev* за замовчуванням приховано заради приватності. Ім'я й email реєстранта сховані за реєстратором; нема публічної сторінки з локальною частиною email, яку можна прочитати. Цей легкий трюк зник для більшості сучасних TLD. Лишаються два вузькі шляхи, обидва із застереженнями. *Історичний* WHOIS — знімки, заархівовані до того, як приватність стала нормою, — іноді зберігає сирого реєстранта, але цей домен був надто молодим, щоб мати такі. *Логи прозорості сертифікатів* записують кожен TLS-сертифікат, виданий для домену, і зрідка з них витікає піддомен чи контактна адреса; тут вони показали лише власну адресу реєстратора. Тож домен заслужив свою вагу чесно — як зв'язок, який суб'єкт *задекларував сам* у біо GitHub, а не як таємний email, який я розшифрував.

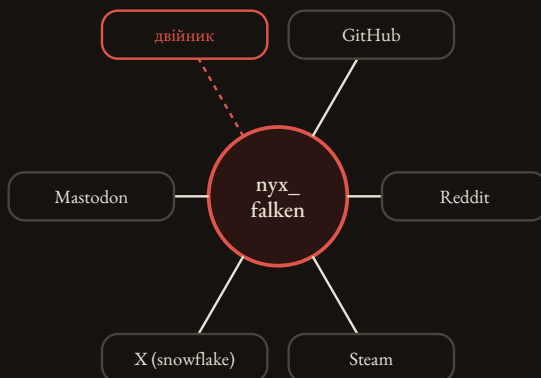
Решта набору трималася на доказах, що переживають перейменування. Біо Mastodon перевикористало дослівну фразу з GitHub — «*code by night, ramen by day*» — слово в слово, незвичний рядок, навряд чи випадковий. Steam і Reddit ділили той самий файл кіберпанкового аватара (ідентичний ресурс, не двійник). Дати створення

вишикувалися в одну правдоподібну дугу 2021–2022.

Сигнали збігаються: дослівна фраза біо на двох платформах (сильний), ідентичний файл аватара ще на двох (сильний), самодекларований особистий домен, що зв'язує набір (сильний), послідовна граматика імен (помірний). П'ять платформ, одна людина — і, що критично, *не* акаунт Twitter/X, який ділив нік.

Я відзвітував сильний — одна особистість на GitHub, Reddit, Steam, Mastodon і особистому сайті — і назвав відхиленого двійника з Twitter/X явно, щоб ніхто нижче за течією його не додав назад. Я не заявляв підтверджено: суб'єкт ніколи не зв'язав усі акаунти в одному місці, і жоден єдиний жорсткий ідентифікатор не розв'язав весь набір унікально. Сильний був чесним щаблем.

МЕРЕЖА НІКНЕЙМІВ



одна звичка на всіх платформах — перевіряй кожну за змістом

Один сід-нік розгортається на багато хітів; контент і граматику стягують справжні в одну особистість, а двійник із тим самим рядком відсікається.

Нотатка про пастки, які ти зустрінеш

Перевикористані ніки — класична пастка. Хтось кидає nux_falken; за рік інша людина хапає звільнене ім'я. Тепер рядок охоплює двох людей крізь *час*, а не лише простір. Дати створення — твій захист: нік, що «передую» відомій активності людини, — це перейменування чи перевикористання, а не машина часу.

Поколінневі ніки й лит-написання розширюють граматику. Людина, що була xX_dragon_Xx у чотирнадцять, може бути dragon.eth у двадцять вісім — та сама людина, еволюціонований неймінг. Читай дрейф, не дай себе ним

обдурити. І пам'ятай зморшку епохи LLM: стиль письма, колись надійний тайбрейкер, вирівнюється AI-асистованим складанням. Спирайся сильніше на жорсткі інваріанти — дати створення, спільні файли зображень, самодекларовані зв'язки — коли проза стає підозріло гладкою.

Вправа

Обери відомого open-source розробника з публічною присутністю — того, хто *хоче*, щоб його знаходили крізь платформи, щоб це лишалося твердо на відкритій території. Не обирай приватну особу.

- Засій його найуживаніший нік у два різні еnumератори й порівняй результати.
- Випиши його граматику імен одним реченням. Передбач один нік, який він використовує і якого не знайшов жоден інструмент, тоді перевір.
- Для трьох хітів підтверди ту саму людину на *контенті* — файл аватара, формулювання біо, дата створення — а не на рядку.
- Навмисно полюй на двійника: когось, хто ділить нік і *не* є твоїм суб'єктом. Відхили його письмово, зі своєю причиною.
- Назви свій фінальний шабель і той єдиний доказ, що штовхнув би тебе на наступний.

Підсумок

- Перелічування дешеве й дає гіпотези, а не особистості; дорога, вирішальна робота — це підтвердження.
- Читай граматику імен людини — її послідовний патерн мутації — і передбачай ніки, а не лише натакайся на них.
- Зважуй кожен збіг за рідкісністю: вигадані рядки несуть вагу атрибуції, словникові слова — це болото.
- Пастка однофамільців б'є навіть по рідкісних ніках — той рядок, інша людина, або перевикористане ім'я крізь час. Відхиляй двійників явно.
- Підтверджуй на тому, що переживає перейменування: файл аватара, дослівне формулювання біо, дати створення, соцграф, самодекларовані зв'язки — ніколи на самому рядку.
- Стався до 404 як до «ні», але до таймауту й ліміту запитів — як до «невідомо»: переперевір, перш ніж списувати акаунт.
- Постав усю павутину на драбину й звітуй досягнутий щабель; сильний — чесно, підтверджено потребує самозв'язку чи унікального жорсткого ідентифікатора.



РОЗДІЛ ТРЕТІЙ

Telegram зблизька

Чому числовий ID — це якір, а нік — лише костюм

Люди сприймають Telegram як приватну кімнату. Це не так. Це скляна коробка, яку вони плутають зі стіною.

Вони замикають свій профіль, ховають номер телефону, обирають анонімний нік — а тоді йдуть і *постять* у дюжині публічних груп, пересилають повідомлення одне одного й заходять о тій самій годині щовечора. Кожне з цього — відбиток, лишений на видноті. Нічого з цього не потребує ордера, входу в їхній акаунт чи бодай одного надісланого їм повідомлення.

Цей розділ — про те, як читати ці відбитки добре. Тут ми йдемо вглиб однієї платформи й одного факту, що робить атрибуцію в Telegram довговічною.

Одна заувага 2026 року, перш ніж почнемо, бо вона змінила ставки. Після зміни політики Telegram у вересні 2024 року — тієї, що настала після арешту його засновника у Франції — Telegram тепер розкриває IP-адресу й номер телефону користувача владі за дійсним юридичним запитом у кримінальній справі. Це реально, і це важить. Але це важіль для правоохоронців із судовим ордером за спиною, а не інструмент для тебе, і ніщо в цьому розділі його не торкається. Що ця зміна підтверджує ззовні — це саме той урок, на якому ми будуємо: числовий ID акаунта — довговічний хребет особистості, те, від чого відштовхується кожна система. Юзернейми пішли в інший бік — ними тепер відкрито торгують як активами на власному маркетплейсі Telegram, Fragment, купують, продають і перереєстровують на незнайомців. Костюм має вартість перепродажу. Число не переходить із рук у руки.

Нік — це костюм. Число під ним — це людина.

Одна річ, на якій усе тримається: ID, а не username

Кожен акаунт Telegram несе постійний числовий ID, виданий при реєстрації й ніколи не змінюваний. @username, що сидить зверху, змінний — його можна перейменувати, кинути, продати чи пізніше застовпити геть незнайомій людині.

Цей розрив — уся гра.

- Числовий ID — це додатне ціле, присвоюване приблизно по порядку в часі. Старіші акаунти мають нижчі числа. Це якір.
- ID групи чи каналу від'ємний — супергрупа показується як -100, приклеєне до її внутрішнього числа, тоді як звичайна (не супер) група — це просто від'ємне число без префікса -100 (наприклад, -4829103), маленький натяк, що чат старіший чи простіший.
- @нік — це знімок. Він каже тобі, хто тримає це ім'я *сьогодні*. Завтра не обіцяне.

Тож перший рух у будь-якій справі Telegram той самий, щоразу: розв'яжи нік до його числового ID, і відтоді стався до ID як до свого суб'єкта. Усе довговічне — вік акаунта, минулі імена, історія груп — прив'язується до числа.

Резолвер робить перетворення. Деякі — боти (типу @username_to_id), деякі — вебінструменти без входу. Для

власного контакту пересилання одного з їхніх повідомлень боту-інфо повертає ID відправника — але тільки якщо вони не поставили переслані повідомлення відв'язуватися від акаунта, у такому разі ти отримуєш ім'я і жодного клікабельного профілю. Це твій перший глухий кут, і він не буде останнім.

```
resolve @nightferry_kv
id:      512883471
username: @nightferry_kv
name:    "kv"
status:  ok
```

Резолвер нік → ID у дії

Запиши ID. Тепер це якір справи.

Спробуй (2026). Візьми @нік і розв'яжи його до числового ID користувача: перешли одне з повідомлень акаунта боту-ID типу @username_to_id — наприклад, @username_to_id_bot чи @usinfobot; спробуй один, а якщо він видає помилку або зник, спробуй інший — або встав нік у вебінструмент «username to ID» без входу й прочитай число назад. Те число постійне. Але роби це обережно: будь-який сторонній резолвер чи бот-ID *бачить твій запит* — твій акаунт, час і точний ID, про який ти спитав, — тож запускай його лише з чистого дослідницького акаунта, ніколи проти рідкісного ID у центрі справи, який ти найбільше хочеш захистити. Бадьорий «корисний» бот виглядає саме як пастка-приманка.

Інструменти, простими словами

Майже все в цьому розділі спирається на дрібні спільнотні інструменти — переважно боти, кілька вебсторінок. Перш ніж використовувати будь-який із них, тримай один факт непорушним: *тип* інструмента важить куди більше за його ім'я, бо хоч би який конкретний бот ти знайшов, він буде мертвим чи перейменованим, коли знадобиться знову. Вивчи п'ять категорій.

- Резолвери перетворюють @нік на його числовий ID і назад. Це єдиний довговічний трюк, бо ID ніколи не змінюється.
- Оцінювачі віку вгадують, коли акаунт створено, читаючи його ID проти таблиці відомих дат реєстрації. Оцінка, ніколи не справжня позначка часу.
- Спостерігачі історії звітують старі імена й ніки, які акаунт колись використовував, — але лише зміни, які інструмент особисто бачив зсередини спільних груп.
- Індексатори членства заявляють, що перелічують публічні групи, до яких належить ID, зібрані з їхнього власного краулу публічних чатів. Завжди недооблік.
- Боти-пошуковики беруть номер телефону чи нік і повертають краудсорсне ім'я. Це чутка з наклейкою, а не особистість.

Чому число довговічне: два швидкі читання з ID

Щойно ти тримаєш ID, дві речі випадають із нього напрому — без жодного контакту з ціллю.

Вік акаунта. Оскільки ID лізуть угору приблизно по порядку, ти можеш оцінити, коли акаунт народився, інтерполюючи між ID, чиї справжні дати реєстрації відомі. Спільнотні інструменти тримають таблиці цих якірних пар і читають твій ID проти кривої. Це *оцінка* — точна там, де якірні точки густі, розмита в розріджених ділянках, — тож стався до неї як до « $\pm$ (дні до тижнів)», ніколи як до точної позначки часу.

Навіщо? Це ловить брехню про вік. «Давній учасник», чий акаунт має три тижні, — свіжовиготовлений сокпапет. Кластер акаунтів, усі народжені того самого пополудня, — скоординована партія. Це сам собою *помірний* сигнал, а сильний — коли шикується з іншими доказами.

Історія імен і ніків. Telegram не публікує жодного API історії. Але боти-спостерігачі роками сидять усередині мільйонів публічних груп, тихо логуючи кожну зміну імені й ніка акаунтів, з якими ділили кімнату. Запитай одного за ID — і він звітує переходи, які особисто засвідчив: старі персони, ребрендинг із бруднішого ніка на чистий.

Жорстке застереження, і скажи його вголос: ти бачиш лише те, що спостерігач спостеріг. Перейменування, що сталося

до того, як той бот бодай раз ділив групу з акаунтом, ніхто не записав. Його відсутність у звіті — не доказ, що воно ніколи не відбувалося. Це розвідка, обмежена спостереженням. Вона дає тобі наведення, а не повний реєстр.

Пошук людини через групи, у яких вона постить

Ось рух, який більшість початківців прогавлює. Тобі рідко треба кудись вламуватися. Тобі треба знайти, *де людина вже говорить на видноті*, і прочитати це.

Два напрямки:

Згори вниз — у тебе є людина, ти хочеш її кімнати.

Боти-індекси членства заявляють, що перелічують публічні групи, у яких ID є чи був. Вони працюють, скраулівши публічні групи в масштабі, записуючи кортежі «(цей ID) бачено в (цьому чаті)». Ти запитуєш *їхній* лог, а не Telegram. Тож: масивний недооблік, приватні групи ніколи не з'являються, дати «востаннє бачено» — нижні межі, а деякі з цих ботів годуються скрапленими чи даними витоків — застарілими, хибними, а іноді незаконними для опори. Використовуй вивід як список *місць, куди піти подивитися вручну*, не більше.

Знизу вгору — у тебе є кімнати, ти хочеш людину. Якщо ти вже знаєш кілька цікавих груп, витягни кожен список учасників і перетни їх. Акаунт, що з'являється в *усіх* них, — твоє координаційне ядро, і ти знайшов його, не довіряючи

жодному боту членства. Витяг списку з великої супергрупи вибирається в кілька тисяч імен, тож ти отримуєш вибірку, а не всю кімнату; відсутність у твоєму експорті ніколи не доводить нечленства. Адміні також можуть повністю сховати список учасників, а канали-мовлення зазвичай узагалі не показують підписників — ти бачиш лише тих, хто коментує.

У будь-якому разі виграш той самий: щойно ти в публічній групі, де ціль постить, ти читаєш те, що вона *каже*, а сказане розкриває куди більше за членство.

Читання активності: розпорядок як відбиток пальця

Позначки часу дописів людини, зібрані за пару тижнів, малюють форму. Скластеризуй їх — і тиха смуга, години без активності, — це приблизно коли вона спить. Той провал наближає її часовий пояс, а часовий пояс звужує регіон, навіть для акаунта з фейковим ім'ям і без фото.

Наклади зверху *що* вона постить: мову, сленг, локальні відсилання, футбольний клуб, коли вона нарікає на дорогу до роботи. Ніщо з цього — не одне чисте число. Це повільне накопичення дрібних натяків, кожен слабкий, що разом лізуть драбиною від *слабкого* до *помірного* і — з підтверджувальним хітом з іншої осі — до *сильного*.

Пильнуй пастки. Заплановані дописи брешуть про години постера. Спільний акаунт, керований двома людьми у двох часових поясах, розмазує патерн у шум. А обережний оператор постить навмисно поза графіком, щоб ввести тебе в оману. Часовий пояс із таймінгу — це наведення, яке ти підтверджуєш, ніколи не вердикт, який ти оголошуєш. Розділ сьомий покаже, *чому* це лише наведення: дві різні людини з того самого міста й тієї самої онлайн-сцени за замовчуванням поділяють ці патерни, тож збіг таймінгу між двома акаунтами сам собою не є доказом того, що це одна людина.

Оператор бачить твій запит

Ось річ, яку тобі не скаже ніхто, хто продає ці боти, і це найважливіший абзац у розділі. Щоразу, коли ти надсилаєш запит стороннього резолвера, спостерігача історії, індексатора членства чи бота-пошуковика, ти вручаєш своє питання незнайомцеві. Людина, що керує тим ботом, бачить твій запитуючий акаунт, час, коли ти спитав, і точний ІД чи номер, про який ти спитав. Інструмент — не торговий автомат. Це людина посередині, і вона читає середину.

Подумай, що це зливає: твій інтерес. Проти недбалої цілі це нічого не значить. Проти організованої — шахрайської бригади, кільця цькування, ворожої групи з власними технарями — це може бути вся справа. Реальна частка цих «корисних» ботів — це пастки-приманки: керовані тими

самими спільнотами, які слідчі досліджують, або дата-брокерами, що логують кожен запитуючий акаунт на перепродаж. Згодуй одному рідкісний ID у центрі твоєї справи — і ти щойно, можливо, сказав своїй цілі, що хтось шукає, і вручив їй нік, на який озирнутися. Це, конкретно, спосіб, яким слідчого викривають.

Тож працюй так, наче середина ворожа, бо іноді так і є:

- Віддавай перевагу офіційному клієнту й власному інструментарію. Усе, що ти можеш прочитати, сам прогорнувши публічну групу, читай так — це нікому нічого не розкриває.
- Припускай, що кожен сторонній бот тебе логує. Запитуй лише з чистого дослідницького акаунта, який ніколи не веде назад до тебе чи твого клієнта, ніколи зі справжнього.
- Не годуй оператора історією. Розв'яжи ID, якщо мусиш, але уникай вручати одному боту *весь* патерн рідкісних запитів, що сказав би людині за ним, над якою справою ти працюєш.
- Проти організованих цілей стався до резолверів і ботів-пошуковиків як до спалених за замовчуванням. Зручність ніколи не варта викриття.

Ніколи не використовуй якір-ID чи крос-платформний резолв, щоб зняти маску з

людини, яка анонімна заради власної безпеки.

Антикорупційне джерело, протестувальник за авторитарного уряду, викривач — той самий рух «нік → довговічне число», який ловить акаунт цюкування, — це саме те, за що ворожий клієнт заплатить, аби вказати на них. Замовлення, чий інтерес у знятті маски з такої людини — помста, а не підзвітність, — це червоний прапор, щоб відмовитися, а не бриф, який треба виконати. Інструменти цього розділу не знають різниці. Ти знаєш.

Боти-пошуковики: пасивне — не значить непомітне

Тебе спокушатимуть боти пошуку за телефоном і ніком — згодуй номер, отримай ім'я; згодуй нік, отримай «хто це». Використовуй їх з розплющеними очима, бо вони несуть чотири чесні проблеми.

- Вони обмежені за частотою. Безкоштовний тариф часто — один пошук на день. Масові запити позначають твій дослідницький акаунт і банять його.
- Вони інколи хибні. Ім'я з caller-ID чи краудсорсу може бути *старим власником* перевикористаного номера або міткою, яку зберіг якийсь незнайомец. Це наведення, а не особистість.
- Вони інколи порушують умови сервісу — або годуються дампами витоків, чиє використання може бути

незаконним за твоїм мандатом. Вирішуй це *до* запиту, а не після.

- «Пасивне» — не значить «непомітне».

Резолвінг-акаунт лишає сліди. Синхронізація контактів проти номера реальної людини — це акт обробки даних у багатьох місцях. Додати логуючий бот до чужої групи — зовсім не пасивно: це потребує згоди, якої в тебе нема.

Розібраний кейс: від чистого ніка до впевненого імені

Отримую від клієнта один нік: @nightferry_kv, прив'язаний до низькосортної кампанії цькування в регіональному спільнотному чаті. Це все. Ні імені, ні номера.

Спершу якір. Розв'язую його. ID 512883471. Відтепер ID — мій суб'єкт.



Змінний нік сидить зверху; постійний числовий ID під ним — те, від чого відштовхуються вік акаунта, історія імен і сліди груп.

Перевірка віку. Оцінка створення ставить акаунт приблизно на чотири роки. Не свіжий сокпапет — усталена особистість. Це корисно; це означає, що за ним можуть бути роки публічного сліду.

Перший глухий кут. Сам профіль чистий. Без фото, ім'я лише «kv», біо порожнє, лінкування пересланих повідомлень вимкнене. Акаунт не дає мені нічого напряму, а бот-пошук за ніком повертає:

```
query: @nightferry_kv  
ім'я (crowd): "Andriy Petrenko"  
телефон:      недоступний  
впевненість:  низька / неперев.  
note: crowd-мітка, джерело невід.
```

Що повертає бот-пошук за ніком

Ім'я. Спокусливо. І я відхиляю його — поки що. «Crowd-мітка, джерело невідоме» — це саме той caller-ID-подібний осад, що називає старого власника чи здогад незнайомця. Воно йде у файл як *непідтверджене, низька впевненість*, не більше.

