

The Shadow Files

Том 1

Основи

YEHOR SELIN

Зміст

Перш ніж почати	3
Для кого ця книга	5
Як влаштовано The Shadow Files	7
Пролог	10
Що таке OSINT насправді	12
Правила	18
Спершу захисти себе	33
Шукай як профі	48
Нікнейми	63
Email	80
Номери телефонів	98
Твоє перше справжнє розслідування	114
Епілог	134
Додаток	136

Перш ніж почати

Ця книга — навчальний вступ до розвідки за відкритими джерелами, OSINT. Її написано для початківців і для всіх, хто хоче зрозуміти, як інформацію про людей та організації можна знаходити, перевіряти й захищати, користуючись лише тим, що вже є публічним.

Усе, що викладено на цих сторінках, тримається в межах суворих етичних і правових рамок — про них докладно в розділі 2. Закони різняться від країни до країни, і до одного пошуку можуть застосовуватися закони не однієї країни. Знай правила там, де перебуваєш, а коли не впевнений — спершу отримай дозвіл.

Тут усе вигадане

Кожне ім'я, кожен нікнейм, кожна 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.

Чому приклади показано повністю

Щоб уроки відчувалися справжніми, у прикладах використано повні, звичайні на вигляд дані замість затертих символів. Оскільки кожна деталь вигадана, ніщо тут не може

зачепити реальну людину — і водночас ти бачиш точно, як виглядає й поводить ся справжній слід.

Правило, яке стоїть вище за будь-яку техніку

Розуміння того, як люди стають відкритими, існує тут з однією метою: щоб розслідувати відповідально й краще захищати себе та інших. Користуйся тим, що вивчиш, законно, етично й обережно.

Якщо ти прийшов сюди, щоб захистити себе

Дехто відкриває цю книгу не для того, щоб когось розслідувати, а тому, що переживає, що його знайдуть — незнайомиць, колишній, переслідувач. Тобі тут раді, і ця книга — для тебе теж. Тобі не обов'язково спершу читати всім розділів: перейди одразу до Додатка D, «Поверни собі контроль», де є простий, розставлений за пріоритетами чекліст того, як зменшити власний слід, а тоді повертайся до початку, коли будеш готовий. Розуміння того, як працює відкритий слід, — це саме те, що дозволяє його перекрити.

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

Для кого ця книга

Ця книга написана для тих, хто починає з нуля.

Тобі не потрібно бути хакером. Тобі не треба писати код. Тобі не потрібні спеціальні програми чи потужний комп'ютер. Якщо ти вмієш користуватися рядком пошуку — у тебе вже є все необхідне, щоб почати.

Ця книга для тебе, якщо ти

- Цілковитий новачок, якому просто цікаво, як слідчі про все дізнаються.
- Той, хто хоче захистити себе — побачити, що незнайомиць міг би про тебе дізнатися, і зачинити ці двері.
- Майбутній аналітик чи слідчий, який хоче справжній, професійний метод із першої ж сторінки.
- Практикуючий фахівець — у HR, безпеці, журналістиці чи праві, — якому потрібен структурований, обґрунтований спосіб перевіряти людей і твердження.

Що ти зможеш робити наприкінці

Узяти одну маленьку зачіпку — нікнейм, електронну адресу, номер телефону — і крок за кроком відповідально скласти навколо неї чітку та чесну картину. Не вгадуючи. Методом.

Це і є вся обіцянка цього першого тому: фундамент, на
якому будується все інше.

Як влаштовано The Shadow Files

Серія, цей том і те, як побудовано кожен розділ.

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

- Том 1 — Фундамент. Спосіб мислення, правила та твої перші справжні навички. *(Ця книга.)*
- Том 2 — Крос-платформна атрибуція. Як стежити за людиною крізь соцмережі, месенджери, фотографії та витоки.
- Том 3 — Складні цілі. Видалені акаунти, геолокація, інфраструктура та незвичні прийоми, що дивують людей.
- Том 4 — Професіонал. Корпоративна робота, звіти, контррозслідування й перетворення навички на ремесло.