Півот до історії ID. Я запитую спостерігача історії імен за числовим ID. Він звітує колишній нік, крізь який акаунт пройшов два роки тому: @k_veranko. Поточний акаунт

вичищений; *старий* нік не будували для цього.

Крос-платформно на старому ніку. Я проганяю @k_veranko — не поточний, а викинутий — крізь перелічування нікнеймів. Воно виявляє багаторічний, досі публічний акаунт на іншій платформі: той самий нік, аватар, біо з лінком на особистий блог, і ім'я з ініціалом: «Kateryna V.»

Тепер «Andriy Petrenko» з крауд-бота вже не просто виглядає непідтвердженим — він виглядає *хибним*. Два незалежні, самоопубліковані сигнали вказують на зовсім іншу людину. Крауд-мітку викинуто начисто.

Підтвердження на контенті групи. Назад у спільнотному чаті я читаю публічні дописи цілі за два тижні. Тихі години шикуються з локальним розкладом сну — правильний регіон. Повторювані відсилання до конкретного трамвайного маршруту й названого місця роботи. Старий блог із крос-платформного хіта згадує те саме місце роботи.

Це дві осі, що вказують в один бік: викинутий нік, простежений крізь платформи до блог-персони, і публічний контент групи, що ставить ту персону в те саме місто й місце роботи. Аватар на старому акаунті збігається з блогом; місце роботи назване у двох місцях, які вона опублікувала сама.

Тепер придивися пильно до того, що я насправді тримаю, бо саме тут початківці перебільшують. Ім'я — це ім'я з ініціалом — «Kateryna V.» — не повна особистість. Блог міг би

належати тезці. Спільне місце роботи наводить на думку, але не вирішальне в місті такого розміру. Числовий ID — *підтверджений* якір для *акаунта*, але стрибок від акаунта до конкретної названої людини все ще спирається на м'які, самоопубліковані збіги й один перевикористаний нік. Кожна ланка того другого ланцюга правдоподібна. Жодна з них не жорстка.

Вердикт: Я атрибутую до «Kateryna V.» на **помірний** впевненості — солідне, назване наведення, а не замкнена особистість. Щоб піднятися до сильного, я хотів би ще одну незалежну вісь: другу платформу, що прив'язує те саме обличчя до того самого повного імені, або документ. Я не маю ні того, ні того й не фабрикуватиму їх. Тож я звітую **помірний**, називаю дві опорні осі, позначаю відхилене крауд-ім'я, щоб клієнт бачив розвилку, яку я обрав, і прямо записую, що зрушило б стрілку. Глухий кут чистого акаунта ніколи не був перешкодою; *старий* нік, який він забув поховати, був входом — він просто не доніс мене аж до дому. Зупинитися на помірному й сказати так — це і є знахідка.

Зверни увагу, чого я ніколи не робив: я не приєднувався до приватної групи під фейковою легендою, я не писав цілі, я не надсилав логуючого лінка. Кожен крок читав публічну поверхню.

Вправа

Безпечне тренування (власний акаунт). Розв'яжи власний нік до числового ID будь-яким резолвером. Тоді прожени ID крізь оцінювач дати створення й порівняй результат із місяцем, коли ти насправді приєднався. Зверни увагу на межу похибки — цей розрив і є та невизначеність, яку ти маєш нести в кожне твердження про вік *чужого* акаунта. Не запитуй чужі номери для практики; використовуй лише себе.

У стилі CTF (публічні, згодні дані). Обери відомий публічний Telegram-канал з активною секцією коментарів. Не приєднуючись ні до чого приватного: збери видимі позначки часу дописів трьох найгаласливіших коментаторів за тиждень і накресли провал тихих годин кожного. Запиши часовий пояс, який ти б *вгадав* для кожного, — тоді перелічи, чесно, кожне альтернативне пояснення (планувальник, спільний акаунт, навмисне введення в оману), що зламало б твій здогад. Тренована навичка — не здогад. Це список способів, якими здогад хибний.

Підсумок

- Розв'язуй кожен нік до його числового ID на самому старті й стався до ID як до суб'єкта відтоді. Username — змінний костюм, тепер буквально виставлений на аукціон на Fragment; число — людина і ніколи не переходить із рук у руки.

- Два читання йдуть прямо з ID без контакту: вік акаунта (оцінка, ±дні-тижні — ловить сокпапетів і скоординовані партії) і історія імен/ніків (обмежена спостереженням — відсутність нічого не доводить).
- Знаходь людей через публічні групи, у яких вони постять: згори вниз через боти членства (недооблік, перевіряй вручну) або знизу вгору перетином списків, які ти витягнув сам.
- Таймінг активності наближає часовий пояс і розпорядок — повільне накопичення слабких натяків, підтверджене на другій осі, ніколи не оголошуване саме.
- Боти-пошуковики обмежені за частотою, інколи хибні, інколи порушують ToS чи живляться витоками. Ім'я від caller-ID може бути старим власником. Кожен вивід бота — наведення для підтвердження.
- Оператор бачить твій запит. Кожен сторонній бот вручає твій інтерес тому, хто ним керує — багато з них пастки-приманки чи керовані супротивником, і проти організованої цілі це спосіб, яким тебе викривають. Віддавай перевагу офіційному клієнту й власному інструментарію; запитуй лише з чистого дослідницького акаунта; стався до зручних ботів як до спалених за замовчуванням.
- Довговічний півот часто — це старий, невичищений нік, а не чистий поточний, — гони персону, яку ціль

забула поховати.

- Працюй лише з відкритими поверхнями — жодних приватних груп під фальшивим приводом, жодних повідомлень цілі, жодних логуючих лінків.



РОЗДІЛ ЧЕТВЕРТИЙ

Обличчя й фотографії

Фотографія — це дві зачіпки в одній: кадр і обличчя

Фотографія — найщедріша річ, яку людина може тобі вручити, і найнебезпечніша річ, яку ти можеш хибно прочитати. Щедро, бо несе дві зачіпки, зварені разом. Небезпечна, бо обличчя смикає за щось старше за судження — ти *бачиш* збіг, і твоє нутро кричить *це він*, перш ніж мозок зробив бодай якусь роботу.

Дві зачіпки в одному кадрі. Перша — усе, що в картинці: метадані, запечені у файл, вивіска крамниці за плечем, відображення в сонцезахисних окулярах. Друга — саме

обличчя: ключ, що може, іноді, відчинити інші двері на інших платформах.

Ми беремо обидві. Кадр тут — *легка* версія: досить, щоб прочитати фото на наведення. Глибока геолокація, мистецтво прив'язати картинку до даху з димаря й тіні, — це третій том. Тут ми лишаємося на рівні «що це фото каже мені про кого й де, і яку з цих ниток я можу потягти».

І перед усім цим одна жорстка лінія. Пошук за обличчям — найінтрузивніший інструмент у цій книзі. Ніщо інше з того, що ти вивчиш, і близько не стоїть.

Шаблон обличчя — це чутливі персональні дані, а інструменти пошуку за обличчям перебувають у правовій сірій зоні, що різко різниться від країни до країни. Клієнт, який тебе наймає, — це не закон, що дає тобі дозвіл. Перевір, що дозволено там, де ти працюєш, перш ніж запускати такий.

Кадр: що в картинці

Почни з файлу, перш ніж почати з обличчя. Дві причини. Це менш інтрузивно, і це часто працює краще.

Кожне оригінальне фото може нести EXIF — блок даних, який камера записує при зйомці. GPS-координати.

Позначку часу. Марку й модель телефону. Застосунок редагування, що торкнувся його останнім. На *оригінальному*

файлі це подарунок.

Заковика, і ти маєш це засвоїти: соцплатформи його зрізають. Instagram, Facebook, X, WhatsApp — майже всі вони стирають EXIF при заливці. Так само скріншот. Так само більшість PerezBerezhnyy. Якщо ти витягуєш фото профілю з Instagram і не знаходиш GPS, це не каже тобі нічого про те, де зроблено фото. Це каже тобі, що фото пройшло крізь Instagram.

```
ЧИТАЧ EXIF-МЕТАДАНИХ
Файл: holiday_original.jpg
-----
Make       : Apple
Model      : iPhone 13
DateTime   : 2024-08-03 17:42:11
GPS        : 41.3874, 2.1686
Software   : -
-----
Файл: profile_pic_from_ig.jpg
-----
Make       : -
Model      : -
DateTime   : -
GPS        : (немає)
Note: EXIF стерто при заливці
```

Читач метаданих — оригінал проти стертого платформою

Коли GPS *присутній*, стався до числа як до заяви, а не факту. GPS можна відредагувати чи підробити. Тож підтверджуй його: кинь координату в супутник чи street view і перевір, що фон збігається — будівлі, рельєф, вивіски. Якщо метадані

кажуть Фінікс, а кадр показує засніжені піки, вір пікам, а не числу.

Решту кадру читають оком і реверс-пошуком. Бейдж з ім'ям. Нік водяним знаком у кутку. Логотип на худі. Дорожній знак. Ці «середовищні якорі» — золото саме тому, що вони часто виживають, коли обличчя провалюється, і їх куди менш інтрузивно гнати.

Реверс-пошук зображень, зроблений як слід

Аматори заливають усе фото в один рушій, нічого не отримують і кидають. Ось професійна версія.

Прожени кілька рушіїв. У них різні індекси й різні алгоритми. Вони не взаємозамінні — нульовий результат на одному не є нульовим результатом. Груба поділка праці:

- Yandex — робоча конячка близьких збігів. Найкращий безкоштовний інструмент для пошуку *інших фото тієї самої людини*, сильний на східноєвропейському й кириличному вебі. Його схожість зважена в бік геометрії обличчя.
- Google Lens — читач сцени. Об'єкти, орієнтири, вітрини, текст у зображенні. Слабкий на обличчях за задумом (він придушує збіги особистості), сильний на всьому, що довкола людини.
- TinEye — трекер походження. Знаходить точні й майже точні копії й, що критично, може сортувати за

найстарішим, виявляючи, де картинка вперше сплила.
Жодного розпізнавання обличчя.

- Bing Visual Search — додатковий прохід. Інше покриття, ловить те, що інші прогавлюють. Сильно комерційний.

Спробуй (2026). Обріж туго до обличчя, тоді прожени той обріз крізь кілька рушіїв, кожен з яких робить іншу роботу (див. поділ праці вище). Тоді роби справжню роботу: відкривай *сторінки, на яких живуть хіти*, і читай ніки, підписи й коментарі — ніколи не роби висновку на балі схожості рушія, який є наведенням, а не ідентифікацією.

Обріж до суб'єкта. Це множник, що перетворює нуль на хіт. Більшість рушіїв чіпляється за найбільше обличчя чи об'єкт у кадрі. Якщо твій суб'єкт стоїть біля двох інших людей і великого пса, рушій може радо піти й ідентифікувати пса. Обріж туго до одного обличчя, одного знака, одного тату. Шукай кожне окремо.

Шукай обличчя проти всього зображення — навмисно, як два різні питання. Усе зображення знаходить *саме цю картинку* деінде: репости, оригінальне джерело, перевикористання катфішером. Тугий обріз обличчя питає інше: *де ще з'являється ця людина*, на інших фото, в іншому одязі, в інші роки. Ти хочеш обидві відповіді.

Трюк із віддзеркаленням. Шахраї й репост-акаунти часто дзеркалять зображення горизонтально, щоб ухилитися від виявлення точного збігу. Залий сам віддзеркалену копію другим проходом — з'являються нові хіти. Використовуй віддзеркалення, щоб *знаходити репости*, ніколи щоб *порівнювати обличчя*, бо дзеркалення спотворює асиметричні риси, які важать.

Попередження, що випливає з того, як ці рушії працюють: вони повертають схожість, ніколи не особистість. Кожен із них вручить тобі двійників, не змигнувши. Це не баг, який можна підкрутити.

Обличчя як вхід

Тепер саме обличчя. Маючи обличчя, спеціальні face-рушії шукають те саме обличчя деінде в вебі.

Зрозумій механізм, бо він пояснює режими провалу. Рушій виявляє обличчя, перетворює його на числовий ембедінг — вектор із кількох сотень чисел, що описують геометрію, — і знаходить найближчих сусідів до цього вектора у своєму індексі. «Збіг» — це близький сусід у векторному просторі. Це не відбиток пальця. Частота хибнопозитивів сильно гуляє від пози, освітлення, якості зображення й демографії. Власний бал упевненості рушія — не ідентифікація.

Покриття різниться від рушія до рушія, так само як для реверс-пошуку. Одні індексують відкритий веб — новини,

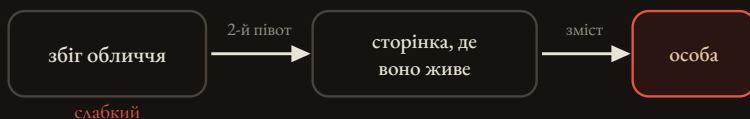
блоги, особисті сайти — і навмисно пропускають великі соцплатформи. Інші налягають на соцмережі й сірозонні каталоги. Ще інші спеціалізуються на регіональних мережах. Якщо твій суб'єкт східноєвропеець, загальний рушій може бути тонким там, де регіональний багатий.

Ось правило, що керує всією дисципліною, і це наскрізна лінія цієї книги:

Хіт обличчя — це наведення. Він лишається наведенням, поки контент його не підтвердить, — ніколи не щабель вище лише на силі збігу.

Ідентифікація не приходить від рушія. Вона приходить від *другого півота* — переходу від хіта обличчя до сторінки, на якій він живе, і читання її. Нік. Підписи. Коментарі. Хто позначений. Фон, який ти бачив на іншому фото твого суб'єкта. Ось де наведення стає знахідкою.

ОБЛИЧЧЯ — ЛИШЕ ЗАЧІПКА



рушій знаходить сусіда; півот робить знахідку

Хіт обличчя лише відчиняє двері. Перший півот приземляє тебе на сторінку; другий півот — читання контенту на тій сторінці — це те, що насправді ідентифікує. Бал збігу ніколи не лізе драбиною сам.

Одне обличчя, чотири двері, дві з них хибні

Дай пройти кейс. Наскрізь вигаданий, але форма справжня — включно з частинами, де все йде не так, а це більшість.

Клієнт наймає мене перевірити бізнес-контакт перед угодою. У мене є письмове уповноваження, але мандат клієнта — це не згода суб'єкта, тож перш ніж я щось прожену, я підтверджую, що робота захищувана там, де я працюю, що контакт — публічна ключова фігура, названа в паперах угоди, а не приватна особа, за якою стежать заради розваги, і що я спираюся лише на відкриті джерела. У мене одна річ, з якої працювати: фото профілю зі сторінки «Про нас» компанії. Чоловік, назвемо його Marco Feldt, середина сорока, просте портретне фото.

Крок перший, перед будь-яким face-рушієм: чи це взагалі реальна людина? Сокпапети й шахрайські профілі дедалі частіше використовують AI-згенеровані обличчя. Тож я шукаю класичні ознаки — асиметричні окуляри, викривлена межа волосся, спотворений текст на фоні, рідинні відображення в очах. Фото Марко не показує жодної з них. Але у 2026-му це нічого не вирішує. Нинішнє покоління

моделей зображень виправило ці видачі, і виявлення синтетичних зображень оком уже ненадійне — видимі ознаки здебільшого зникли. Тож чесне прочитання таке: «явних ознак нема, але це не доказ реальної людини». Я логую це як відкрите питання, а не закрите, і продовжую з вердиктом реальне-проти-синтетичного, що досі висить над справою, — чимось, що доведеться розв'язати пізнішому підтвердженню, а не моїм очам.

Я обрізаю туго до обличчя й проганяю крізь два рушії з різним покриттям.

```
ПОШУК ОБЛИЧЧЯ – РУШІЙ А
Query: marco_feldt_crop.jpg
-----
Результат 1 збіг 94% новини
    підпис: "M. Feldt, keynote"
Результат 2 збіг 91% той сайт
Результат 3 збіг 88% conf-стор.
Результат 4 збіг 71% сток-фото
    -> позначено: можл. повтор
-----
4 хіти. 1 позначено низьк. довір.
```

Face-рушій відкритого вебу — ранжовані хіти

Верхні три кластеряться на одному новинному сайті й сторінці конференції, усі називають М. Feldt на галузевій події. Це когерентно. Четвертий, на 71%, вказує на бібліотеку сток-фото — я відкладаю його як підозрілий і повернуся.

Рушій два, із соц-покриттям, дає мені четверті двері:

```
ПОШУК ОБЛИЧЧЯ — РУШІЙ В
Query: marco_feldt_crop.jpg
-----
Хіт 1 бал 82 X / нік
@m_feldt_biz bio: "founder"
Хіт 2 бал 79 LinkedIn
"Marco Feldt — CEO"
Хіт 3 бал 68 профіль знайомств
ім'я: "Marc, 41" місто: далеко
-----
Замало облич на Хіті 3 для рангу.
3 хіти. 1 неоднозначний.
```

Фасе-рушій із соц-покриттям — ранжовані хіти

Тепер у мене три кандидатні акаунти й два вільні кінці. Час робити справжню роботу — півоти.

Двері один, двійник. Хіт 3 на рушії В, «Marc, 41», на профілі знайомств в іншому місті. Бал обличчя — правдоподібні 68%. Моє нутро, якби я дав, занотувало б це як «той самий хлопець, таємне життя». Тож я читаю *контент*. Фото профілю знайомств містять випускний знімок, датований за роки до відомої кар'єри Марко, в університеті, який Марко ніколи не згадує, у країні, якої його перевірена історія LinkedIn ніколи не торкається. Дати не шикуються. Місце не шикується. Я відхиляю. Це двійник — реальна, інша людина, що випадково сидить біля Марко у векторному просторі. Фасе-рушій зробив саме те, що робить: знайшов близького сусіда. Це була моя робота, не рушія, помітити, що вони не можуть бути тією самою людиною.

Високий бал збігу зі зламаною хронологією — це не таємниця. Це незнайомець.

Двері два, глухий кут. Назад до того хіта сток-фото на 71%. Відкриваю. Обличчя Marco на роялті-фрі зображенні під назвою «впевнений бізнесмен в офісі». Ой-ой — чи це означає, що фото Marco фейкове, сток-зображення, вбране в SEO? Я проганяю трюк із віддзеркаленням і ще кілька реверс-проходів на самому сток-зображенні. TinEye, сортування за найстарішим. Копія сток-бібліотеки стара, але конференційні фото Marco, з названої події з датованою програмою, передують їй — і показують його наживо на сцені з іншими ідентифікованими, перевірними людьми. Що насправді сталося — нудне: сток-бібліотека скрапила чи перевиставила справжнє фото. Сток-хіт *не веде ні до кого*. Це репост без нової людини за ним. Реверс-пошук, що знаходить лише репости картинки, яку ти вже маєш, не знайшов тобі нічого. Я зачиняю двері. Щабля не здобуто, щабля не втрачено.

Двері три й чотири, справжні. Нік у X @m_feldt_biz і LinkedIn «Marco Feldt — CEO». Тут півоти окупаються. LinkedIn перелічує ту саму компанію, що й сторінка «Про нас», з якої я почав. Акаунт X, за місяці дописів, відсилає до тієї самої конференції з новинних хітів Marco — постить фото з події, ту саму сцену, з позначкою часу того тижня. Дві незалежні нитки — професійна сторінка й соцакаунт —

тепер узгоджуються щодо роботодавця, події й хронології. Я беру відновлений нік і проганяю крізь інструмент нікнеймів, щоб побачити, де ще живе m_feldt_biz, що виявляє збіжний профіль ще на одній платформі, самоавторський, те саме біо.

Де це лишає мене? Обличчя саме було слабким. Обличчя плюс один підтверджувальний акаунт було б помірним. Обличчя плюс два незалежні акаунти, що узгоджуються щодо роботодавця, події й дат, плюс послідовний нік крізь платформи — це сильний. Не підтверджено — підтверджено хотіло б чогось жорсткішого, прямої заяви, документа, власного визнання суб'єкта. Я зупиняюся на сильному й записую це як сильний, із ланцюгом, що привів мене сюди. Я не даю яскравому верхньому хіту на 94% спокусити мене назвати це підтвердженням.