Кілька слів про межі теми, щоб ти розумів, що тримаєш у руках: цей том — про пошук і перевірку людей за слідами, які вони лишають. Полювання на *інфраструктуру* — домени, сервери, піддомени, відкриті файли, розвідку, якою живе пентестер, — це теж справжній OSINT, але це інший набір інструментів, і він чекає на Том 3. Якщо ти прийшов по розвідку активів, ти прийшов завчасно, а не помилився

дверима.

Усередині цього тому

1. Що таке OSINT насправді 2. Правила: закон, етика та межі, які ніколи не переступають 3. Спочатку захисти себе: OPSEC і сокпапет 4. Шукай як профі: оператори та дорки 5. Нікнейми: перша нитка 6. Електронна пошта: головний ключ 7. Номери телефонів: особистий якір 8. Твоє перше справжнє розслідування

Як побудовано кожен розділ

Той самий простий ритм щоразу, 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 можна стежити хід за ходом.
- Вправа — щось безпечне й законне, що ти робиш сам.
- Підсумок — три речі, які варто запам'ятати.

Одна обіцянка про інструменти

Ця серія навчає спершу методу, інструментів — потім. Сайти й застосунки приходять і зникають — деяких, названих тут, може вже не бути на момент, коли ти це

читаєш, а їхнє місце займуть нові. Це нормально. *Мислення* не змінюється ніколи. Опануй метод — і будь-який інструмент стане просто швидшим способом зробити те, що ти вже розумієш.

Пролог

Усе завжди починається з однієї дрібниці.

Нікнейм, який хтось обрав багато років тому й забув.
Світлина, викладена в добрий настрій. Номер телефону,
вписаний не в те поле. Один рядок у старому профілі.

Ніщо з цього не здається чимось значним. Саме тому воно
таке потужне.

Люди уявляють, що дізнатися про когось можна лише
таємними інструментами, або зломом, або в якомусь
темному закутку інтернету. Це не так. Майже все важливе
лежить відкрито, на видноті, залишене там звичайними
людьми, які живуть звичайним життям. Робота не про те,
щоб зламувати замки. Вона про те, щоб помічати — і знати,
що робити з поміченим.

Саме цього ремесла навчить тебе ця серія. Не трюків.
Способу бачити.

Ти навчишся брати одну маленьку, забуту дрібницю й іти за
нею — обережно, чесно, — доки вона тихо не розкаже тобі
історію. Ти також опануєш другу половину, ту, яку більшість
пропускає: скільки *ти* сам віддаєш назовні й як повернути
це собі.

Я роками займався цією роботою — у правоохоронних органах, у приватних розслідуваннях і навчаючи її професіоналів по всьому світу. І найважливіше, що я можу сказати тобі перед початком, ось що: сила бачити ясно приходить з обов'язком використовувати її гідно. Ми часто говоритимемо про цей обов'язок, бо саме він відрізняє професіонала від решти.

Кожен лишає тінь. Наприкінці цієї книги ти знатимеш, як її прочитати — і, що не менш важливо, коли відвести погляд.

Кожна тінь має ім'я. Навчімося його знаходити.

Що таке OSINT насправді

— і як мислить слідчий

Почнімо з чесної версії, без жаргону.

OSINT — це дізнаватися про людину чи річ, користуючись лише тим, що вже є відкритим. Жодного зламу. Жодного проникнення. Жодного входу в чужий акаунт. Усе, що ти коли-небудь робитимеш у цій книзі, користується дверима, які *вже відчинені*, — публічними профілями, публічними дописами, публічними реєстрами, публічними фотографіями. Ти не зломщик. Ти той, хто читає те, що всі полишили лежати на столі.

Перше, від чого треба відвикнути: тобі не потрібно бути «хакером». Тобі потрібні дві речі — готовність дивитися і спосіб мислити. Дивитися легко. Уся ця книга насправді про мислення.

Одна ідея, на якій будується все

Ось воно, усе ремесло в одному рядку:

Кожен лишає сліди. Ти починаєш з одного сліду, ідеш за ним до наступного й рухаєшся далі, доки шматочки не вкажуть на реальну людину.