Вправа, яку можна безпечно прогнати

Не практикуй це на незнайомцеві. Уся суть розділу в тому, що ти цього не робиш. Практикуй на *безпечному* суб'єкті, одному з цих трьох:

1. Собі. Обріж фото власного обличчя й прожени крізь пару реверс- і face-рушіїв. Побач, що відкритий веб тримає на тобі. Некомфортно, повчально й повністю зі згодою.
2. Охочому другові, який каже так, словами, спершу.
3. Публічній фігурі зі справжньою причиною — політику, керівнику, чию публічну роль ти законно перевіряєш.

Завдання: візьми одне фото. Прочитай спершу його кадр — чи є EXIF, чи його стерто? Якись якорі на фоні? Тоді прожени крізь щонайменше два різні реверс-рушії й, для згодного чи публічного суб'єкта, фасе-рушій. Для кожного хіта примусь себе написати один рядок: *це справжній новий сигнал, репост того самого зображення чи двійник?* Прожени один відновлений нік до другого акаунта. Тоді постав свій висновок на драбину — слабкий, помірний, сильний — і напиши ланцюг, що виправдовує щабель.

Якщо твоя чесна відповідь — «слабкий», зупинися там і скажи так. Навчитися зупинятися на слабкому — це навичка.

Підсумок

- Фото — це дві зачіпки: кадр (метадані, фон, якорі) і обличчя (крос-платформний ключ). Читай спершу кадр — він часто продуктивніший.
- EXIF — подарунок на оригінальних файлах і зазвичай стертий соцплатформами. Відсутній GPS нічого не доводить. Присутній GPS — це заява для перевірки проти фону, а не факт.
- Реверс-пошук як слід: кілька рушіїв, обріж до суб'єкта, шукай обличчя й усе зображення як *два різні питання*, використовуй трюк із віддзеркаленням для репостів. Кожен рушій повертає *схожість, ніколи не особистість*.

- Хіт обличчя — це наведення, знижене, поки контент не підтвердить. Ідентифікація приходить від другого півота — сторінки, а не рушія.
- Чекай глухих кутів: двійники, відхилені зламаними хронологіями, сток- чи AI-аватари, що ведуть ні до кого, реверс-пошуки, що знаходять лише репости. Чисто відхиляти їх — це робота.
- Приземляйся на захищений щабель і пиши ланцюг. Сильний — прекрасне, чесне місце зупинитися. Підтверджено потребує більшого за обличчя.
- І лінія, що керує всім цим: пошук за обличчям — найінтрузивніший інструмент, який ти маєш. Письмовий дозвіл, правова перевірка, лише відкриті джерела — і зупиняйся на лінії.



РОЗДІЛ П'ЯТИЙ

Витоки, оброблені чисто

Дані витоку як міст між особами — ніколи як ключ

Витік — це не скорочений шлях. Це перше, від чого треба відучитися.

Більшість людей, коли вперше чують, що email і пароль цілі десь плавають у якомусь дампі, відчувають легкий трепет доступу. *Я міг би зайти.* Відклади це. Ти ніколи цього не зробиш — принаймні не в межах цієї роботи. Те, що дає тобі витік, набагато корисніше й набагато менш захопливе: він дає тобі *нитку*. Той самий email у двох витоках. Той самий рідкісний пароль на двох акаунтах. Нікнейм, який виринає

поруч з адресою, яку ти вже мав. Це нитки, що зв'язують одну особу з іншою. Ти йдеш за ними. Ти ніколи не смикаєш їх, щоб відчинити двері.

Ти можеш перевірити, чи двері лишили відчиненими. Ти ніколи не можеш крізь них пройти.

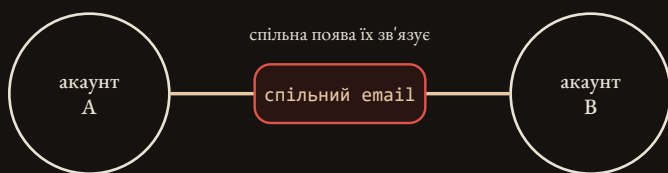
Ти вже знаєш, що нуль збігів у витоках не означає безпеку, лише неіндексованість. Тут ми йдемо глибше: що насправді каже тобі перевірка витоків, як email стає крос-платформним з'єднувачем, чому спільний пароль може зняти відбиток людини, і жорсткі межі кожного з цих кроків.

Ідея: витоки з'єднують, вони ніколи не заходять

Подумай, що таке насправді набір даних витоку. Сервіс скомпрометували, і його записи користувачів вилилися — email, іноді нікнейми, іноді паролі чи хеші паролів, іноді номери телефонів та адреси. *Лог стилера* — це знов інше: це вивід шкідливого ПЗ на власній машині людини, що записує кожен сайт, куди вона заходила, поки була заражена. Дві різні речі, і ти мусиш тримати їх окремо у своїх нотатках, бо вони означають різне про людину. Зсув 2026 року, який варто назвати: класичні комболисти дедалі більше витісняються свіжими логами стилерів — Redline, Lumma, MetaStealer, — якими торгують у Telegram-каналах, що парсять їх на льоту. Метод відбитка пароля нижче через це не змінюється; він так само зв'язує акаунти, лише *джерело* зсунулося.

Але для атрибуції — для роботи з доведення, що два акаунти належать одній людині — зміст важить менше, ніж *співпоява*. Коли dmitri.works@gmail.com виринає у витоку форуму 2019 року поряд з нікнеймом nightferry, ти тепер маєш зв'язок між email і нікнеймом. Коли той самий nightferry з'являється на ігровій платформі та на сайті обміну фото, email, з якого ти почав, тихо перетворився на карту слідів людини.

ВИТІК — ЦЕ МІСТ, А НЕ КЛЮЧ



Email, нікнейм чи пароль — це міст між двома особами: він дає тобі перейти від одного запису до іншого. Він ніколи не ключ: він не відчиняє — і не має відчиняти — акаунт на дальньому кінці.

Ніщо з цього не потребує пароля. А коли пароль *таки* потрапляє в картину, він потрапляє як *відбиток*, ніколи як обліковий запис для входу. Я повернуся до цього, гучно.

Метод: що дає перевірка витоків, і що вона приховує

Почни з найпростішого інструмента. Перевірка членства у витоках — Have I Been Pwned є сталомом — бере email і каже тобі, у яких відомих витоках він з'являється, коли вони сталися і які *класи* даних кожен з них розкрив. Паролі, дати народження, адреси, номери телефонів: вона називає категорії, а не значення. НІВР ніколи не видасть тобі пароль. Так задумано, і саме цей задум тримає її в межах закону.

Account: dmitri.works@gmail.com

Breaches found: 3

- Collection #1 (2019-01)
Exposed: Emails, Passwords
- ForumRunner (2016-08)
Exposed: Emails, Usernames, IP addresses
- MyFitDiary (2018-03)
Exposed: Emails, Passwords, Names, DOB

Що повертає перевірка членства у витоках

Прочитай це уважно, бо воно вже каже тобі багато без жодного пароля. Три витоки за три роки. Один з них, ForumRunner, розкрив *нікнейм* — це півот. Інший розкрив *ім'я і дату народження* — вони підкріплюють особу, яку ти, можливо, вже підозрюєш. Email зареєстровано щонайменше на трьох сервісах, один з них — щоденник фітнесу, що розміщує людину на цій платформі у 2018 році.

Тепер частина, яку новачки пропускають. Запусти ту саму перевірку на трохи іншій адресі — і можеш отримати ось це.

Account: d.works1990@outlook.com

Breaches found: 0

No pastes found.

Що повертає перевірка членства у витоках (порожньо)

Нуль. Що означає нуль? Він не означає, що акаунт чистий, безпечний чи фальшивий. Він означає, що *перевірятьник не проіндексував витік, який його містить*. Адреса може бути незапямованою. Вона може лежати в дампі, який ще ніхто не розібрав і не завантажив. Вона може бути новісінькою.

Порожній результат — це факт про *індекс*, а не про *людину*: дані, а не вердикт. Запиши це як «неіндексовано», ніколи як «без витоків».

Є ще одна річ, яку ці інструменти виносять на поверхню: *пасти*. Паста — це шмат тексту, який хтось скинув на сайт для вставок — Pastebin та його родичі — часто сирий список украдених облікових даних або комболист. Коли перевіряльник витоків каже, що твій email з'явився у пасті, він каже тобі, що адреса циркулювала в якомусь дампі, який скопіювали у відкритий доступ. Корисно як сигнал циркуляції. Але пасти неохайні, часто дубльовані й нерідко помилково підписані не тим «джерелом». Стався до збігу в пасті як до *помірного* доказу витoku щонайбільше, і піді прочитай дату й контекст пасти, перш ніж на неї спиратися. Одне застереження на 2026: збір паст значною мірою заморожений, відколи сайти вставок посилили доступ, тож цей канал зараз застарілий і мізерний — порожній рядок «no pastes» відображає перевіряльник, який здебільшого перестав слухати, а не чистого суб'єкта.

Спробуй (2026). Для перевірки членства у витоках зайти на Have I Been Pwned, введи адресу, якою ти володієш, і прочитай повернутий список витоків з датами й розкритими класами даних. Для рідкості пароля використай на тому ж сайті діапазонну перевірку Pwned Passwords, яка повертає, як часто рядок з'являвся, ніколи не

бачачи твого повного пароля чи хеша. Сервіси й інтерфейси змінюються, тож підтверди поточний інструмент, перш ніж на нього покладатися.

Метод: email як крос-платформний з'єднувач

Ось де один email заробляє собі на хліб. У тебе є dmitri.works@gmail.com. Перевірка витоків дала тобі нікнейм nightferry з ForumRunner. Тепер ти розгортаєшся віялом.

Ти береш nightferry і шукаєш його по платформах — інструментарій перебору нікнеймів, з яким ти познайомився в Томі 1. Ти знаходиш nightferry на ігровому сервісі та night.ferry на фотосайті. Це та сама людина? Ще ні. Спільний нікнейм — це *слабкий* доказ сам собою; нікнейми копіюють, займають і перевикористовують незнайомці. Тобі потрібне підкріплення.

Тож ти повертаєшся до шару витоків. Той night.ferry з фотосайту — чи прив'язаний цей акаунт до якогось email у наборі даних витоку? Якщо пошуковий індекс витоків показує, що night.ferry зареєстрований з dmitri.works@gmail.com, ти щойно замкнув цикл. Нікнейм і email співпояву в незалежному джерелі. Це вже не збіг імен; це два записи, дві платформи, один email. Твій щабель піднімається від слабкого до помірного.

Зверни увагу, чого ти *не* робив. Ти не заходив у фотоакаунт. Ти ніде не пробував пароль. Ти читав витоки і читав співпояву, і дав фактам скластися стосом.

Метод: пароль як відбиток (і лише як він)

Це техніка, яку люди найчастіше роблять неправильно, тож я буду обережним.

Деякі набори даних витоку розкривають паролі — у відкритому вигляді або як хеші. Припустімо, два акаунти на двох непов'язаних сервісах обидва використали пароль Tramline!7743xQ. Це не поширений пароль. Він довгий, дивний, не має словникової форми. Якщо той самий рідкісний рядок захищає два акаунти, найімовірніше пояснення — що *одна й та сама людина задала обидва*. Люди перевикористовують свої дивні паролі. Це перевикористання — відбиток.

Ти можеш це використати. Якщо dmitri.works@gmail.com використав Tramline!7743xQ в одному витоку, а акаунт під зовсім іншим email, zorin.market@proton.me, використав ідентичний рядок в іншому, ти тепер маєш помірний-до-сильного доказ, що обидва email належать одній людині. Пароль зробив зв'язування.

Він не відчинив нічого. І ось межа:

Ти можеш використати украдений пароль, щоб зв'язати дві особи. Ти ніколи не можеш використати його для входу. Ввести украдений пароль у форму входу — це несанкціонований доступ, злочин, не OSINT.

Тепер межі, бо у відбитка їх три гострих.

Перша: поширені паролі не знімають жодного відбитка.

Якщо два акаунти ділять Password123, чи liverpool, чи qwerty2020, це не зв'язок — ними користувалися мільйони.

Пароль знімає відбиток лише тоді, коли він *достатньо рідкісний, щоб збіг був неправдоподібним*. Ти можеш перевірити рідкісність за допомогою перевіряльника паролів на k-анонімність, який каже, скільки разів рядок пароля з'являвся у витоках, при цьому ти ніколи нікуди не надсилаєш сам пароль — чи навіть його повний хеш: ти надсилаєш лише короткий *префікс* його хеша як діапазонний запит і завершуєш зіставлення на власній машині. Пароль, побачений чотири мільйони разів, нічого не вартий як відбиток. Пароль, побачений двічі — сильний.

Друга: дані витоку старі й брудні. Пароль з дампу 2016 року каже тобі про 2016 рік. Люди міняють паролі.

Комболисти переробляють і переприписують записи, тож «той самий» обліковий запис може з'явитися в десятку дамтів з неправильним сервісом — а у 2026 році ринки логів

стилерів та комболистів більші й переприписані сильніше, ніж будь-коли.

Третя, і найтонша — ця обпекла обережних аналітиків, тож я називаю її прямо. Спільний рідкісний пароль не сам собою доводить спільного *власника*. Він так само може означати спільну *жертву*. Назви це пасткою спільної жертви.

Уяви це. Tramline!7743xQ виринає, захищаючи dmitri.works@gmail.com у дампі 2019 року, а потім знову на акаунті криптобіржі в дампі 2023 року. Спокуслива читка — «та сама людина, два акаунти». Але друга історія вкладається в ті самі факти рівно: зловмисник зібрав рідкісний пароль Дмитра з комболисту 2019 року і набив ним облікові дані — пробував цю украдену пару email-і-пароль проти сайтів, якими Дмитро ніколи не користувався, серед них біржа. Якщо спрацювало, акаунт біржі був *скомпрометований*. Він належить тому, проти кого набили обліковий запис Дмитра, або зловмиснику, який його відкрив — не Дмитру. У будь-якому разі другий акаунт — це *жертва витоку Дмитра*, а не друга особа *самого* Дмитра. Пароль зв'язує два записи; він не каже тобі, чи ділять вони власника, чи ділять зловмисника.

Тож ти розриваєш зв'язку, перш ніж робити висновок, ніколи не після. Перевір порядок подій: якщо другий акаунт створили або зламали *після* того, як пароль Дмитра вже циркулював у комболистах, набивання лежить живе на

столі, і єдиний власник не доведений. Тоді шукай сигнали власності, які украдений пароль не може підробити — чи несе другий акаунт власний email відновлення, власний послідовний нікнейм, власний IP, що перетинається з першим? Один пароль і нічого більше, на акаунті, що вирінув після того, як витік став публічним, — це не знахідка про єдиного власника. Це слід з двома живими поясненнями, і ти тримаєш обидва, поки щось незалежне не вб'є одне.

Один розібраний кейс: від email до другого нікнейму

Дай пройду кейс реальної форми, з тупиками включно.

Насіння. Клієнтське замовлення — санкціоноване, задокументоване — дає мені один email:

info@meridian-imports.co. Питання — хто керує певним анонімним акаунтом маркетплейсу, merid_trade, який клієнт вважає пов'язаним з цією маленькою імпортною фірмою.

Крок перший — перевірка насіння у витоках. Я пропускаю info@meridian-imports.co крізь перевіральник членства.

Account: info@meridian-imports.co

Breaches found: 2

- B2BLeadDump (2020-05)

Exposed: Emails, Company names

- ForumRunner (2016-08)

Exposed: Emails, Usernames, IP addresses

Що повертає перевірка членства у витоках

ForumRunner розкрив нікнейм. Перспективно. Я витягую пов'язаний запис, і він дає мені нікнейм merid_trade, прив'язаний до info@meridian-imports.co. На мить це виглядає завершеним — нікнейм маркетплейсу, отут поруч з email компанії.

Тупик. Це не завершено, і ось чому. info@ — це *рольова поштова скринька*. Це не людина; це спільна скринька, яку кілька співробітників Meridian Imports можуть читати й з якої слати. Будь-хто в тому офісі міг зареєструвати merid_trade, використавши спільну адресу. Зв'язування merid_trade з info@meridian-imports.co не приписує його *людині* — воно приписує його *скриньці компанії*. Це справжня знахідка, але вона відповідає не на те питання. Клієнт хоче людину. Рольова скринька не мається на жодну одну людину, і я позначаю цю гілку мертвою.

Крок другий — знайти особисту адресу. Мені потрібен людський email. Поле IP-адреси ForumRunner і часові мітки витоку дають мені побачити, що акаунт merid_trade був найактивнішим з одного IP, і той самий IP з'являється у

витоку, прив'язаний до *другого*, схожого на особистий email: dana.rurik88@gmail.com. Тепер у мене є кандидат-людина.

Крок третій — підкріпити другим джерелом. Я перевіряю dana.rurik88@gmail.com у витоках. Вона з'являється в пасті й в одному іншому витоку, що розкрив *хеш* пароля. Окремо я знаходжу dana.rurik на фотоплатформі. Слабко поки що — збіг імені та IP. Мені потрібне щось твердіше.

Крок четвертий — відбиток і відкинутий збіг. Витік, прив'язаний до dana.rurik88@gmail.com, розкрив пароль. Так само і старий акаунт, який я знайшов під email відновлення нікнейму маркетплейсу. Обидва паролі: summer2019. Мій пульс підскакує — потім я зупиняюся. Я пропускаю summer2019 крізь перевіральник k-анонімності. Він з'являвся у витоках понад шістдесят тисяч разів. Він не знімає *жодного* відбитка. Пів інтернету використали summer2019. Я відкидаю збіг цілковито. Це збіг обставин, не зв'язок, і якби я подав його як доказ, я був би неправий і безрозсудний.

Назад до повільнішого, кращого доказу. Я читаю далі. Інший витік розкриває для dana.rurik88@gmail.com пароль Rurik_kite#4402. І email, пов'язаний з нікнеймом маркетплейсу, в ще одному дампі використав ідентичний рядок. *Цей* пароль, перевірений на рідкісність, з'являється рівно один раз, окрім цих двох акаунтів. Це справжній відбиток — і перш ніж на нього спертися, я усуваю пастку

спільної жертви: обидва акаунти передують дампам, що злили рядок, обидва несуть власний IP, що перетинається, і жоден не виринув *після* пароля іншого, коли той став публічним. Це перевикористання однією рукою, не набивання зловмисником.

Крок п'ятий — твердий ідентифікатор. Сильний — це не там, де цей кейс закінчується, бо нитка поза шаром витоків його завершує. Акаунт фотоплатформи, [dana.rurik](#), — самоавторський і публічний. Його біо веде на маленький особистий блог, і на тому блозі — словами самого автора, під повним іменем Dana Rurik — лежить пост, що оголошує запуск магазину маркетплейсу [merid_trade](#), з прямим посиланням на нього. Але блог — це *самовстановлена* поверхня: будь-хто може підняти сторінку під будь-яким іменем, тож перш ніж йому вірити, я перевіряю, що походження блогу незалежно її. Так і є: блог має посилання з фотоакаунта [dana.rurik](#), який я вже прив'язав до неї за IP та відбитком рідкісного пароля, а реєстрація його домену й вхідні посилання ведуть назад до того самого акаунта — тож це справжнє самопосилання, а не сторінка тезки чи підсаджена, щоб мене ввести в оману. Лише тепер воно рахується. Це не співпоява у витоках. Це суб'єкт, публічно, прив'язує власне ім'я до того самого акаунта, про який мене запитали. Самоавторська публічна заява, щойно її походження підтверджено як власне цілі, — це твердий ідентифікатор.

Приземлення. То де я, чесно? Шар витоків проніс мене довгий шлях: IP, що зв'язує нікнейм маркетплейсу з особистим email; рідкісний спільний пароль, очищений від пастки спільної жертви, що зв'язує той email з адресою відновлення нікнейму; збіг імені на фотоплатформі. Незалежні, складені стосом, жоден з них — не вхід — і на самих *лише* даних витoku я зупинився б на **сильному**, бо застарілі записи кримінального походження ніколи не заробляють *підтверджено* самі собою. Що піднімає це до підтверджено — самопосилання, що лежить цілком поза витоками: Dana Rurik, публічно, під власним іменем, заявляє про акаунт. Я пишу звіт на «підтверджено», називаю твердий ідентифікатор, що заробив щабель, перелічую кожен дамп і дату, що привели мене до сильного, і позначаю тупик info@, щоб наступний аналітик не повторив мого півдня.

Вправа: перевір власні витоки, безпечно

Цю ти запускаєш цілком на собі. Жодних цілей, жодних третіх осіб.

- Візьми одну зі *своїх власних* email-адрес. Пропусти її крізь перевіряльник членства у витоках (НІВР чи еквівалент). Запиши кожен витік, його дату й розкриті класи даних. Зауваж, скільки незнайомиць міг би виснувати лише зі *списку* — якими сервісами ти користувався, приблизно коли.

- Тепер запусти другу адресу, якою ти рідко користуєшся. Якщо вона повертається порожньою, напиши «неіндексовано», не «безпечно». Посидь з цією різницею. Ця порожнеча — рівно та пастка, у яку ти ніколи не маєш впасти, коли це адреса цілі, а не твоя.
- Візьми пароль, який ти вивів з ужитку (ніколи не поточний), і пропусти його крізь перевіральник паролів на к-анонімність. Подивися, скільки разів він з'являвся. Якщо лічба висока, цей пароль ніколи не міг би зняти нічийого відбитка — зрозумій *чому* власними словами.
- Насамкінець напиши одне речення: різницю між перевіркою того, що пароль було злито, і використанням його для входу. Якщо ти можеш сказати це прямо, розділ у тебе є.

Не роби нічого з цього, у жодну мить, проти акаунта іншої людини, і ніколи не вводь жоден украдений пароль у жодну форму входу — навіть свій власний старий на живому сайті, щоб «побачити, чи він ще працює». Перевіряй витоки. Ніколи не тестуй доступ.

Підсумок

- Витоки — це мости, не ключі. Вони з'єднують особи; вони ніколи не відчиняють акаунти. Яскрава межа — дивитися проти торкатися, і вона не зсувається.
- Перевіральник витоків каже тобі членство, дати й класи даних — ніколи значення паролів. Він читає

витоки. Саме це тримає його в межах закону.

- Порожній результат — це дані, не вердикт. Нуль збігів означає *неіндексовано*, *не безпечно*, *не чисто*.

- Email — це крос-платформний з'єднувач. Співпоява у витоках перетворює одну адресу на нікнейми, IP та альтернативні email, які ти можеш розгорнути віялом і підкріпити.

- Рідкісний спільний пароль знімає відбиток людини. Поширений не знімає нічийого. Перевір рідкісність, перш ніж йому довіряти, і відкидай збіги без жалю.

- Спільний пароль може означати спільну жертву, не спільного власника. Набивання облікових даних може посадити украдений пароль однієї людини на акаунт іншої. Усунь пастку спільної жертви — порядок подій, незалежні сигнали власності — перш ніж робити висновок про єдиного власника.

- Рольові скриньки називають організації, не людей. info@ та її родичі не мапляться на жодну одну людину — ніколи не давай одній маскуватися під атрибуцію.

- Дані витоку застарілі й брудні, і ніколи не заробляють підтверджено самі собою. Підкріплюй через джерела, називай кожен дамп і дату. Витоки можуть перекинути тебе мостом до *сильного*; лише твердий ідентифікатор поза шаром витоків — публічне самопосилання, документ — заробляє *підтверджено*.



РОЗДІЛ ШОСТИЙ

Граф особи

Як знайти того, хто себе сховав

Ось проблема, з якою ти зустрічатимешся знов і знов.

У тебе є ціль. Ім'я, можливо, фото, можливо, посада. Ти йдеш шукати — і не знаходиш нічого. Її Instagram закритий. Її Facebook — сірий силует і стіна. Її LinkedIn — три рядки. Кожні двері зачинені.

Більшість людей зупиняється тут. Вони пишуть «немає присутності онлайн» і йдуть далі.

Це помилка. Бо людина не зникла. Вона лише замкнула власні вхідні двері.

Один розділ тому ти використовував коло зв'язків, щоб *підтвердити* особу, яку вже підозрював — ти мав ім'я на думці, і мережа сказала тобі, чи воно пасує. Цей розділ біжить у протилежний бік. Тут ти починаєш з людини, яка навмисно себе сховала, і ти *відкриваєш* особу, про існування якої не знав. Той самий граф людей; протилежна робота.

Хід, до якого я тягнуся, коли прямий пошук вмирає, — це той, який я називаю Сімейним ланцюгом. Ідея проста, і щойно ти її побачиш, ти не зможеш її розбачити. Ти не штурмуєш стіну. Ти обходиш її, крізь людей, що стоять поряд з нею.

Ніколи не запускай Сімейний ланцюг, щоб знайти того, хто пішов у тінь заради власної безпеки.

Пережила домашнього насильства чи будь-хто, хто ховається від тієї самої людини, яка хоче його знайти, — це не бриф для виконання: такий «клієнт» — червоний прапорець, щоб відмовитися ще до того, як ти намалюєш перший вузол. Повна версія цієї межі — наприкінці розділу; вона йде першою тут, бо знак «стоп» ні до чого, якщо ти зустрічаєш його лише після методу.

Єдине, що вони забувають сховати

Обережна людина може замкнути все, чим володіє. Кожен профіль, кожен пост, кожне налаштування. Це вимагає зусиль, але це можливо.

Чого вона не може зробити — це замкнути всіх, хто з нею пов'язаний.

Подумай, хто оточує людину. Дружина. Чоловік. Сестра. Мати. Брат. Старі шкільні друзі. У цих людей власні акаунти, власні звички, власне уявлення про приватність — яке зазвичай *геть відсутнє*. Вони постять сімейну відпустку. Вони тетають усіх повними іменами. Вони заливають святкову вечерю. Вони лишають старий номер телефону в оголошенні про продаж дивана.

Твоя замкнена ціль з'являється в усьому цьому. Позначена тегом, сфотографована, згадана, названа. Вона на це не погоджувалася і може навіть не знати, що це існує.

Будь чесним про те, як це змінилося. До 2026 року платформи за замовчуванням тримають приватність тугішою, ніж раніше: тегування часто потребує схвалення, списки друзів ховаються, «тільки я» — поширене налаштування, а молодше, обережніше покоління замикає все за звичкою. Сімейний ланцюг — уже не та вольниця, якою був десять років тому. Але він досі працює, бо йому не потрібно, щоб *усі* були недбалими — потрібно, щоб *один*

родич таким був. Тітка, яка не змінювала налаштувань з 2013 року. Двоюрідний брат, який лишає тегування відкритим, бо схвалювати теги — морока. Ти не ставиш на те, що ціла сім'я неохайна. Ти ставиш на одні відчинені двері в будинку, повному замкнених, і ця ставка досі окупається.

Я колись працював над кейсом, де клієнту завинив велику суму чоловік, що заявляв, ніби його бізнес згорнувся і в нього нічого не лишилося. Онлайн він був фахівцем серед фахівців. Приватний усюди. Бездоганний, запечатаний профіль. Прямий пошук не дав мені нічого. Нормальний аналітик підшив би «немає присутності онлайн» і закрив би тікет.

Я не пішов на нього. Я пішов на людей навколо нього. Стара сторінка його дружини, напівзабута й досі відкрита. Звідти — її публічний Instagram. У її Instagram — згадки про її сестру. Профіль сестри був широко відкритий — і в сімейному відпустковому фото вона позначила його тегом. Не під його справжнім, замкненим іменем. Під *другим* нікнеймом, про який, як він гадав, ніхто не знав. Той другий акаунт був там, де його справжнє життя — і його нібито мертвий бізнес — тихо тривали.

Метод, а не історія

Я щойно розповів тобі історію, тож не довіряй їй трохи. Історія вручає тобі одну щасливу кінцівку й ховає десять кроків, що могли піти не так. Тож дай я обдери цю історію до повторюваного методу під нею: п'ять кроків, які ти можеш запустити на будь-кому, без потреби в моєму везінні.

Крок 1 — Намалюй найближче коло. Перш ніж кудись півотити, намалюй людей. Ціль — центральний вузол. Навколо неї йдуть вузли, які ти можеш назвати чи вгадати: партнер, батьки, брати й сестри, діти, близькі друзі, ділові партнери. Тобі ще не потрібен доказ. Тобі потрібні кандидати. Ім'я з весільного оголошення, «брат» у старому теговому коментарі, спільне прізвище — усе це йде на карту як вузол.

Крок 2 — Знайди, які вузли відкриті. Тепер перевір кожен вузол на пульс. У кого з цих людей публічний профіль? У родичів зазвичай є. Особливо у старших родичів — Facebook матері з 2013 року, широко відкритий, — золота жила. Ти їх ще не читаєш. Ти лише позначаєш кожен вузол відкритий або закритий.

Крок 3 — Півотни в ціль крізь відкритий вузол. Це той хід. Ти заходиш в акаунт відкритого родича і шукаєш *ціль усередині нього* — її теги, її фото, її згадки, коментарі, які вона лишила. Ти тут не для того, щоб вивчати родича. Ти тут, щоб

знайти, де він указує назад на твою замкнену людину.

Крок 4 — Підтверди перехресними зв'язками. Одна згадка — це слід, не факт. Складай стосом незалежні зв'язки: те саме обличчя на двох фото, та сама подія тієї самої дати, той самий нікнейм, що з'являється у двох непов'язаних місцях. Кожен збіг піднімає тебе на щабель.

Крок 5 — Зупинися, коли робоче питання отримало відповідь. Тієї миті, коли ти маєш те, що робота насправді потребувала, ти зупиняєшся. Ти не продовжуєш розбирати родичів на шматки заради спорту. Про це докладніше нижче, бо це важить більше за техніку.

Спробуй (2026). Обери публічну постать із замкненою особистою присутністю — або, краще, згідного друга, який погодився бути твоєю тренувальною ціллю. Випиши трьох-чотирьох названих родичів, яких ти можеш ідентифікувати з публічних джерел: чоловіка/дружину, брата чи сестру, батька чи матір, свояка, двоюрідного. Перевір акаунт кожного на пульс — познач їх відкритий або закритий — і обери найвідкритішого родича. Тепер зайти *всередину* акаунта того родича й шукай лише *ціль усередині нього*: теги, сімейні фото, згадки, коментарі, які лишила ціль. Тієї миті, коли ти маєш відповідь на своє одне робоче питання, зупинися — не записуй нічого про родича, що не є відповіддю, і не читай далі «просто щоб побачити».

Застереження: уся ця вправа живе всередині безпекової межі

в кінці розділу — ніколи не запускай її проти того, хто ховається заради власного захисту, хоч би яким охайним виглядав тренувальний кейс.

Малювання графа

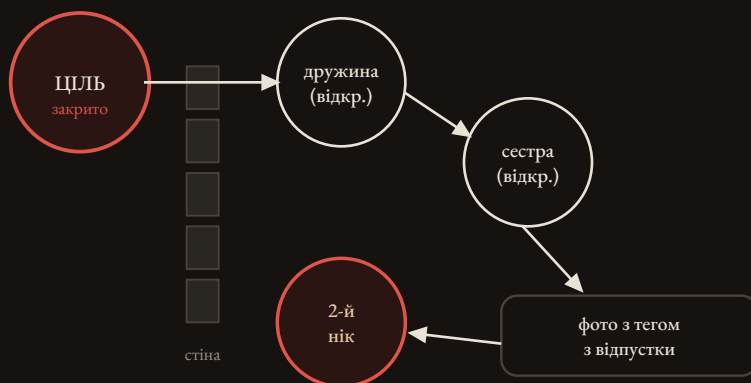
Нанеси його на папір. Груба схема б'є розумну пам'ять.

```
identity-graph.txt
```

```
TARGET  (locked)
|
[ WALL ]  <- direct search dies here
|
+--> WIFE ..... OPEN
      |
      +--> SISTER ..... OPEN
            |
            +--> family photo
                  tags TARGET as
                  a 2nd handle -> EVERYTHING
```

Читай його згори вниз. Ціль запечатана. Стіна зупиняє фронтальний пошук. Тож ти крокуєш убік до дружини, яка відкрита, і знову вбік до сестри, яка відкрита — і сестра там, де ціль протікає. Стрілки ніколи не йдуть *крізь* стіну. Вони йдуть навколо неї.

СІМЕЙНИЙ ЛАНЦЮГ



ти не лізеш через стіну — ти йдеш в обхід

Замкнена ціль сидить за стіною, яку фронтальний пошук не може перетнути. Родичі стоять на видноті навколо неї. Шлях не йде крізь стіну — він біжить убік, від відкритої дружини до відкритої сестри до тегованого фото, і дістає ціль зі спини.

Розібраний кейс, зі збереженими хибними поворотами

Дай я проведу його як слід. Усе тут вигадане, але тертя справжнє — тупики, схожі люди, хибний зв'язок, який довелося викинути. Це частини, які більшість описів видаляє. Це частини, які навчають.

Бриф. Клієнту завинив великий, визнаний судом борг чоловік на ім'я Marat Devlin. Marat присягається, що його маленька логістична фірма розвалилася, що він банкрут, і що

повертати нічого. Юрист клієнта підозрює інше — що Marat тихо продовжив торгувати під іншим іменем, щоб винести бізнес поза досяжність. Моє питання — *єдине* питання, за яке мені платять, — таке: чи Marat досі керує прихованою бізнес-особою? Є активна, законна суперечка, справжній борг і справжній законний інтерес до з'ясування, чи Marat приховує активи. Тримайся за це, бо ми повертаємося до нього жорстко, коли ланцюг проходить крізь його сім'ю.

Прямий пошук. Мертвий по прибутті. Один LinkedIn, три рядки, без фото. Facebook із сірою головою і нічим публічним. Instagram, виставлений приватним, 0 видимих постів, 411 підписників. Він зробив роботу. Вхідні двері на засуві.

Тож я перестаю тиснути на двері.

Крок 1 — Намалюй коло. Я зшкрябую те мале, що публічне. Його LinkedIn перелічує фірму; дрімлива сторінка «Про нас» фірми називає співзасновника, Devlin, те саме прізвище — імовірно, брат або підпис дружини. Його замкнений Facebook, до того як його замкнули, одного разу кешувався пошуковиком з єдиним видимим рядком: «одружений з Lena». Тож моя карта:

circle-map.txt

```
TARGET: Marat Devlin (locked)
- Lena Devlin ..... wife? node
- "Devlin" co-fndr .. sibling? node
- unknown parents ... node
- unknown siblings .. node
```

Чотири вузли. Два названі, два порожні. Достатньо, щоб почати.

Крок 2 — Хто відкритий. Я шукаю кожного. «Lena Devlin» повертає публічний Instagram — фото з подорожей, собака, жодної приватності. Співзасновник «Devlin» виявляється Sam Devlin, і ось мій перший тупик: я припустив, що Sam — брат Marat. Неправильно. Власні пости Sam роблять ясным, що він діловий партнер, без кровної спорідненості, і живе на іншому континенті. Він вузол, але не *сімейний* вузол, а сім'я — там, де протікання. Я позначаю Sam як низький пріоритет і рухаюся далі. Вгаданий зв'язок, що не спрацював, — це не змарнований час, це на одну хибну дорогу менше пізніше.

Крок 3 — Півот крізь відкритий вузол. Instagram Lena — це вхід. Я не сиджу й не читаю її життя. Я шукаю Marat. І в її стрічці, за два роки, вона тричі згадує «мою сестру Kira». Kira — новий вузол — родичка, якої я не мав на кроці один, вручена мені відкритим акаунтом. Це ланцюг, що продовжує сам себе.

Тепер другий тупик і хибний зв'язок, який я мало не купив. Я шукаю «Kira Devlin» і знаходжу цілком відкритий

профіль — публічний, балакучий, багато сімейних фото. Джекпот, думаю я. Потім я пригальмовую й роблю арифметику замість того, щоб довіряти трепету.

По-перше, базова ставка. Наскільки дивовижна збіжна «Kira Devlin»? Не дуже. Прогони ім'я крізь публічний довідник для країни — і знайдеш їх десятки; це нечасте-але-не-рідкісне ім'я, і «Kira Devlin існує в Instagram» близьке до гарантованого. Такий дешевий збіг — це не доказ; це те, чого ти й очікуєш за випадковістю. Щоб чогось вартувати, кандидат мусить побити базову ставку — вона мусить нести факти, яких *випадкова* Kira Devlin майже ніколи не мала б.

Тож я перевіряю незалежні факти, і два з них ламають збіг цілковито. Один: сестра ділить *дівоче* прізвище, а дівоче прізвище Lena — зовсім не Devlin — тож справжня сестра взагалі не була б «Devlin». Прізвище, що затягнуло мене, — не те прізвище, якого слід чекати. Два: тегована сім'я цього профілю, рідне місто і школа всі належать зовсім іншому кластеру людей, жоден з яких не перетинається з Lena. Вона тезка — поширене ім'я, що зіткнулося за випадковістю, не більше. Спільне ім'я сильне рівно настільки, наскільки рідкісне саме ім'я, а це геть не рідкісне.

Я відкидаю її. Дешевий збіг, спростований деталями, що мають значення, з драбини цілком. Якби я побіг з нею, я б збудував цілу хибну особу для Marat з родичів незнайомки.

Назад до Lena. Її підписи зрештою видають справжній нікнейм сестри — @kira.m.travels — жодного прізвища Devlin. Той профіль теж відкритий. І в пляжному фото з сімейної відпустки троє дорослих позначені тегами. Один тег читається @md_offgrid — нікнейм, який я ніколи не бачив на чомусь, пов'язаному з «Marat Devlin».

Крок 4 — Підтверди перехресними зв'язками. Один тег — це *слабкий* слід. Я не святкую. Я складаю стосом — і я суворий щодо того, чого кожен шматок насправді вартий:

- Обличчя на пляжному фото (@md_offgrid) *схоже* на єдину розмиту, низькороздільну мініатюру, кешовану зі старого Facebook Marat. Я хочу, щоб це був він. Але розмите обличчя — це слід, не факт — правило Розділу чотири тримається і тут, і я відмовляюся дати нутру виміняти нечітку мініатюру за доказ. Я записую це як слабкий сигнал, привід шукати далі, і не більше. Само собою воно не зрушує мене зі слабого.
- Кілька публічних постів @md_offgrid показують фургон з логотипом компанії. Логотип — той самий знак — той самий словесний знак, ті самі кольори — що й логістична фірма зі старого LinkedIn Marat. Цього я не задавав, і він не задавав; це специфічний, перевірюваний артефакт з іншого джерела, ніж обличчя. Це піднімає мене до помірного.

- Локація й дата відпустки збігаються із запискою «фургон на заході, назад наступного тижня», опублікованою на публічній сторінці фірми того ж тижня. Третя незалежна нитка — час, з ще одного джерела — приземлюється на ту саму людину. Це веде мене до сильного: @md_offgrid дуже ймовірно — прихований, досі активний акаунт Marat Devlin.

Зверни увагу, звідки прийшла вага. Не обличчя — обличчя ніколи не піднялося вище слабкого, і я ніколи не дав. Підйом від слабкого до сильного несуть цілком два сигнали, у які я *не* міг себе умовити: незалежний логотип і незалежна дата. Розмита мініатюра відчувається як драматична зачіпка. Це найслабша річ у списку. Нудні, перевірювані узгодження — ось що насправді збудувало щабель.

Що відповів другий акаунт. @md_offgrid зовсім не поза мережею. Фургон працює — він постить замовлення, забори й контакт для бронювання, усе під новим брендом, усе в ті тижні, коли Marat присягався, що бізнес мертвий. Це прямо суперечить «фірма розвалилася, повертати нічого». І *це відповідь на бриф*. Юрист питав, чи Marat досі торгує під прихованою особою. За відкритими доказами — так.

Тепер чесна частина про щабель. Я досяг сильного — три незалежні нитки, що узгоджуються — але я *не* досяг підтверджено, і я кажу це прямими словами. Підтверджено означало б шматок доказу, що прив'язує людину Marat

Devlin до того акаунта поза межами конкурентного пояснення: витребуваний судом запис платформи, платіжний слід, зізнання. Я не можу дістати цього з відкритої мережі, і я не роздму сильний у підтверджено, щоб догодити клієнту. Тож мій звіт каже саме це: *сильний доказ, що @md_offgrid — активний акаунт Marat; рекомендую юристу витребувати записи платформи й платежів, щоб закрити останню прогалину*. Робота з відкритих джерел веде це так далеко, як чесно веде робота з відкритих джерел, а потім передає естафету людям, які можуть примусити решту.