Ми даємо цим трьом рухам назви, і ти чутимеш їх до кінця серії:

- 1. Відкритий слід — слід, який людина по собі лишила (нікнейм, фотографія, номер телефону, старий допис).
- 2. Півот — використання цього сліду, щоб знайти *наступний*. Одна зачіпка передає тобі іншу.
- 3. Атрибуція — коли зачіпок вишиковується достатньо і вони вказують на одну реальну особу.

Слід → півот → атрибуція. Ось і все. Кожен кейс у кожній книзі — це просто ця петля, прокручена знову й знову.

Згадай відірвану нитку на светрі. Ти не накидаєшся на весь светр. Ти знаходиш *одну* нитку й тягнеш — обережно, — і вона веде до наступної петлі, і до наступної. OSINT — це витягування ниток. Майстерність у тому, щоб знати, *яку* нитку і *наскільки сильно* тягнути.

Як насправді мислить слідчий

Чотири звички відрізняють професіонала від того, хто просто вбиває ім'я в рядок пошуку.

- Починай з однієї точки. Не «хто ця людина» — це надто велике, щоб відповісти. Натомість: «У мене є цей один нікнейм. Що він може мені дати?» Маленькі питання мають відповіді.

- Кожна відповідь — це нове питання. Знайшов електронну адресу? Добре — а *де ще живе ця адреса?* Ти ніколи не завершуєш; ти просто робиш півот до наступного питання.
- Схоже — не те саме. Два акаунти з нікнеймом «shadowfox» — це не автоматично одна людина. Це помилка, яка губить початківців. Ти не *робиш висновок* — ти *підтверджуєш*, другою й третьою незалежними зачіпками.
- Пильнуй власні бажання. Тобі *хотітиметься*, щоб зачіпка вказувала на твою ціль, — і саме це хотіння небезпечне. Тієї миті, коли ти відчуваєш упевненість, свідомо шукай факт, який довів би, що ти *помиляєшся*. Ця одна звичка врятує тебе від помилок, які гублять початківців.
- Це структурована цікавість. Не магія, не удача. Спокійний, повторюваний процес, який може опанувати будь-хто.

Крихітний приклад, щоб ти побачив петлю

Усе нижче вигадане — вигадана людина, щоб показати мислення, а не інструменти.

Тобі дають одну річ: нікнейм j.karas_88.

- Крок 1 — Відкритий слід. Ти перевіряєш, де цей точний нікнейм існує на різних платформах. Він виринає

на ігровому форумі та на старому сайті для обміну фото.

- Крок 2 — Півот. У профілі на форумі згадано місто, Riverton, і прив'язано другий нікнейм: jaykaras. Нова нитка, яку можна потягнути.
- Крок 3 — Ще один півот. Цей другий нікнейм з'являється в публічному профілі, де видно ім'я, Jason, та контактну адресу: jaykaras88@mailbox.com.
- Крок 4 — Підтверджуй, не припускай. Те саме місто на двох сайтах. Те саме фото профілю на обох. Та сама дивна манера письма («cheers all!»). Три незалежні сигнали тепер указують в один бік.
- Крок 5 — Атрибуція. Ти більше не вгадуєш. Один нікнейм став названою людиною — бо кожен крок *заслужив* наступний.

Зверни увагу, що зробило роботу. Жоден хитрий інструмент. Це зробили півоти. Інструменти лише пришвидшують кроки, які ти вже розумієш. Саме тому ця серія навчає спершу методу — інструменти змінюються щороку; петля — ніколи.

Першого разу, коли я робив це по-справжньому, я починав з одного нікнейма й поганого передчуття. Я не чекав багато чого. За годину я дивився на цілу постать людини — де вона працює, кого знає, у якому місті прокидається, — зібрану цілком зі шматочків, які вона лишила на видноті, крок за маленьким кроком. Ніхто мені нічого з цього не подав; я

просто поставив правильні маленькі питання в правильному порядку. Я ніколи не забував того відчуття. Не влади, точніше — радше тихого клацання замка, який ти не зламав, а лише зрозумів.