Ця стриманість — подавати сильний як сильний, не наряджати його підтвердженням — сама по собі є достовірністю знахідки. Щабель, який ти можеш захистити, вартий більше за щабель, який тобі доведеться відкликати.

Я пишу знахідку. Потім я зупиняюся.

Де ти зупиняєшся, і чому це справжнє вміння

Техніка працює на недбалості невинних людей — дружини, сестри, які нічого поганого не зробили і ніколи не погоджувалися бути частиною чийогось розслідування. Саме тому їй потрібна жорстка межа, і одна межа передує всім іншим:

Ніколи не запускай Сімейний ланцюг, щоб знайти того, хто пішов у тінь заради власної безпеки.

Пережила домашнього насильства, колишня партнерка, з якою розірвано стосунки, людина, що обірвала контакт і не хоче, щоб її знайшли — знаходження її може поставити її в реальну, фізичну небезпеку, іноді від тієї самої людини, що тобі платить. «Клієнт», який хоче, щоб ти знайшов того, хто навмисно сховався *від нього*, — це червоний прапорець, щоб відмовитися, а не бриф для виконання. Це та єдина робота, якій ти кажеш ні, попри будь-який гонорар.

Ось межа. Ти береш лише те, що відповідає на робоче питання, і решту лишаєш. Мені треба було встановити, чи Marat досі торгує під прихованою особою. Історія подорожей Lena, стосунки Kira, кличка собаки, домашня адреса сім'ї — ніщо з цього не відповідає на бриф, тож ніщо з цього не йде у звіт. Я побачив решту. Я її не використовую. Я її не зберігаю. І тримайся лише відкритих джерел: весь метод спирається на те, що люди лишили публічним, тож ти ніколи не додаєшся в друзі, не обманюєш і не втираєшся в закритий профіль.

Одна юридична межа, за яку варто триматися: дозвіл твого клієнта покриває розгляд його цілі, а не каталогізацію приватних життів родичів, крізь яких ти проходиш. Коли ставки регульовані — працевлаштування, кредит, страхування, будь-що транскордонне — це перестає бути тим, що ти оцінюєш на око, і стає тим, що ти отримуєш письмово, з юрисконсультом. Повний посібник живе в Томі

4.

Аналітик, який не може зупинитися, не ретельніший. Він просто цікавіший до чужого, і зрештою переступає межу, через яку весь його звіт викидають — а з ним і його репутацію.

Вправа

Візьми публічну постать із замкненою особистою присутністю — засновника, політика середньої ланки, будь-кого, хто явно добре керує власною приватністю. Постав собі одне вузьке робоче питання, як-от: *у якому місті вона насправді живе?* Не її адресу. Її місто.

Тоді запусти п'ять кроків.

1. Намалюй її коло з публічних джерел — чоловік/дружина, брати й сестри, батьки. Намалюй граф. 2. Познач кожен вузол відкритим або закритим. 3. Півотни крізь одного відкритого родича і шукай усередині лише ціль. 4. Спробуй відповісти на своє одне питання, і запиши, якого щабля ти досягаєш — слабкий, помірний, сильний, підтверджено — і *чому*. 5. Свідомо потренуй зупинку: перелічи три речі, які ти побачив про родичів і які ти обираєш не записувати.

Бонус, і це важлива половина: змусь себе знайти один хибний зв'язок і відкинути його письмово. Тезку, неправильно вгаданий зв'язок, обличчя, яке виявляється

кимось іншим. Якщо ти не наштовхнувся на жоден тупик, ти не був чесним із доказами.

Підсумок

- Людина може замкнути власні профілі. Вона не може замкнути людей навколо себе.
- Сімейний ланцюг: не штурмуй стіну — обійди її, крізь теги, фото й згадки відкритих родичів.
- П'ять кроків: намалюй коло, познач відкриті вузли, півотни всередину крізь відкритого родича, підтверди складеними перехресними зв'язками, зупинися на робочому питанні.
- Родичі досі відчинені двері, навіть під тугішими захистами 2026 року — тобі потрібен один недбалий родич, не недбала сім'я.
- Впевненість будується з *незалежних* зв'язків, які ти не міг влаштувати — незалежний логотип і дата провели цей кейс. Розмите обличчя лишається слабким; нутро не має права його підвищувати.
- Спільне ім'я вартує рівно стільки, наскільки ім'я рідкісне. Побий базову ставку незалежними фактами або відкинь збіг.
- Чекай на тупики: тезки, неправильно вгадані зв'язки, хибні обличчя. Відкидати їх — це робота, а не її провал.

- Дозвіл клієнта покриває розгляд цілі, а не каталогізацію родичів, крізь яких ти проходиш. Бери лише те, що відповідає на питання, потім зупинися. Корпоративні й транскордонні деталі: Том 4.
- Ніколи не запускай ланцюг, щоб знайти того, хто ховається заради власної безпеки — цей «клієнт» — червоний прапорець, щоб відмовитися.



РОЗДІЛ СЬОМИЙ

Як змусити сигнали погодитися

Одна зачіпка — це здогад. Багато незалежних зачіпок, що узгоджуються, — це відповідь.

Новачки полюють на вбивчу зачіпку. Той один скріншот, той один злитий email, ту одну деталь, що завершує суперечку. Вони думають, що атрибуція — це замок, і десь є єдиний ключ.

Так майже ніколи не буває.

Справжня атрибуція тихіша. Це купа малих, непримітних спостережень — коли хтось постить, як пише, який емодзі

перевикористовує, хто раз у раз виринає в його відповідях — які самі собою не доводять нічого, але *разом* указують в один бік і відмовляються вказувати в будь-який інший. Жоден окремий сигнал не несе кейсу. Узгодження між ними — несе.

Висновок, збудований на одній зачіпці, падає, коли падає та зачіпка. Висновок, збудований на п'яти незалежних зачіпках, треба збивати п'ять разів.

Том 1 дав тобі драбину: слабкий, помірний, сильний, підтверджено. Цей розділ про те, як ти насправді *дереш* її — не знаходячи сильніших зачіпок, а складаючи стосом чесні й спостерігаючи, як вони узгоджуються. І він про ту одну помилку, що тихо руйнує більше атрибуцій, ніж будь-яка інша: рахувати той самий сигнал двічі.

Одну річ треба залагодити перед початком, бо вона збиває людей з пантелику. Ти побачиш ті самі чотири слова — слабкий, помірний, сильний, підтверджено — вжитими у *двох* місцях, і вони означають дві споріднені речі. Вони оцінюють окремий сигнал: скільки ваги ця одна зачіпка несе сама собою. І вони оцінюють твій загальний висновок: наскільки ти впевнений після складання всього стосом. Двоє пов'язані рахуванням — але рахунок це орієнтир, не тест. Розділ про Міст задав правило для висновку. *Сильний* заробляється тим, що незалежні узгодження, разом, важко

пояснити будь-якою суперницькою гіпотезою. Зазвичай це потребує трьох чи більше — але два важкі, діагностичні сигнали (побайтово ідентичний аватар плюс перевірене самопосилання) можуть його досягти, а три слабкі, поширені можуть і ні. Два узгоджені незалежні сигнали — звичайна підлога для *помірного*. Тож один «сильний, незалежний» сигнал — це не те саме, що сильний *висновок* — це одна важка зачіпка, яка, з ще однією-двома, доводить тебе до сильної знахідки. Коли я маркую сигнал нижче, я оцінюю ту зачіпку; коли я називаю щабель наприкінці кейсу, я оцінюю купу. Тримай ці два значення нарізно — і розділ лишається ясним.

Ідея: незалежне узгодження — ось що зрушує стрілку

Два акаунти. Ти хочеш знати, чи одна людина керує обома. Ти ніколи не отримаєш сертифіката. Замість цього ти отримуєш набір сигналів, кожен з яких трохи узгоджений — або трохи неузгоджений — з «та сама людина».

Чарівне слово — незалежний.

Два сигнали незалежні, коли вони походять з *різних джерел*, і один міг би бути правдою, поки інший хибний. Коли вони все одно узгоджуються, це узгодження важко пояснити випадковістю, і твоя впевненість швидко дереться вгору. Коли вони *не* незалежні — коли вони таємно походять з

того самого джерела — вони відчуються як двоє свідків, але це один свідок, що говорить двічі. Складання їх стосом дурить тебе хибною впевненістю.

Ось найчистіший спосіб відчуті різницю.

Скажімо, два акаунти обидва показують ім'я «Andrii Melnyk». Вражає? Ні. Показуване ім'я — *самозадане*. Людина набрала його в обидва поля. Якщо це та сама людина, то воно, звісно, збігається — але якщо це самозванець, воно теж збігається, навмисно. Узгодження показуваного імені каже тобі майже нічого, бо імена обох акаунтів походять з *того самого одного акту набирання тим, хто ними керує*. Одне джерело. Один сигнал.

Тепер скажімо, акаунт А постить майже лише між 22:00 і 02:00 за київським часом, а акаунт В — на іншій платформі, яку ти перевіряв окремо — *теж* мовчить цілий день і оживає після 22:00. Жоден акаунт не оголошував своїх годин. Ти виміряв їх, незалежно, з двох різних стрічок часу. Їхнє узгодження — не те, що людина задала навмисно. Це узгодження — справжній сигнал.

Однаково виглядають докази. Цілком різна вага. Питання ніколи не «чи вони збігаються?». Воно — «чи вони збігаються з *причин, які могли б розійтися, і не розійшлися?*».

Тепер частина, яку більшість пропускає, і це вся причина існування цього розділу. «Чи задала це ціль?» — лише

половина незалежності. Є другий, підступніший спосіб, яким сигнали перестають бути незалежними: коли дві зачіпки ділять приховану спільну причину, що змусила б їх узгодитися *навіть для двох різних людей*. Постав справжній тест уголос — чи узгодилися б ці два сигнали за випадковістю для двох різних людей, узятих з тієї самої популяції? Якщо відповідь так, це не два незалежні голоси. Це один голос у двох пальтах.

Ось пастка в одній картині. Припустімо, твоя справжня суперницька гіпотеза не «та сама людина проти випадкового незнайомця», а «та сама людина проти *іншої людини з того самого міста й тієї самої онлайн-сцени*». Тепер подумай, що двоє таких людей ділили б *за замовчуванням*: той самий часовий пояс, отже, ті самі години постингу. Той самий місцевий сленг. Той самий емодзі своєї групи. Ті самі регіональні дивацтва написання. Ніщо з цього не тому, що вони та сама людина — це тому, що спільне місто й спільна субкультура — це спільна причина, що штовхає обидва акаунти до однакового вигляду. За цією гіпотезою час, сленг, емодзі й одруки — усе похідне від однієї речі. Рахувати їх як чотири незалежні влучення — це рахувати один збіг чотири рази.

П'ять робочих коней-сигналів

Це сигнали, до яких ти тягтимешся знов і знов. Жоден не вирішальний сам. Вивчи, чого кожен вартий і, що важливіше, чи він незалежний від інших, які ти вже маєш.

- **Час активності.** Коли хтось постить, за тижні, окреслює його часовий пояс і денний розпорядок — вікно нічної сови, обідній штиль, мертву зону, поки він спить. Це поведінкове й важко підробити, бо підробити означає ніколи не осковзнутися місяцями. Два акаунти з тим самим відбитком постингу за багато днів — це тихо сильно. *Незалежність: висока проти випадкового незнайомця — ти виміряв її, вони не задали. Але обережно: двоє різних людей у тому самому місті ділять часовий пояс, тож широке «постить уночі» слабше, ніж виглядає. Вагу заробляє специфічний, особистий підпис — ті самі дивні сплески о 03:40, ті самі мертві недільні ранки — а не просто «обидва нічні».*

- **Стиль письма (стилометрія-лайт).** Не хитре ПЗ — просто тики, яких людина не може перестати робити. Звичне «tbh», кома перед «but», британські написання, змішані з американськими, підписова одрука, початок речень із «So». Один тик — це збіг. П'ять специфічних, незвичних тиків, спільних для акаунтів, — це відбиток. *Незалежність: помірна до високої, якщо тики справді відмітні — але стережися, люди в тій самій субкультурі ділять сленг.*

- Звички щодо емодзі та пунктуації. Підвид стилю, вартий власного рядка, бо він такий липкий. Точний емодзі, до якого хтось тягнеться (проти), подвійні пробіли після крапок, «!!!» проти самотнього «!», усе-малими-літерами. М'язова пам'ять. Люди міняють своє ім'я раніше, ніж міняють свій емодзі. *Незалежність: помірна — те саме застереження, що й для стилю.*

- Перевикористані активи — біо, посилання, аватари. Те саме фото профілю, те саме речення біо, той самий прив'язаний вебсайт чи Telegram-нікнейм на різних акаунтах. Це високоцінне, *але читай незалежність уважно*. Перевикористаний файл аватара (побайтово ідентичний, не просто схожий) — сильний.

Перевикористаний *самонаписаний рядок біо* слабший, ніж виглядає — він самозаданий, як показуване ім'я, тож самозванець може скопіювати його навмисно.

- Спільні зв'язки. Ті самі друзі, ті, хто відповідає, співучасники груп, що обертаються навколо обох акаунтів. Соціальний граф людини дорого підробити й повільно рухати. Коли два акаунти ділять не одного, а *кластер* тих самих справжніх приятелів, це один із найсильніших сигналів, що існують — бо він живе на *чужих* сторінках, поза контролем цілі. *Незалежність: висока.*

Зверни увагу на візерунок. Сигнали, які ти *спостерігаєш ззовні* — час, граф — схильні бути незалежними й сильними. Сигнали, які акаунт *задає про себе* — показуване ім'я, текст

біо — схильні бути залежними й слабкими, бо той, хто керує акаунтом, керує ними напряму, чесно чи ні.

Тож ось правило, що перетворює це з розпливчастого хвилювання на арифметику — і це єдине найважливіше правило в розділі для рахування, що надходить:

****Час, сленг, емодзі й одруки — це одна сім'я сигналів, не чотири. Оцінюй усю сім'ю як єдиний фактор, і задавай вагу того фактора тим, наскільки *рідкісна* спільна риса — а не тим, скільки рис ти можеш перелічити.****

Тож чотири узгоджені тики з однієї субкультури — це не чотири шаблі доказу, це одне спостереження, «ці двоє виглядають так, ніби походять з того самого середовища», пораховане один раз. Порятунком — *специфічність*. Поширений тик («постить уночі», «каже based») доводить мало й не може бути відмитий у силу нагромадженням більшої кількості поширених тиків поряд. Але дивний, особистий — послідовна унікальна одрука, саморобне скорочення, яким ніхто більше не користується, емодзі, до якого ніхто в тій сцені не тягнеться — рідкісний достатньо, щоб випадковий збіг між двома незнайомцями був справді малоюмовірним. *Це* те, що несе вагу, і один рідкісний тик може вартувати більше за десять поширених.

Тож незалежність має тепер два питання, і ти ставиш обидва до кожного сигналу:

1. Чи задав це власник акаунта? Якщо так (показуване ім'я, текст біо), воно самозадане й слабке — самозванець копіює його навмисно. 2. Чи узгодилося б воно за випадковістю для двох різних людей з тієї самої популяції? Якщо так (спільний часовий пояс, внутрішньогруповий сленг), воно корельоване, і воно згортається в один фактор зі своїми родичами.

Сигнал зараховується як повний, незалежний голос лише тоді, коли відповідь на обидва — ні.

Метод: збудуй таблицю сигналів, потім перевір незалежність

Не тримай це в голові. Упередження живе в голові. Постав це в таблицю.

Для кожного сигналу пиши чотири речі, і тримай останні дві в *окремих* стовпцях, бо це окремі питання. Одне: що це. Два: значення, яке ти спостеріг на кожному акаунті. Три: сила — скільки ця одна зачіпка вартує сама собою (слабкий, помірний, сильний). Чотири — стовпець, який усі забувають — незалежний?, що означає обидва наші тести: не самозаданий і не збіг, який ділили б двоє незнайомців з тієї самої популяції. Сила й незалежність — не та сама вісь. Сигнал може виглядати сильним, але бути незалежним (скопійоване біо), або скромним, але ідеально незалежним (одна дивна одрука). Ніколи не згортай їх в один стовпець.

НЕЗАЛЕЖНІ СИГНАЛИ

сигнал	тип	незалежний?
ім'я профілю	сам задав	НІ
текст біо	сам задав	НІ
години постів	спостережене	так
соцграф	спостережене	так
сленг + емодзі	один стиль	рахуй раз

викресли рядки «сам задав» перед підрахунком — кількість ≠ незалежність

Дві купи. Ліворуч — сигнали, які акаунт задає про себе — показуване ім'я, біо, вибір аватара — які самозванець копіює навмисно. Праворуч — сигнали, які ти спостерігаєш ззовні — ритм постингу, хто відповідає, рідкісна одрука — які власник не може тихо скоординувати. Робота таблиці — розсортувати кожну зачіпку в правильну купу перед тим, як рахувати, а стовпець «незалежний?» — це там, де це сортування записується.

Ось справжня, з кейсу нижче.

```
signal-table.txt
kv_designs vs kateryna.v.art
```

signal	strength	indep?
display name	weak	NO self-set
bio text	weak	NO self-set
avatar (bytes)	moderate	YES observed
posting hours	moderate	YES *style-fam
emoji " " close	moderate	YES *style-fam
typo "wich"	strong	YES *style-fam
bio link	moderate	NO! see note
shared repliers	strong	YES 3rd-party

```
-----
* style-fam: timing+emoji+typo are
  correlated -> COUNT AS ONE factor,
  weighted by the rarest (the typo).
! bio link is self-set, BUT a replier
  posted it first -> promote to YES.
-----
```

*Сила й незалежність — окремі стовпці: сигнал може бути сильним, але залежним, або скромним, але незалежним. Три рядки *style-fam згортаються в один фактор перед тим, як рахувати.*

*Читання позначок: indep? питає «чи це незалежний голос?» — YES означає, що він зараховується сам собою, NO означає, що ні. *style-fam тегає одну корельовану стиле-сім'ю (час, сленг, емодзі, одруки), яку рахують один раз, а не по рядку. 3rd-party означає, що сигнал живе на чужих сторінках, поза контролем цілі. ! — це прапорець-примітка — він указує тобі на нумеровану примітку під боксом.*

Читай ту таблицю так, як я, у два проходи. Перший прохід: викресли самозадані рядки. Показуване ім'я, текст біо і — спершу — посилання біо, бо це речі, які власник просто набрав, і які самозванець міг би скопіювати. Геть.

Другий прохід, і це нова дисципліна: я *не* рахую три рядки *style-fam як три голоси. Години постингу, кінцевий емодзі й одрука корельовані — двоє різних людей з міста й дизайнерської сцени Катерини могли б поділити нічні години й навіть рослинний емодзі за випадковістю. Тож я згортаю сім'ю в один фактор і задаю йому вагу за найрідкіснішим членом: одрукою «wich», яка достатньо дивна, щоб випадковий збіг між двома незнайомцями був справді малоймовірним. Той один фактор приземляється на помірному-до-сильного сам собою.

То що насправді виживає, щоб бути порахованим? Ідентичний файл аватара (помірний, незалежний). Стиле-й-часова сім'я, порахована один раз (помірний-до-сильного). Кластер спільних тих, хто відповідає, що живе на чужих сторінках (сильний, незалежний). Плюс підвищене посилання біо. Це три-чотири справді незалежні узгоджені фактори — не сім рядків, з яких таблиця почалася, і не «п'ять сигналів», які заявила б недбала читка.

Рядок посилання біо має зірочку, і це тонкий хід у другий бік. Само собою посилання самозадане — нічого не вартує.

Але я виявив, що один зі *спільних тих, хто відповідає*, постив те саме посилання Linktree місяцями раніше, тегаючи Катерину, до того як будь-який акаунт його показав. Це дає посиланню незалежне походження поза акаунтом, тож я підвищив його до YES. Дисципліна ріже в обидва боки: ти знижуєш корельовані тики, які лише виглядають багатьма, і ти підвищуєш самозадане поле, коли його походження виявляється незалежним. Ти ніколи не оцінюєш сигнал за тим, як він виглядає — лише за тим, звідки він *прийшов* і чи міг би він узгодитися за випадковістю.

Розібраний кейс, зі спокусливим збігом

Клієнт вів маленьку дизайн-студію. Другий акаунт, [kateryna.v.art](#), постив зображення їхнього портфоліо як власні й брав замовлення. Клієнт присягався, що це колишня фрилансерка, Катерина, яка пішла на поганих умовах. Моя робота: чи [kateryna.v.art](#) насправді Катерина, чи хтось, хто видає себе за неї, щоб її очорнити — чи просто випадковий крадій контенту? Вигадані імена, справжній метод.

Спокусливий збіг, спершу. Обидва акаунти показували «Kateryna V.», і обидва біо читалися, слово в слово, «designer · plants · slow living». Мій клієнт розмахував цим як доказом. Це відчувалося як доказ. Це не був — і це рівно та пастка, про яку розділ.

Показуване ім'я й біо — *самозадані*. Якби це був самозванець, що будує фальшиву Катерину, він скопіював би ім'я й біо *навмисно* — у цьому весь сенс видавання себе. Тож збіг однаково узгоджений з «це справді вона» і з «хтось прикидається нею». Сигнал, що пасує кожній гіпотезі однаково, не розрізняє жодної з них. Я записав його в таблицю, позначив **НО** — не незалежний і відмовився дати йому зрушити мою впевненість хоч на щабель. Мій клієнт це ненавидів. Добре.

Тепер справжня робота. Я витягнув файли аватарів з обох акаунтів і порівняв побайтово. Не «схожі» — ідентичний файл, той самий актив. Це важче пояснити самозванцем, який радше зробив би скріншот чи перекадрував. *Помірний, незалежний*.

Тоді сім'я стиле-й-часових сигналів, і тут я навмисно обережний, щоб *не* перерахувати зайве. Я фіксував час постингу три тижні: обидва акаунти жили в тому самому вікні 21:00–01:00 і обидва мовчали в недільні ранки. Обидва завершували більшість постів одним . І обидва писали «which» з помилкою «wich» — та сама специфічна осквозка, двічі від А, тричі від В. Тепер, ледачий аналітик списав би це як три окремі сильні влучення. Я цього не роблю, бо вони корельовані: інший дизайнер з того самого міста й того самого закохано-рослинного кутка інтернету міг би правдоподібно поділити нічні години й емодзі за

випадковістю. Тож я згортаю час, емоції й одруку в один фактор і задаю йому вагу за найрідкіснішим, найособистішим членом — одрукою «wіch», яку жодна спільна субкультура не пояснює. Як один фактор, він приземляється на *помірному-до-сильного, незалежному*. Один фактор, не три.

Тупик. Я збудився через спільний номер телефону. *kateryna.v.art* мав Telegram-посилання, а клієнт дав мені старий номер Катерини з договору. Вони збіглися. Годину я думав, що закінчив.

Потім я перевірів, *звідки прийшов номер на акаунті*. Його витягли зі студійної власної публічної сторінки «наша команда» — яка перелічувала номер Катерини, поки вона там працювала, і досі перелічувала. Тож гіпотеза самозванця пояснювала це так само добре: будь-хто міг зняти той номер зі сторінки, яку студія сама опублікувала. Номер не був незалежним від публічного запису. Він пасував обом історіям. Відкинуто — закреслено в моїх нотатках, «недіагностично, публічно доступне». Зачіпка, що пасує обом твоїм гіпотезам, вартує рівно нічого, хай як вона відчувається перемогою.

Що встояло. Вирішальним був граф. Я намапив постійних тих, хто відповідає, на обох акаунтах. Четверо з шести найчастіших імен були *тими самими справжніми людьми* — колишній однокласник, двоє екс-колег, брат/сестра — і на

власній публічній стіні однокласниці вона відповіла katernyna.v.art з «Kate, це твоя нова сторінка?» і отримала назад підписане «yeah, finally!». Той обмін жив на *чужій* сторінці, поза контролем будь-якого акаунта, і він самопов'язав акаунт зі справжньою людиною.

Склади це стосом, рахуючи чесно — фактори, не рядки, і жодного свідка двічі. Ідентичний файл аватара (помірний, незалежний). Стиле-й-часова сім'я, порахована один раз і несена рідкісною одрукою (помірний-до-сильного).

Спільний кластер приятелів — але однокласниця рахується один раз. Я зараховую її обмін на стіні, тож я не рахую її також усередині кластеру приятелів; кластер дає *трьох інших* справжніх людей (двоє екс-колег і брат/сестра), що все одно сильний. І публічне самопідтвердження однокласниці на власній стіні (сильний), майже-самопосилання, яке власник акаунта не міг би інсценувати. Це чотири справді незалежні узгодження — не шість-сім, до яких порядковий підрахунок роздув би це, і не п'ять, бо однокласницю порахували б двічі. Чотири незалежні фактори, всі узгоджені, з майже-зізнанням серед них, — це добряче за підлогою три-плюс, що заробляє сильний. Я подав підтверджено — та сама людина, це власний акаунт Катерини, і я міг захистити кожен щабель, включно з тими, які я відмовився рахувати двічі.

І я сказав клієнту прямо: збіг імені й біо, та річ, яку *ти* знайшов найпереконливішою, — це той один шматок доказу, який я викинув. Він не доводив нічого. Нудні речі — коли вона постить, хто їй відповідає — доводили все.

Вправа

Візьми два акаунти, які ти вже вважаєш однією людиною — Instagram друга і його Twitter, скажімо. Тепер належно провір власне переконання.

- Збудуй таблицю сигналів з чотирма стовпцями: сигнал · спостережене значення на кожному · сила · незалежний? Тримай силу й незалежність в окремих стовпцях — це різні питання.
- Для кожного рядка постав обидва жорсткі питання. Чи самозадав це власник? І чи могли б двоє різних людей з того самого міста чи субкультури поділити це за випадковістю? Так на будь-яке означає NO у стовпці незалежності.
- Тепер згрупуй свої корельовані сигнали. Будь-які узгодження часу, сленгу, емодзі й одруки йдуть в один стиле-й-часовий фактор, зважений за *найрідкіснішою* рисою в ньому — не рахований по одному.
- Викресли кожен рядок NO і згорни корельовану сім'ю. Порахуй, що лишилося. Скільки справді *незалежних* узгоджених факторів у тебе насправді є?

- Знайди один сигнал, який ти вважав незалежним, і доведи, що він не є — простеж його до єдиного джерела (самозадане поле, публічна сторінка, з якої обидва скопіювали, чи одна спільна субкультура).
- Напиши свій чесний щабель, використовуючи лише вцілілі незалежні фактори. Чи він нижчий, ніж казало нутро? Зазвичай так.

Урок приземляється, коли твоя впевненість *падає* після перевірки. Це падіння — метод у дії. Воно означає, що ти був за крок від того, щоб порохувати свідка двічі.

Підсумок

- Атрибуція — це не одна вбивча зачіпка; це багато малих, незалежних сигналів, що узгоджуються.
- Незалежність має два тести, не один. Сигнал незалежний лише якщо власник не самозадав його і двоє різних людей з тієї самої популяції не поділили б його за випадковістю. Він мусить провалити обидва, щоб зарахуватися як повний голос.
- Незалежні сигнали — будь-що, що акаунт *самозадає*, як показуване ім'я чи текст біо — відчуються як доказ, але не розрізняють нічого. Самозванець копіює їх навмисно.
- Корельовані тики — це один фактор, не багато. Час, сленг, емодзі й одруки рухаються разом для людей з того самого міста чи субкультури — оцінюй їх один раз, за

тим, наскільки *рідкісна* спільна риса, ніколи за тим, скільки ти можеш перелічити.

- Чотири драбинних слова оцінюють дві речі: силу *окремого сигналу* й твій *загальний висновок*. Два незалежні узгодження зазвичай заробляють помірний; три чи більше зазвичай заробляють сильний — але кількість лише орієнтир. Що насправді заробляє *сильний* — це те, що ці узгодження разом важко пояснити будь-якою суперницькою гіпотезою. Один «сильний» сигнал — це не сильна знахідка.
- Збудуй таблицю сигналів з окремими стовпцями сила й незалежний?. Викресли самозадані рядки, згорни корельовану сім'ю, потім порахуй, що вижило.
- Зачіпка, що пасує *обом* твоїм гіпотезам однаково, недіагностична — відкинь її, хай як добре вона відчувається.
- Найсильніші сигнали живуть на *чужих* сторінках, поза контролем цілі. Зважуй їх відповідно.



РОЗДІЛ ВОСЬМИЙ

Боротьба з власною певністю

Акаунт, який тобі найбільше треба розслідувати, — це той, що веде розслідування.

У тебе гарна атрибуція. Кілька незалежних сигналів, усі узгоджені, чистий підйом драбиною. Воно відчувається завершеним. Ти можеш уявити, як пишеш «підтверджено».

Це відчуття — найнебезпечніша мить у всій роботі.

Бо на цей момент ти вже *хочеш*, щоб воно було правдою. Ти витратив на це години. Ти сказав клієнту, що близько. Твій мозок люб'язно перестав шукати проблеми й почав захищати

відповідь. Кожна нова деталь якось пасує. Ніщо більше тебе не дивує. Це не справа, що міцніше — це ти сліпнеш.

Перший том сказав тобі стежити за власною упередженістю. Цей розділ — вправа, щоб насправді це робити: набір конкретних ходів, що змушують тебе атакувати власний висновок раніше, ніж це зробить хтось інший. Мета — не відчувати впевненість. Мета — *заслужити* свою впевненість і вміти сказати «не можу атрибутувати» вголос, коли не можеш.

Ідея: спробуй зламати власну відповідь, навмисно

Інстинкт, щойно ти маєш теорію, — піти зібрати більше доказів *за* неї. Це відчувається як старанність. Насправді це пастка. У кожному розслідуванні досить шуму, щоб рішуча людина завжди знайшла ще одну річ, що «пасує».

Нагромадь досить підтверджувального сміття — і навіть хибна теорія виглядає в броні.

Ліки — інвертувати пошук. Замість питати «що ще це підтримує?», ти ставиш питання, що насправді перевіряє теорію:

Що я очікував би побачити, якби був неправий — і чи бачу я це?

Це прохід на спростування. Ти формулюєш висновок як гіпотезу, уявляєш світ, у якому вона хибна, перелічуєш, що той хибний світ лишив би валятися довкола, а тоді йдеш шукати *саме це*. Якщо ти жорстко полюєш на спростування й справді не можеш його знайти, твій висновок виживає — і тепер він випробуваний у бою, а не просто затишний. Якщо ти знаходиш спростування, ти щойно врятував себе від публікації помилки.

Це та сама логіка, що й дисципліна конкурентних гіпотез, яку використовують аналітики: ти виграєш не нагромадженням підтримки для улюбленої, а *усуненням альтернатив*.



Дві живі гіпотези — «та сама людина» (А) і «двоє людей, одна субкультура» (В). Сигнал, що пасує до обох, не пояснює нічого; тільки сигнал, що пасує до однієї й ламає другу, тебе рухає. Прохід на спростування полює на факт, що вбиває

твою улюблену — і тут один такий є.

Це важить тим більше, чим довше ти працював над справою. Зусилля тихо стає власністю. За десять годин теорія вже не просто теорія — це *твоя* теорія, і збити її відчувається як зізнання, що ти змарнував десять годин. Ось чому прохід на спростування має бути *процедурою*, а не настроєм. Добрі наміри тебе не врятують; у тебе вже добрі наміри, і ти все одно упереджений. Що рятує тебе — це сісти, написати чекліст хибного світу й перемолоти його, хочеш ти того чи ні — особливо коли не хочеш.

Метод: чотири ходи до висновку

Проганяй їх по порядку, щоразу, коли відповідь починає відчуватися певною. Вони забирають двадцять хвилин і врятовують твою репутацію.

1. Сформулюй гіпотезу одним пласким реченням. Запиши її, прямо. «Акаунт В веде та сама людина, що й акаунт А.»

Назвати її означає перетворити тепле відчуття на твердження, яке можна перевірити. Твердження, яке ти ніколи не записав, — це твердження, яке ти не можеш атакувати — і за яке тебе не притягнеш.

2. Зроби прохід на спростування — «що доведе, що я неправий?» Перелічи спостереження, яких ти очікував би, *якби теорія була хибна*, тоді йди шукати кожне. Якщо А і В — та сама людина, вони ніколи не мають постити в ту саму

хвилину з несумісних місць. Тож: чи вони колись постили *одночасно*? Чи В знає щось, чого А знати не міг? Чи В продовжував протягом тижня, коли А був доказово офлайн? Ти намагаєшся спіймати власну теорію на суперечності. Полюй так, ніби тобі платять за те, щоб її зламати.

3. Напиши альтернативні пояснення й візьми кожне серйозно. «Та сама людина» рідко є єдиною історією. Змусь себе назвати інші, бо збіг, який ти ніколи не сформулював, — це той, який ти не можеш виключити:

- Двоє різних людей, що справді ділять субкультуру, сленг, рідне місто — тож їхній стиль і час схожі з нудних причин.
- Спільний акаунт — пара, команда, малий бізнес — тож «людина» — це дві руки на одному логіні, а твоя стилometрія — усереднення обох.
- Перевикористаний нік — юзернейм закинули й перереєстрував незнайомиць, тож «історія акаунта» — це насправді дві людські історії, зшиті на даті передачі.
- Підсадка чи маріонетка — хтось *збудував* В, щоб той виглядав як А, навмисно, копіюючи самозадані сигнали, щоб підставити чи видати себе. (Це точнісінько чому сьомий розділ змусив тебе викинути самозадані поля.)

Для кожної альтернативи спитай: який доказ вона лишила б, і чи я насправді її виключив — чи просто не подумав про неї?

4. Відділи факт від висновку у своїх нотатках. Пройди файл і познач кожен рядок одним чи іншим. *Факт*: «обидва акаунти постили 21:00–01:00 протягом трьох тижнів» — ти спостеріг це. *Висновок*: «отже, вони в тому самому часовому поясі» — ти це виснував. Висновки можуть бути хибними, поки факти лишаються правдою (планувальник, VPN, безсоння в іншому поясі). Коли ти розмиваєш ці двоє, ланцюг здогадів починає читатися як ланцюг доказів. Тримай їх у різних колонках, щоб завжди знати, який несе навантаження.

Ось як той розподіл виглядає на папері.

нотатки справи — тримай колонки нарізно	ФАКТ (спостережено)	ВИСНОВОК (зроблено)
-----		-----
обидва пост. 21-01		той самий пояс
обидва пишуть "wich"		той самий автор
В знав новий тел. А		В близький до А
А мовчить 3-9 бер.,		??? -> див.спрост.
В постив щодня		
-----		-----
позначка: рядок 4 — це СУПЕРЕЧНІСТЬ,		
не підтвердний факт. не підшивай		
його під "докази за".		

факт і висновок у окремих колонках

Подивись на той четвертий рядок. Це факт, що *не* пасує до теорії — А був доказово офлайн тиждень, поки В постив щодня. Підтверджувальний розум прослизає повз нього. Прохід на спростування витягує його на світло, у власну

колонку, з позначкою. Той рядок — це там, де тепер живе справжня перевірка справи.

Спробуй (2026). Візьми атрибуцію, у яку ти зараз віриш — власну живу справу чи публічну, яку ти бачив упевнено оголошеною, — і запиши на чистому аркуші два питання: *«що я очікував би побачити, якби був неправий?»* і *«який один факт це вбив би?»* Тоді проведи двадцять хвилин, полюючи лише на той вбивчий факт — не на більше підтримки, не на «колір», лише на спростування. Коли двадцять хвилин вийшли, чесно переоціни свій щабель проти того, що знайшов (чи не знайшов). Якщо твоя впевненість упала на щабель або приземлилася на «не можу підтвердити», прохід спрацював рівно так, як задумано. Це найкорисніша професійна звичка в цій книзі — та, що більше за будь-який інструмент відділяє людей, чиї знахідки витримують виклик, від тих, чиї — ні.

Проблема калібрування: слабкі купи — це не сильно

Є повільний, тихий режим провалу, що ловить обережних людей. Ти збираєш десять слабких зачіпок. Жодна не сильна. Але їх *десять*, і сама купа починає відчуватися як сильна справа. Тож «слабкий × 10» тихо стає «підтверджено» у твоєму резюме, і ніхто — включно з тобою — не помічає, як стається підвищення.

Сьомий розділ уже сказав тобі чому: десять зачіпок, що простежуються до одного джерела, — це одна зачіпка, порахована десять разів.

Тож не питай, скільки сигналів у тебе є. Питай, скільки *незалежних* — і чи їхнє узгодження важко пояснити, хіба що акаунти — одна людина. Пиши чесний щабель.

Обстоюваний «сильний» б'є необстоюваний «підтверджено» щоразу.

Розібраний кейс, що не розв'язується

Ньюзрум попросив мене підтвердити, що анонімний акаунт, @civic_watch_ua, що постив гостру критику місцевої ради, справді був конкретною працівницею ради — назвемо її О. — що зливала зсередини. Це *відчувалося* певним за годину. Це відчуття — причина, чому я розповідаю цю історію. Вигадані деталі, справжній метод.

Спокуслива купа. @civic_watch_ua постив лише 22:00–01:00 — відомі позаробочі години О. Він використовував конкретний процедурний жаргон, який знав би інсайдер ради. Він одного разу згадав бюджетний рядок до того, як той став публічним. І його біо казало «погляди мої власні · держслужбовець». Час, інсайдерське знання, майже-зізнання в біо. Репортер був готовий друкувати.

Я написав гіпотезу пласко: «*@civic_watch_ua — це О.*» Тоді я зробив прохід на спростування, і воно розпалося в моїх руках.

Спростування, хід за ходом. *Що я побачив би, якби це хибно?* Спершу: біо. «Держслужбовець» самозадане — О. написала б це, але так само й будь-хто, хто хоче, щоб акаунт *читався* як інсайдер, включно з суперником, що намагається звалити провину на О. Воно пасувало до «це О.» і «хтось підставляє О.» однаково. Не діагностично. Викреслено.

Бюджетний «злив» відчувався сильним, поки я не пополював на альтернативу. Я знайшов ту саму цифру в циркулярі комітету, що пішов до *сорока* людей. Інсайдерське знання, так — інсайдер для сорока, не для однієї. Це звузило автора до великої кімнати, не до О. Знижено до слабкого.

Тоді спростування завдало справжнього удару. Я перевірів суперечність — чи акаунт колись працював, поки О. була доказово деінде? О. постила відпускні фото зі свого власного, справжнього, іменного акаунта з-за кордону, з видимим поясом телефону, дев'ять днів поспіль.

@civic_watch_ua постив усі дев'ять, у тому *самому* вікні 22:00–01:00 за київським часом, ніколи не зсуваючись на відпускні години. Два прочитання: або це не О., або О. запланувала пости, або це спільний акаунт, і *інша* рука постила далі. Я не міг сказати, яке. Той єдиний факт зламав чисту історію, і я не міг її роззламати.

Альтернативи, взяті серйозно. *Двоє людей*: правдоподібно — радний сленг і позаробочі години пасують будь-кому з кількох інсайдерів. *Спільний акаунт*: правдоподібно — могла бути мала група працівників, що пояснило б постинг прямо крізь відпустку О. *Перевикористаний нік*: перевірено, виключено, акаунт був заюним. *Підсадка*: справді можливо — суперницька фракція мала мотив зробити так, щоб зливи виглядали, ніби йдуть від О. Я не міг усунути ні першого, ні другого, ні четвертого.

Чесний результат. Я мав час, що пасував О., але також пасував трьом іншим історіям. Я мав інсайдерське знання, спільне для сорока людей. Я мав самозадане біо, що нічого не вартувало. І я мав один твердий факт — постинг прямо крізь її підтверджену відсутність — що активно боровся з теорією. Відділяючи факт від висновку, мої факти були справжніми, але кожен місток до «це О.» був висновком із живою альтернативою під ним.