Одне правило, яке ніколи не згинається

Усе тут лишається на законному, публічному боці лінії — тільки відкриті джерела, нічого, на що потрібен дозвіл. Наступний розділ повністю присвячений цій лінії: де вона проходить і чому знати це робить тебе ефективнішим, а не обережнішим. Поки що досить одного: аматор питає, що ще він може дістати; профі знає, де далі — стоп.

Твоя перша справа

Розслідуй найлегшу ціль, яку ти коли-небудь матимеш, — себе.

- Запиши найстаріший нікнейм, яким ти коли-небудь користувався (той ігровий чи форумний нік із давніх років).
- Пошукай його, точно, на кількох платформах.
- Подивися, що досі існує, з чим воно пов'язане і — чесно — наскільки далеко від нього міг би зробити півот незнайомиць.

Ти навчишся двох речей одразу: як *відчувається* петля і наскільки ти вже відкритий.

Підсумок

- OSINT — це складання картини з лише публічної інформації — без зламу.
- Усе ремесло — це одна петля: слід → півот → атрибуція.
- Починай з малого, роби півот і *підтверджуй*, перш ніж робити висновок — і пам'ятай, що схоже ім'я ще не та сама людина.

Далі: правила — де проходить лінія і чому лишатися на правильному її боці робить тебе ефективнішим, а не навпаки.

РОЗДІЛ ДРУГИЙ

Правила

Закон, етика та межі, які ніколи не переступають

Почну з найзаспокійливішого, що я можу тобі сказати. Майже все, чого ти навчишся в цій книзі, — цілком законне, цілком відкрите й таке, що ти можеш робити з чистим сумлінням. Ти нікуди не вламаєшся; ти читаєш те, що вже стоїть на полиці.

Тож цей розділ не для того, щоб тебе налякати. Він — щоб дати тобі компас. Щойно ти зрозумієш кілька простих ідей, ти *відчуватимеш*, де проходить лінія, і не шукатимеш її щоразу. І ось що дивно: люди, які найкраще розуміють правила, — водночас і найсміливіші слідчі. Вони рухаються швидко, бо ніколи не хвилюються, що переступили лінію. Знання, де стіна, дозволяє добігти прямо до неї.

Покажу тобі, де ця стіна.

Яскрава лінія — дивитися чи торкатися

Є одна лінія, що важить більше за всі інші — уяви її як яскраву світну смугу, намальовану на підлозі. Усе, що ти робиш в OSINT, — або на безпечному її боці, або на неправильному, і сама лінія проста.

*Дивитися на те, що вже публічне, — це нормально.
Пробиратися в те, що замкнене, — ні.*

Простіше нікуди:

- *На безпечному боці:* читати публічний профіль, реєстрацію компанії, новинну статтю, викладену кимось фотографію, номер телефону у відкритому довіднику. Усе це на видноті. Будь-хто може це бачити. Ти — представник публіки, який дивиться на публічні речі.
- *На неправильному боці:* входити в чужий акаунт, вгадувати чи використовувати чийсь пароль, прослизати повз екран входу, потрапляти в будь-що, що мало бути приватним і захищеним.

Уяви будинок на вулиці. Тобі дозволено йти вулицею й дивитися: колір, сад, авто на під'їзді, ім'я на поштовій скриньці. Усе це публічне. Тобі *не* дозволено відчиняти вхідні двері й заходити — навіть якщо ти випадково знаєш, що ключ під килимком. Тієї миті, коли ти торкаєшся тих дверей, ти переступив лінію, хоч би як легко це було.

У світі комп'ютерів «вхідні двері» — це будь-що з паролем, входом чи замком. Якщо крок вимагає, щоб ти *увійшов як хтось інший* або *обійшов засіб захисту*, зупинися: ти досяг яскравої лінії.

Є навіть закони з іменами, прив'язані до цієї ідеї. У США це *CFAA* — Computer Fraud and Abuse Act. Завчати його не

треба, потрібна лише суть в одному реченні: використати знайдений пароль, щоб увійти в акаунт, який тобі не належить, — це «несанкціонований доступ», і це злочин. Прочитати, що акаунт *існує*, — нормально. Відкрити його — ні.