Я відзвітував це так, як знайшов: не можу підтвердити — не робіть висновку. Слабкий-до-помірного, що автор — інсайдер ради; *жодної* обстоюваної атрибуції конкретно до О.; жива, невиключена можливість, що акаунт збудували, щоб *підставити* її. Я сказав ньюзруму прямо, що назвати О. не витримає виклику й могло б віддати наклепу довіру їхнього видання. Вони притримали матеріал. За місяці судова заява назвала групу з трьох осіб — жодна з них не О.

Мое «не можу підтвердити» витримало час.

«Підтверджено» було б катастрофою з моїм ім'ям на ній.

Це весь сенс розділу. Дисциплінована відповідь іноді — «я не знаю», і подати цю відповідь чисто — відмовившись дати теплому відчуттю й товстому файлу заштовхати тебе на шабель, який ти не можеш обстояти, — це не провал. Це найпрофесійніше, що ти колись зробиш.

«Я не можу це підтвердити» — це знахідка. Кажи це з тією ж упевненістю, з якою сказав би «підтверджено».

Вправа

Візьми атрибуцію, у яку ти зараз віриш — таку, що відчувається твердою. Тепер спробуй її знищити.

- Напиши гіпотезу одним пласким реченням. Без застережень, без відчуття — твердження.
- Прожени прохід на спростування: перелічи, що б ти побачив, якби воно було хибне, і йди пополюй на кожен пункт. Чи акаунти колись постили одночасно? Чи один знає щось, чого інший не міг? Будь-яка суперечність, повз яку ти прослизаш?
- Запиши всі чотири альтернативи — двоє людей, спільний акаунт, перевикористаний нік, підсадка. Для кожної назви, що б її виключило, і чи ти це насправді

маєш.

- Розділи нотатки на дві колонки: факт, який ти *спостеріг*, проти висновку, який ти *зробив*. Порахуй, скільки твоїх містків до висновку — це висновки з живою альтернативою під ними.
- Перерахуй свої *незалежні* сигнали — не спостереження, незалежні. Тепер напиши щабель. Якщо він упав або приземлився на «не можу підтвердити», ти зробив вправу правильно.

Якщо твоя певність вижила після справжньої спроби її вбити, вона була справжньою. Якщо ні — ти щойно ухилився від помилки, що завершує кар'єри.

Підсумок

- Найбільша загроза атрибуції — аналітик, що хоче бути правим; певність — це попереджувальне світло, не фінішна лінія.
- Інвертуй пошук: не збирай більше підтримки, спитай «*що доведе, що я неправий?*» і йди пополюю на спростування.
- Чотири ходи до висновку: сформулюй гіпотезу пласко, прожени прохід на спростування, назви й перевір кожну альтернативу (двоє людей / спільний акаунт / перевикористаний нік / підсадка) і відділи факт від висновку у нотатках.

- Купа слабких чи не незалежних зачіпок — це не сильна справа. Кількість — це не незалежність; сто чуток з одного рота — це один рот.
- «Не можу атрибутувати» — це законна, професійна знахідка. Подай її чисто, а не силуй висновок, якого докази не втримають.



РОЗДІЛ ДЕВ'ЯТИЙ

Повна атрибуція

Кожна нитка, зіткана заразом

Усе досі було однією ниткою, витягуваною повільно.
Нікнейм. Обличчя. Злитий email. Одна техніка за раз, у
чистому світлі.

Справжня робота не така. Справжня робота — це вісім
ниток заразом, більшість із них розлазиться, дві з них тобі
брешуть, і годинник цокає. Цей розділ — один кейс, від
початку до кінця, так, як це насправді трапляється. Безлад
навмисно.

Питання було мале. Відповідь забрала тиждень.

Я покажу тобі й тупики. Кейс без тупиків не розслідували — його оздобили.

Запит

Клієнт вів маленький бізнес з перепродажу електроніки. Хтось на маркетплейсі скуповував повернений товар оптом під ім'ям продавця **voltbin_ua**, потім перепродував його як новий і, коли покупці скаржилися, постив справжню адресу компанії клієнта як «склад» для злих самовивозів. Клієнт хотів одну річ:

Хто стоїть за voltbin_ua, і це одна людина чи вітрина?

Це все. Не арешт. Не дім. Ім'я і рівень впевненості, чесний достатньо, щоб діяти. Усе нижче служить тому одному реченню.

Я відкрив свіжу нотатку кейсу з трьома стовпцями: твердження, докази, щабель. Ніщо не йде у звіт, поки не заробить щабель.

Зачіпка й перша стіна

Одна зачіпка для початку: сторінка продавця.

```
marketplace – seller profile
-----
seller:    voltbin_ua
joined:    2023-11
sales:     412
rating:    4.1
location:  Kyiv (self-reported)
contact:   via platform messages only
-----
```

публічна картка продавця маркетплейсу

Це вся публічна поверхня. Ні телефону. Ні email. Обмін повідомленнями замкнено за платформою. Вхідні двері зачинені; бічні вікна — інша справа.

Тож я перестав пробувати вхідні двері. Я не намагався купити товар, щоб запустити розкриття контакту — це виготовляє транзакцію й ставить справжню людину на гачок. Тільки відкриті джерела.

Єдине, що стіна дала мені задарма, — сам рядок: `voltbin_ua`.

Півот нікнейму

Тож я прогнав `voltbin_ua` і корінь `voltbin` по платформах — вручну й інструментом пошуку нікнеймів, потім перевірів кожне влучення за *змістом*, ніколи за самим збігом.

```
handle sweep – root "voltbin"
-----
voltbin_ua telegram EXISTS
voltbin    instagram EXISTS
voltbin    github    404
voltbin_ua twitter/x suspended
voltbin.shop domain  parked, no records
voltbin    reddit    EXISTS (1 post, 2019)
-----
```

перевір нікнеймів, неперевірений

Шість влучень. Більшість — шум, поки не доведено інше.

Дивися, як швидко вони падають.

reddit voltbin — один пост, 2019, на форумі про акваріуми, написаний англійською користувачем, чії інші коментарі твердо розмішують його в Канаді. Наш продавець приєднався до маркетплейсу у 2023 і торгує в Україні. Не та тема, не та країна, не ті роки. Я не відкинув це через те, що ім'я було *трохи* інше — воно було ідентичне. Я відкинув це за змістом і датами.

Відкинуто: reddit/voltbin. Не наша ціль. Щабель: н/д.

github 404 і запаркований домен просто порожні.

Порожнеча — не знахідка. Я написав «немає даних» і рушив далі — відсутність корисна лише якщо ти спершу очікував присутності.

Лишаються telegram і instagram. Обидва живі. Обидва варті повільного погляду.

Telegram — тільки публічне

Telegram-нікнейм `voltbin_ua` розв'язався в користувача. Публічний профіль, без біо, типовий аватар. Але нікнейм з'явився як *автор* у двох публічних групах перепродажу — відкриті канали, які будь-хто може читати, ні до чого приватного не приєднуючись.

```
telegram — public group mention
-----
group:  @kyiv_tech_resale (public)
from:   voltbin_ua
text:   "partii lcd matrytsi, samovyviz
        livyi bereh, opt vid 10 sht"
date:   2024-02-18
-----
```

публічний пост каналу, машинно зчитаний

Українською: «*партії LCD-матриць, самовивіз, Лівий берег, опт від 10 штук.*» Та сама торгівля, те саме місто, узгоджено з продавцем маркетплейсу. Це помірного-щабля зв'язок між `voltbin_ua` маркетплейсу й `voltbin_ua` Telegram — тема, географія й час вирівнюються, але спільний нікнейм плюс спільна тема — це досі лише два сигнали, що вказують в один бік. Це не доказ, що одна рука набирає обидва.

Я витягнув числовий Telegram user ID і занотував його. Нікнейми міняються; ID — хребет акаунта. Якщо `voltbin_ua` перейменується завтра, ID досі зшиває історію докупи. Я не приєднувався до жодної закритої групи, не писав акаунту, не додавав номер у контактну книгу, щоб виростити ім'я.

Публічне читання, ID записано, стоп.

Одна тиха річ: акаунт одного разу переслав повідомлення з каналу під назвою @denys_zip_kyiv. Пересилання — це стосунок *якогось* роду — але слабкий, і я хочу бути ясним наперед про те, чим воно не є. Це не самопосилання, не спільне фото, не спільна кімната. Я запаркував це як вільну нитку. Воно повертається пізно в цьому розділі, і — спойлер — воно ніколи не заробляє собі шляху у відповідь.

Проблема обличчя

Instagram voltbin мав одинадцять фото — переважно коробки товару, два верстаки й одне чоловіка, що тримає паяльник, обличчя чітке, зняте в чомусь схожому на гараж.

Обличчя — це міст, не ім'я. Я не прогнав його крізь рушій пошуку облич, що зшкрябує відкриту мережу, аби знайти кожне інше фото цієї людини — питання клієнта цього не потребувало, і той інструмент тягнеться повз відкритий постинг у побудову біометричного досьє на приватну особу. Я зупинився при тій межі й записав, що зупинився, і чому.

Що я *міг* зробити з відкритими джерелами: порівняти фото верстака зі зображеннями, вже прикріпленими до акаунтів, які я мав законну публічну причину переглядати. Telegram voltbin_ua місяцями раніше постив фото ремонтного верстака в публічній групі. Той самий відмітний зелений різальний килимок, той самий бренд лампи-лупи, ті самі

грати на вікні на задньому плані.

visual cross-check (analyst notes)

IG "voltbin" bench photo:

- green cutting mat, worn corner
- magnifier lamp, ring type
- barred window, 4 vertical bars

TG bench photo (public group):

- green cutting mat, worn corner
- magnifier lamp, ring type
- barred window, 4 vertical bars

ручне порівняння сцени, не біометричне

Це збігання *сцени* — кімнати, не чоловіка. Два акаунти сфотографували той самий фізичний верстак. У поєднанні зі спільним нікнеймом і спільною торгівлею кластер маркетплейс / Telegram / Instagram тепер тримається купи на сильному щаблі — та сама *майстерня*, майже напевно. Чи означає це одного оператора, чи двох людей, що ділять кімнату, — питання, яке прохід спростування мусить залагодити пізніше; саме збігання кімнати не може. Досі без імені.

Міст із витоку

Щоб перетворити цей кластер на *людину*, мені потрібен ідентифікатор, що живе у світі — email, телефон — прив'язаний до одного з цих акаунтів через відкрите джерело, не через купівлю.

Instagram-акаунт роками раніше вів на неіснуючий особистий блог, voltbin-repairs.blogspot, заархівований. Заархівована контактна сторінка перелічувала бізнес-email:

```
web archive – blog contact page
-----
captured: 2022-06-30
"Napyshit: voltbin.fix@gmail.com"
"Telegram: @voltbin_ua"
-----
```

заархівована сторінка, публічне захоплення

Email, який акаунт *опублікував сам*. Це чесна гра — його виклали відкрито для клієнтів. Чи з'являється цей email у якомусь відомому публічному корпусі витоків? Витік може сказати тобі, що email *співпояву* з ім'ям чи телефоном у якомусь дампі. Він не може, сам собою, сказати тобі правду тієї пари. Дампи брудні. Люди брешуть у формах реєстрації. Обліковими даними набивають.

```
breach-index lookup (fictional)
-----
query: voltbin.fix@gmail.com
-----
source A "electro-forum-2021"
  username: voltbin
  reg_name: Denys K.
  phone: +380 (67) 555 0148
source B "coupon-site-2020"
  name: Denys Koval
  city: Kyiv
source C "gaming-2019"
  name: Artem Bond
  phone: +380 (50) 555 0921
-----
```

агрегований результат індексу витоків

Три джерела. Двоє з них (А, В) узгоджуються на імені: Denys, одне дає прізвище Koval, Київ, і телефон. Третє (С) каже Artem Bond з іншим телефоном. Ця суперечність — не морока, це інформація. Одне з цих — справжня реєстрація нашого оператора, і принаймні одне — шум:

перевикористаний пароль, набитий деінде, або хтось, хто набрав цей email випадково, або навмисно фальшиве ім'я.

Я не обрав «Denys», бо двоє б'ють одного і це відчувалося правильним. Двоє брудних джерел можуть ділити ту саму помилку. Я позначив увесь крок email→ім'я як слабкий, поки щось *поза* корпусом витоків це не підкріпить. Це мить, коли більшість кейсів іде не так — правдоподібне ім'я з'являється, і слідчий тихо підвищує здогад до факту.

Коло й замкнені двері

Хід «Сімейний ланцюг». Коли власний профіль цілі зачинено, люди навколо неї часто ні, а стосунки несучі.

Спершу спокуса, від якої я відмовився. Дамп *прошенотів* прізвище — «Koval», з джерела В — а запарковане пересилання прийшло з каналу під назвою @denys_zip_kyiv, корінь імені, що теж виглядав як «Denys». Було б легко сплести ці дві нитки до купи й оголосити «Denys Koval». Але подивися, з чого зроблено цю плетінку: брудний запис витоків і рядок-нікнейм. Два слабкі, майже-самозадані клапти

не стають сильними від того, що їх зв'язали одне з одним. Я відклав обидва й пішов шукати прізвище дець, що могло б його насправді *понести*.

Я знайшов його в самому кластері акаунтів. Instagram voltbin мав одне фото, у якому його публічно позначив тегом інший акаунт — @koval_secondhand, маленька крамниця вживаної електроніки. Тег — це двобічна публічна дія: крамниця обрала прикріпити себе до посту нашого оператора, відкрито, за роки до мого приходу. Той зв'язок не маршрутується крізь @denys_zip_kyiv взагалі. Він стоїть сам по собі.

Я подивився на @koval_secondhand публічно, і кімната зробила решту. Одне з його фото верстака показувало *той самий зелений різальний килимок, зношений у тому самому кутку, і те саме вікно з чотирма ґратами*, вже прив'язане до кластера збіганням сцени. Тож цей акаунт не був незнайомцем, що випадково поділив ім'я — його сфотографували всередині тієї самої майстерні, від якої відштовхується весь кластер. І керував ним, відкрито, один О. Koval.

Ранній шепіт «Koval» із витоку тепер виглядає як підкріплення — третя дорога, що випадково узгоджується, — ніколи не джерело.

Я таки спробував дістати власне ім'я оператора в лоб — і вдарився об стіну: особистий Facebook, натякнутий телефоном із джерела А, був повністю замкнений. Ні публічних постів, ні списку друзів, нічого. Тупик через вхідні двері — знову.

Тож, хід Розділу шість: не *крізь* замкнені двері, *навколо* них. @koval_secondhand був публічний і балакучий. Пост там, що вітав когось із днем народження, називав «Denys» і показував фото біля верстака — *той самий зелений різальний килимок і вікно з ґратами* зі збігання нашої сцени.

```
public post – @koval_secondhand
-----
date: 2024-05-12
text: "Z dnem narodzhennia, brat!
      Denys, nekhai remontuietsia
      lehko :)"
photo: bench, green mat, barred
       window (matches cluster)
-----
```

публічний пост родича до дня народження

Родич, відкрито, поставив ім'я на точну кімнату, яку ми вже прив'язали до кластера акаунтів незалежним методом. Ім'я Denys уже не прибувало задарма — воно прибувало зі *сцени* тепер, не з дампу.

Я не контактував з родичем і нічого в нього не питав. Я прочитав те, що вже було публічним, і зупинився — втертися до члена сім'ї, щоб виманити прізвище, за межею.

Складання стосом, потім спроба зламати

Викладу справді незалежні фактори пліч-о-пліч для твердження `voltbin_ua` → Denys Koval. Два факти, що прибувають через один акаунт, — це одне джерело, а не два голоси — саме навколо цієї пастки й вибудований цей список:

- Спільний нікнейм на маркетплейсі, Telegram, Instagram (*фактор 1*)
- Той самий фізичний верстак на фото TG + IG (*фактор 2 — кімната, не рядок, тож незалежний від нікнейму*)
- Самоопублікований email на заархівованому блозі (*фактор 3*)
- Ім'я — прізвище *Koval* і ім'я *Denys* обидва прибувають через `@koval_secondhand`, один акаунт, прив'язаний до кластера збіганням кімнати. Два факти, одне джерело (*фактор 4*)

Тож чесна лічба — три-чотири справді незалежні фактори, не п'ять. За задумом відсутні: здогад дампу про ім'я й пересилання `@denys_zip_kyiv` — жоден не несе особи. Фактор 4 — єдина точка відмови для *імені*; фактори 1–3 тримають знахідку про самотнього оператора самі собою. Ця багаточасова структура зрушує твердження до сильного — і, з проходом спростування нижче, що вистояє, до сильного-сильного — на один сигнал нижче за

підтверджено, поки суперник-брат лишається відкритим.

Тоді я зробив те, що відчувається як саботаж і ним не є: я спробував *спростувати* це. Якби я був неправий, що я б очікував побачити?

- Якби *voltbin_ua* був *вітриною* — кілька людей ділять один логін — стиль письма по постах Telegram мав би дрейфувати: різні години, різні формулювання, різний діалект. Він не дрейфував. Послідовні вечірні пости, послідовне суржикове формулювання (суржик — мішана українсько-російська мова), послідовна одрука (*samovyviz* завжди одним словом). Читається як одна рука.
- Якби *email* належав комусь іншому, хто його просто перевикористав, самоопублікований блог, що пов'язує цей email з *@voltbin_ua* у 2022, мусив би бути збігом тричі. Він виживає виклик.
- Якби «Denys Koval» був зшивкою двох різних людей, кімната верстака не з'являлася б і під кластером акаунтів, і під постом родича. Вона з'являється під обома.
- Найжорсткіший суперник, і той, який охайна версія пропускає: що як оператор — О. Koval — брат, що керує *@koval_secondhand*, — а *Denys* лише той брат, який теж з'являється біля того верстака? Обидва Ковалі користуються тією кімнатою, тож збігання кімнати саме собою не може розрізнити братів. Два тонкі факти нахиляють оператора до Denys: *власний* опублікований

ідентифікатор оператора — email `voltbin.fix@gmail.com` і нікнейм `voltbin` — співпояву в корпусі витоків з Denys (джерела А і В), ніколи з О.; і саме О. Koval у пості до дня народження звертається до Denys як *брат* — пишучи до операторської особи ззовні неї, не як вона. Брудна прив'язка, нечистий нахил — суперник не вмирає повністю. Він стискається до залишку, і я тримаю його названим.

`voltbin_ua` — це самотній оператор, що працює з майстерні Ковалів — найімовірніше Denys Koval, Київ, з його братом О. Koval як названою залишковою альтернативою, яку я не міг чисто виключити. Щабель: сильний, на межі підтверджено.

Гілка, що не хотіла закриватися

Тепер частина, яку чисті підручники пропускають.

Повніше занепокоєння клієнта було в тому, що `voltbin_ua` — це фронт для *організованого кільця шахрайства з поверненнями* — що «Denys» був одним вузлом серед кількох скоординованих продавців. Пересилання з `@denys_zip_kyiv`, крамниця брата, кілька інших нікнеймів перепродажу, що кросс-постили ті самі фото товару — це *пахло* мережею.

Я гнався за цим. І мушу сказати тобі чесно: я не міг це закрити.

```
network hypothesis – status
-----
voltbin_ua -> Denys Koval STRONG
koval_2hand -> O. Koval related
denys_zip -> ??? same as Denys?
    handle name matches, but:
    - different posting hours
    - no shared photos
    - no self-link either way
    status: UNRESOLVED
ring coordination? NOT SHOWN
-----
```

дошка статусу аналітика, відкриті пункти

@denys_zip_kyiv ділить ім'я й переслане повідомлення з нашою ціллю. Це все. Години постингу не збігаються зі встановленим візерунком. Немає спільних фото. Жоден акаунт ніколи не посилається на інший як на *себе*. Це міг би бути той самий Denys, що керує другим акаунтом. Це міг би бути справді інший Denys у тій самій маленькій торгівлі — а в київській сцені запчастин, поширене ім'я, перетинні постачальники, це цілком звично. Спільний корінь нікнейму — найслабший сигнал, що існує, а пересилання — це контакт, не особа.

Тож я не розв'язав це.

І це та частина, що тримає весь звіт чесним: бо та гілка лишилася слабкою, вона живила *ніщо* в атрибутції над нею. Викресли @denys_zip_kyiv з кейсу цілком — і «Denys Koval, самотній оператор, сильний» не зрушиться ні на міліметр.