Публічне не завжди означає «можна все»

Ось де початківці спотикаються, тож пригальмуймо на секунду.

«Якщо воно публічне, я можу робити з ним що завгодно.»
Це здається правдою. Це не так. Щось може бути *на видноті* й усе одно заслуговувати на *повагу*.

Публічне дає тобі дозвіл дивитися. Воно не вручає тобі дозволу робити що завгодно.

Приклад робить це очевидним. Хтось викладає фотографію в невеликій групі підтримки для людей, які одужують від хвороби. Технічно ти можеш її знайти. Але людина поділилася нею в маленькому, тихому закутку інтернету, розраховуючи на маленьку, тиху аудиторію. Якщо ти вирвеш її з того закутка й вставиш у звіт, ти зробив те, що *законно бачити*, але *неправильно так використовувати*. Ти порушив обіцянку, яку дало їй те середовище.

У професіоналів є правило для цього, і воно прекрасне у своїй простоті: *поважай початковий контекст*. Спитай себе:

«Чому ця людина цим поділилася і де?» Весільна фотографія, показана всьому світу, — це інше, ніж лікарняне оновлення, показане жменьці друзів. Слова публічні в обох випадках. *Дух* — ні.

Є також ціла родина законів про приватність — у Європі головний називається *GDPR* (це General Data Protection Regulation, але назва не має значення). Знову ж таки, одна проста ідея: навіть публічну інформацію про реальну, живу людину треба обробляти з поважної причини, зберігати лише стільки, скільки потрібно, і не накопичувати «про всяк випадок». Ти не збираєш гору деталей про людину лише тому, що *можеш*. Ти збираєш те, що тобі справді потрібно для справжнього питання, на яке ти відповідаєш. Це називають *мінімізацією даних*, і це просто хороші манери з красивою назвою — бери тільки те, що є у твоєму списку.

Згода, приватність і людина на тому кінці

За кожною електронною адресою, кожним нікнеймом, кожним розмитим фото профілю стоїть людина. Справжня. Із родиною, іноді поганим днем, почуттями, життям. Я хочу, щоб ти тримав цю людину в кімнаті поруч із собою весь час, поки працюєш.

Ця єдина звичка вбереже тебе від халепи більше, ніж будь-який закон. Бо більшість хибних поворотів у OSINT

приходять не від незнання правил. Вони приходять від забування, що «ціль» — це людина.

Тож кілька м'яких стандартів:

- Май *причину*. Перш ніж когось шукати, зумій сказати навіщо. «Мені цікаво» і «Я хочу зібрати досьє на колишнього» — це не причини, це червоні прапорці. Хороша причина прив'язана до справжнього, чесного завдання.
- Не *вдавай когось іншого*, щоб отримати інформацію. Здобувати доступ до даних брехнею — наприклад, кажучи компанії, що ти роботодавець цієї людини, — називається *претекстингом*, і це заборонено. Питай прямо або не питай зовсім.
- Не *контактуй і не обманюй* людину, яку розслідуєш. Жодних фальшивих запитів у друзі, щоб обійти її налаштування приватності. Жодного улепшування, щоб вона щось розкрила.

Ніщо з цього не робить тебе слабким слідчим. Це робить тебе *тим, кому довіряють*. А в цій сфері бути тим, кому довіряють, — це вся кар'єра.

Коли ти робиш це за роботою — діють додаткові правила

Усе досі стосувалося кожного. Але тієї миті, коли ти робиш OSINT для *організації* — перевіряєш кандидата на посаду,

працівника, партнера, — вмикається другий шар правил, і їх порушення може бути окремою халепою, навіть коли кожне джерело було публічним. Тобі не треба бути юристом. Тобі треба знати, що ці розтяжки існують, і залучати людей, які ними опікуються.