Це тест на карантин — якщо видалення нерозв'язаного сліду ослабило б твою впевнену знахідку, згодом підпирав відповідь. Тут — ні.

Чесний щабель тут — слабкий, а слабкий не йде у висновки. Він іде в секцію «не вдалося підтвердити», за іменем, щоб клієнт знав точно, чого я не знаю.



Увесь граф на одній сторінці: насіння *voltbin_ua*, що півотить назовні через маркетплейс, Telegram, Instagram і заархівований блог, з чотирма незалежними сигналами (нікнейм, збігання кімнати, самоопублікований email, прив'язаний до кімнати акаунт родича), що сходяться на одній особі — Denys Koval, сильний. Гілка *@denys_zip_kyiv* звисає збоку, пунктирна й відкрита: досягнута, але ніколи не розв'язана, і навмисно несуча ні для чого.

Міні-звіт рішеного ґатунку

Усе вище стискається до однієї сторінки, за якою клієнт може діяти.

ATTRIBUTION SUMMARY – voltbin_ua

ASKED:

Who operates seller "voltbin_ua",
and is it one person or a front?

FOUND:

Single operator, working from the
Koval workshop, most likely
Denys Koval, Kyiv, electronics
repair/resale. Named residual:
brother O. Koval (shared bench).

CONFIDENCE:

сильний: одинокий оператор
з майстерні Ковалів
хилиться до сильного: саме Denys,
з братом O. Koval як
названим залишком

BASIS (independent factors, ~3-4):

- handle reuse across 3 platforms
- shared physical workbench in
TG + IG photos (scene match)
- self-published email, archived
- name (surname + first name) from
one room-tied account
(@koval_secondhand) - counts as
ONE source, not two, not the dump

RULED OUT:

- reddit "voltbin": wrong country,
topic, years (content-rejected)
- "Artem Bond" in breach index:
unsupported outside the dump
- shopfront theory: writing style
reads as one hand, not many

COULD NOT CONFIRM:

- that voltbin_ua is part of an
organised ring

- that @denys_zip_kyiv is the same person (weak; name-root only)
- > DO NOT CONCLUDE either.

NOT DONE (ethical line):

- no face-search, no purchase to unmask, no locked-profile access
- no messaging target or relatives

SOURCES:

marketplace card; 2 public TG groups; IG public posts; archived blog (web capture 2022-06-30); breach index (3 sources, treated as dirty); relative's public post. All captures archived + hashed.

готовий продукт, одна сторінка

Зауваж форму. Впевнене твердження веде. Відкидання названі. Невирішена гілка вказана *як* не вирішена, не похована. Те, що я обрав не робити, перелічено, бо клієнт заслуговує знати краї роботи так само, як її середину. І джерела несуть архівну примітку — кожен публічну сторінку захопили й гешували на місці, бо відкриті сторінки видаляють, а знахідка, яку ти не можеш перепоказати, — це знахідка, яку ти не можеш захистити.

Про що цей розділ був насправді

Дев'ять технік, і жодна з них не була відповіддю сама собою.

Нікнейм не привів мене нікуди, поки зміст не вбив хибне влучення. Обличчя я відмовився шукати — *кімната* — ось що заговорило. Витік вручив мені ім'я, якому я був правий не довіряти, а те саме ім'я, що прибуло другим шляхом, від родича, — ось що зробило його справжнім. І найохайніша, найзадовільніша нитка — кільце — та, яку я мусив лишити висіти.

Це крос-платформна атрибуція.

Вміння ніколи не було знайти сигнал. Воно було зважити його.

Що ти вмієш тепер

— і що буде далі.

Зупинися на секунду й подивись, як далеко ти зайшов.

У першому томі ти міг узяти одну зачіпку й знайти людину. Тепер ти можеш узяти людину, розкидану по десятку платформ — приватну тут, видалену там, сховану за другим ніком десь ще — і зіткати її назад в одну особистість, за яку ти справді можеш поручитися. Ти можеш обійти стіну замість того, щоб битися об неї. Ти можеш відрізнити незалежний сигнал від збігу. І ти можеш сказати, вголос і чесно, *наскільки ти певен* — включно з найважчим реченням у цьому ремеслі: «Я не можу це підтвердити».

Ця остання навичка — та, що тепер відділяє тебе. Збирати вміє будь-хто. Атрибуція — рішення, що всі ці розкидані шматки — *одна справжня людина* — це там, де живе судження, і де завдається шкода, коли судження підводить. Ти витратив усю цю книжку, вчачись не дурити себе. Тримайся цього.

Тримай звички, не інструменти

Платформи мінятимуться. Той конкретний бот, той конкретний пошук, той конкретний сайт зникне за рік чи буде перейменований. Ніщо з цього не важить. *Форма* роботи не змінюється: знайди відкриті довкола зачинених дверей, півоть із дисципліною, склади незалежні сигнали — окремі джерела, пораховані по разу — зваж кожну знахідку на драбині й зупинися на лінії. Вивчи це — і кожна нова платформа лише ще одні двері для того самого методу.

Де далі гострити

- Працюй над собою, по платформах. Зроби всю річ на власному сліді — знайди кожен акаунт, кожну позначку, кожен витік, що прив'язується до тебе. Тоді прибери це. Найкраща вправа, яка є.
- OSINT CTF і виклики на верифікацію. Вони тренують міжплатформний півотинг і дисципліну доказу, безпечно й безкоштовно.
- Заходи з пошуку зниклих людей (як-от Trace Labs) — справжня, значуща робота, поряд із людьми, що робили це роками, всередині твердого правила безконтактності.
- Поважні гайди — команди на кшталт Bellingcat публікують ретельну, етичну, міжплатформну методологію, до якої варто повертатися.

Місток до Тому Третього

Ця книжка була про людей на платформах, де вони є. Том 3 — Тверді цілі — про місця, де їх *немає*: акаунт, який вони видалили й гадали, що він зник, фото без підпису, яке ти геолокуєш із того, що в кадрі, домен і інфраструктуру за операцією. Це там, де OSINT перестає бути про профілі й починає бути про світ.

Наразі ти зробив те, для чого ця книжка була. Ти можеш простежити одну людину крізь увесь інтернет — обережно, чесно й точно знаючи, де зупинитися.

Тримай нотатки. Лишайся допитливим. Лишайся добрим. Побачимося в Томі 3.

— Yehor

Додаток

Нові терміни, метод на одній сторінці й шаблони, які можна скопіювати.

А — Нові слова в цьому томі

- Шар доступу — відкриті речі *навколо* приватного профілю (спільні друзі, теги, кешовані копії), що витікають те, що сам профіль ховає. Ти також почуєш, що це називають *колом* навколо цілі, або *шарами витоку* — та сама ідея, різні назви. Ця книга використовує шар доступу як провідний термін; вважай *коло* та *шари витоку* його синонімами.
- Комболист — простий список пар email:пароль (або нікнейм:пароль), зазвичай зшитий з багатьох старих витоків і переданий по руках. Корисний лише щоб *зв'язувати* ідентифікатори, ніколи щоб входити.
- Підтвердження сходженням — як ти насправді досягаєш *підтверджено*: кілька незалежних сигналів, що вказують на ту саму людину, і ніщо не суперечить. Жодна окрема зачіпка цього не доводить; узгодження доводить. Іноді зване підтвердженням незалежними сигналами.
- Прохід спростування — навмисний крок, де ти перестаєш будувати кейс і намагаєшся його *зламати* — полюючи на той один факт, що довів би твою неправоту.

Якщо знахідка виживає, вона сильніша. Краще їй провалитися тут, ніж у звіті.

- **Дорк (пошуковий оператор)** — прицільний пошук за допомогою власних операторів рушія (site:, filetype:, лапки, мінус), щоб змусити його показати рівно те, що ти хочеш. Часто зване «google-дорк».
- **EXIF** — приховані дані, запхані всередину файлу фото камерою чи телефоном: дата, час, іноді GPS-локація й пристрій. Багато платформ їх зрізають; деякі ні. Завжди варто перевірити.
- **Сімейний ланцюг** — назва цієї книги для досягнення приватної цілі через її родичів — батька, брата/сестру чи чоловіка/дружину, чиї акаунти відкриті і хто тегає, згадує чи фотографує людину, яку ти не можеш побачити напряму.
- **FOAF** — «друг друга» (friend of a friend); досягнення цілі через людей, пов'язаних з нею.
- **Граф особи** — карта людини як вузлів (акаунти, люди) і зв'язків (те саме обличчя, спільний нікнейм, сім'я), яку ти вирощуєш, поки вона не вкаже на одну особу.
- **Незалежний сигнал** — зачіпка, чиє джерело окреме від інших твоїх зачіпок. Дві зачіпки з того самого джерела рахуються як одна.
- **Перевірка пароля на k-анонімність** — безпечний спосіб перевірити, чи пароль з'являється у відомих

витоках, ніколи не надсилаючи його цілком. Ти надсилаєш лише перші кілька символів його хешу; сервіс повертає кожен збіг для того префікса, і ти завершуєш перевірку на власній машині. Саме так працює сервіс Pwned Passwords від Have I Been Pwned.

- Граматика іменування — особистий, послідовний спосіб, яким одна людина мутує свій нікнейм (ім'я+прізвище, улюблене число, leetspeak), щоб ти міг передбачити нікнейми, яких ще не знайшов.
- Числовий ID — внутрішнє, постійне число платформи для акаунта (наприклад, Telegram user ID), що лишається тим самим, навіть коли нікнейм і показуване ім'я міняються. Тривкий якір. Важать два різновиди: *послідовні* ID (Telegram) видаються приблизно по порядку, тож менше число означає старіший акаунт — саме це дає тобі оцінити вік акаунта; *snowflake*-ID (Discord, Twitter/X) мають мітку часу створення математично вбудовану в саме число, тож ти можеш декодувати точну мить створення. ID Telegram — послідовні, не snowflake — не плутай ці два.
- Джерело сторінки (page source) — сирий HTML за вебсторінкою (правий клік → «Переглянути джерело»). Він часто тримає те, що гарна сторінка ховає: числовий ID, URL повнорозмірного зображення, справжнє ім'я, поховане в тегу. *Застереження 2026:* на багатьох великих платформах сторінка тепер просто JavaScript-оболонка,

тож ID і дані завантажуються постфактум і їх уже нема в сирому джерелі — це досі окупається на менших чи старіших сайтах і для URL зображень.

- Відбиток пароля — рідкісний, перевикористаний пароль, що з'являється на двох акаунтах, використовуваний щоб зв'язати їх (ніколи щоб входити).
- РҮМК (People You May Know, «люди, яких ви можете знати») — функція платформи з пропозиції друзів. Оскільки вона пропонує людей із прихованих зв'язків, вона може тихо розкрити, хто з ким пов'язаний — півот, якщо читати уважно.
- Резолвер (нікнейм → числовий ID) — маленький інструмент чи сервіс, що перетворює публічний нікнейм на постійний числовий ID акаунта (і назад), щоб ти міг продовжувати відстежувати когось після перейменування.
- Лог стилера проти витоку — два різні види злитих даних. Витік — це дані, вилиті з одного зламаного сервісу — користувачі одного сайту. Лог стилера — це все, що шматок шкідливого ПЗ зішкріб з одного зараженого пристрою — логіни, куки й файли багатьох сайтів від однієї жертви. Інша форма, інше значення.
- Стилومتрія (легка) — розрізнення авторів за звичками письма: формулювання, пунктуація, емодзі, час.
- Перебирач нікнеймів — інструмент, що перевіряє один нікнейм на десятках чи сотнях сайтів заразом, щоб

побачити, де він існує. Швидкий спосіб почати мережу нікнеймів (Sherlock і Maigret — приклади).

- **WHOIS** — публічний реєстраційний запис для доменного імені: хто зареєстрував, коли й через кого. Примітка: від часів GDPR більшість особистих даних відредаговано за сервісом приватності, тож WHOIS сьогодні зазвичай тонший, ніж припускають старіші посібники.

В — Стартовий набір інструментів (2026)

Ця книга навмисно майже не називає інструментів — тривкий саме метод. Але новачки раз у раз питають «так, але *що мені відкрити?*», тож ось короткий, чесний стартовий набір, згрупований за завданням. Прочитай це застереження першим: назви інструментів, власники й умови постійно міняються, і будь-що з цього може бути перейменоване, замкнене за платою чи зникле на час, коли ти це читаєш. Перевір поточний статус і законність інструмента, перш ніж на нього спиратися. Це місця, щоб *вивчити метод*, а не милиця, щоб його оминути.

- Членство у витоках — Have I Been Pwned (чи виринав акаунт чи адреса у відомому витоку); його сервіс Pwned Passwords для безпечної перевірки пароля на k-анонімність.
- Перебір нікнеймів — Sherlock, Maigret, WhatsMyName (перевір один нікнейм на багатьох сайтах разом).

- Зображення й обличчя — Yandex Images, Google Lens, TinEye для зворотного пошуку зображень. Спеціалізовані інструменти пошуку *обличч*, як-от PimEyes, існують, але вони піднімають важкі етичні й правові прапорці (біометрія під GDPR і ВІРА) — стався до них як до червоної межі, над якою треба тяжко подумати, а не як до типового вибору.
- Архівування — Wayback Machine і archive.today, обидва щоб *відновити* зниклі сторінки і щоб *зберегти* те, що ти знайшов, перш ніж воно зникне.
- Фреймворки й довідники — OSINT Framework та IntelTechniques, кураторські карти того, що існує, за категоріями.

Кожен з цих — стартова точка для способу *мислення*, який ти вже вивчив у цих розділах. Метод перший, інструменти другі — інструмент — це завжди лише швидший спосіб зробити те, що ти міг би зробити вручну.

С — Метод на одній сторінці (крос-платформно)

1. Почни з однієї зачіпки на одній платформі. 2. Коли б'єшся об стіну, обійди її — працюй з шарами доступу й колом, не із замкненими дверима. 3. Півотни ідентифікатор (нікнейм, email, обличчя, номер) по кожній платформі, якої він може дістати. 4. Склади незалежні сигнали стосом — і рахуй їх лише по одному разу кожен. 5. Дери драбину — слабкий → помірний → сильний → підтверджено. *Сильний* заробляється, коли незалежні сигнали спільно важко пояснити будь-якою суперницькою гіпотезою, а не коли вони просто нагромаджуються — рахунок це підлога, не тест. 6. Спробуй це зламати — полюй на доказ, що довів би твою неправоту, перш ніж робити висновок. 7. Записуй по ходу — скріншот, URL, дата й заархівована копія. 8. Зупинися при межі — бери лише те, що відповідає на питання; лиши приватні життя, крізь які ти пройшов, у спокої.

D — Де практикуватися (безпечно й законно)

- Розслідуй себе, по платформах — знайди кожен акаунт, тег і витік, що ведуть назад до тебе, потім прибери це.
- OSINT CTF та челенджі верифікації — збудовані для крос-платформного півоту й дисципліни доказу.
- Заходи з пошуку зниклих людей (наприклад, Trase Labs) — справжні, під наглядом, без контакту.

- Авторитетні посібники (наприклад, набір інструментів Bellingcat) — обережний, етичний метод, до якого варто повертатися.

Тобі ніколи не треба витратити ні копійки, і тобі ніколи не потрібна справжня третя ціль, щоб цього навчитися.

Е — Шаблони, які можна скопіювати

Звіт про атрибуцію. Кожна крос-платформна знахідка, яку ти комусь передаєш, вкладається в це:

```
CASE:      (one line – what this is)
DATE:      (when)
OBJECTIVE: (the single question, one sentence)

IDENTITY:  (who – name/handle, plainly)
CONFIDENCE: (rung: weak/moderate/strong/confirmed
+ the independent signals it rests on)
RULED OUT: (look-alikes checked and rejected, why)
NOT DONE:  (limits, the line you stopped at,
what you could NOT confirm)
SOURCES:   (numbered: platform + URL + date +
archived copy – include dead ends)
```

Таблиця сигналів. Заповни один рядок на зачіпку; останній стовпець — той, що має значення:

SIGNAL	VALUE	INDEPENDENT?
same handle	mossyfern	weak (common)
profile photo	matches	yes
posting hours	20:00-23:00	yes (own signal)
self-set name	"Deb"	NO (same source)

Застереження: спостережені сигнали стилю/часу з того самого міста чи сцени корельовані — згорни їх в один фактор,

зважаючи за рідкісністю, перед тим як рахувати. Спільні «години постингу» — не безкоштовний незалежний голос, якщо двоє незнайомих з тієї самої популяції поділили б їх.

Граф особи (ескіз). Вузли — це акаунти й люди; зв'язки — це те, що їх пов'язує. Вирішуй його, поки він не вкаже на одну людину:

```
TARGET (locked)
| [wall]
+--> WIFE (open) --> SISTER (open)
                        |
                        +--> family photo
                           tags TARGET's
                           2nd handle
```

F — Зафіксуй це, або цього не було

Знахідка, яку ти не можеш перепоказати, — це знахідка, яку ти не можеш захистити. Джерела зникають, профілі стають приватними, пости видаляють — часто в ту саму мить, коли вони важать. Тож для будь-чого несучого — будь-якого факту, на якому спочиває твій висновок — збережи це в мить, коли бачиш, не пізніше.

Для кожного такого джерела запиши:

- Точний URL — повне посилання, не «я знайшов це в його профілі».
- Дату й час, коли ти це бачив, за UTC — один годинник, який усі можуть звірити, без гадання про часовий пояс.

- ****Скріншот і незалежний архів**** — збережи це у Wayback Machine і в archive.today. Два архіви, щоб один прикрив інший, якщо сервіс лежить, заблокований чи згодом вичищений.
- **Хеш будь-якого файлу, який ти завантажуєш** — SHA-256 зображення, PDF чи дампу. Це відбиток: будь-хто може перехешувати файл пізніше й довести, що це рівно ті байти, які ти бачив, незмінні.
- ****Коли джерело було створене проти того, коли ти його побачив**** — пост, написаний у 2019, і прочитаний тобою у 2026 — це дві різні дати. Занотуй обидві; не давай «побаченому» маскуватися під «створене».

Тримай поточний лог джерел — один рядок на джерело, у порядку, в якому ти їх знайшов:

```
URL | seen-UTC | archive | hash | note
```

скелет — одне поле на стовпець

```
URL      blog.example/about
seen-UTC  2026-05-12T14:03Z
archive   wayback+today
hash      sha256 ab12c...
note      сторінка про
```

заповнений рядок зі справжнього лога

Один рядок на несуче джерело; заповнюй по ходу, не наприкінці.

*Якщо ти не можеш назвати щабель упевненості,
ти не завершив знахідку.*

G — Червоні лінії (одна картка)

Розсіяні по розділах, на одній сторінці. Це професійні відмови, не моральні лекції — відповіді, які ти даєш клієнту або собі, коли спокусливий хід переступає межу.

- Ніколи не набирай злитий пароль у формі входу. Паролі з корпусів витоків — це сигнал зв'язування, ніколи не ключ. Використати такий — це несанкціонований доступ. (Розділ 5)
- Ніколи не запускай пошук облич проти людей без їхньої згоди в юрисдикціях, де це в правовій сірій зоні. Збігай сцену кімнати, не обличчя. Біометричний скрапінг (GDPR, BIPA) — це червона межа, над якою треба тяжко подумати, а не типовий вибір. (Розділ 4)
- Ніколи не переслідуй родичів цілі, щоб знайти того, хто ховається заради власної безпеки. Сімейний ланцюг — це справжня техніка й справжня небезпека; коли інтерес клієнта — знайти людину, що від нього пішла, відмовся від роботи. (Розділ 6)
- Ніколи не знімай маску з анонімного джерела, протестувальника чи викривача для клієнта, чий інтерес — помста. Анонімність — це шар безпеки; зняти її для ворожого замовника — це шкода. (Розділ 3)

- Припускай, що кожен сторонній бот чи lookup-сервіс логує твій запит. Оператор бачить, про що ти спитав.

Стався до «безкоштовного розвідувального інструменту» як до пастки-приманки, поки не доведено інше. (Розділ 3)

- Ніколи не входи через удавання, обман чи соціальну інженерію. Ні фейкової особи родичу, ні виготовленої транзакції, щоб зняти маску з продавця, ні холодного DM, щоб виманити ім'я. Тільки відкриті джерела. (Розділи 1, 9)