- У найму свої закони. У Сполучених Штатах використання довідкової інформації для рішення про найм може підвести тебе під *FCRA* (Fair Credit Reporting Act) — із правилами про дозвіл і про те, щоб повідомити людину, перш ніж діяти на основі знайденого. А антидискримінаційне право (правила *EEOC*) означає, що якщо твій пошук виявляє чиясь релігію, здоров'я, вагітність, вік тощо, і рішення потім обертається проти неї, компанію можуть звинуватити в дискримінації. Безпечна звичка: записуй лише релевантні для роботи, перевірені факти — а не все, що тобі випало побачити.
- Розслідування власних людей потребує задокументованої причини. Регульовані робочі місця не можуть просто перевіряти працівника «бо так». Має бути законна, письмова мета, і часто HR чи юристи мають бути залучені *спершу*. Закони про приватність на кшталт GDPR ставляться до даних працівників з особливою обережністю. Коли сумніваєшся, отримай дозвіл до того, як почати, а не після.
- Обличчя й біометрія — особливі. У деяких місцях є окремі закони про збір чи зіставлення чийогось обличчя

або інших біометричних даних без згоди. Стався до пошуку за обличчям як до інструмента підвищеної обережності (ми повернемося до цього пізніше) і ніколи не запускай його на людях за роботою без юридичної перевірки.

Ніщо з цього не для того, щоб тебе відлякати. Це для того, щоб того дня, коли твоя хобі-навичка знадобиться на роботі, ти вже знав зупинитися й спитати: «Чи є додаткове правило, бо це для роботодавця?» Відповідь часто «так».

Особливий випадок: дані брешів і витоків

Ти багато чутимеш про *бреші* та *витоки*. Визначмо їх просто. Бреш — це коли компанію зламують і інформація її користувачів виливається назовні — іноді разом із паролями. Витік — це та вилита інформація, що плаває довкола потім. В інтернеті є величезні зібрання цього добра.

Це нервує людей, і з цим треба поводитися обережно. Але є законний, корисний, професійний спосіб працювати з цим — і є спосіб, який робить тебе злочинцем. Різниця — знову ж таки одна чиста лінія.

Ти можеш перевірити, чи щось було відкрито. Ти ніколи не можеш використати вкрадений пароль, щоб увійти.

Ось безпечний спосіб про це думати:

- Перевіряти відкритий слід — нормально. Є поважні сервіси, що дозволяють ввести електронну адресу й дізнатися: «Так, ця адреса з'явилася в такому-то бреші 2019 року.» Це *факт про відкритий слід*. Це як прочитати, що в магазині сталося пограбування. Корисно, чесно, дозволено. (Найвідоміший сервіс для цього навіть відмовляється видавати тобі паролі — він лише каже тобі, *що* тебе було відкрито, і робить це навмисно.)
- Використовувати крадене — ні. Узяти злитий пароль і ввести його в чиюсь пошту, щоб побачити, чи він досі працює, — це прохід крізь вхідні двері. Це несанкціонований доступ. Це злочин. Не має значення, що пароль «просто там лежав».

Професіонали інколи використовують злитий пароль одним дуже конкретним, хитрим, *безпечним* способом: як *відбиток*. Якщо той самий точний незвичайний пароль з'являється прив'язаним до двох різних акаунтів, це сильний натяк, що обидва акаунти належать одній людині. Зверни увагу, що тут сталося — пароль використали, щоб *з'єднати крапки*, ніколи щоб *відімкнути двері*. У цьому вся гра. Використовуй ідентифікатори, щоб розуміти й пов'язувати. Ніколи — щоб увійти.

І ще одна нотатка про чесність щодо даних витоків: вони часто старі, безладні або відверто хибні. Пароль із 2016 року розповідає тобі про минуле, а не про сьогодні. Ніколи не

сприймай це добро як істину в останній інстанції. Перевіряй його за другим джерелом, перш ніж вірити.

Як лишатися на правильному боці — простий метод

Ось процедура, яку можна проганяти перед кожним пошуком. Вона займає тридцять секунд і триматиме тебе чистим усю кар'єру.

- Запиши свою причину. Одне чесне речення: «Я перевіряю цей бізнес перед підписанням контракту з ним.» Якщо ти не можеш написати це речення — не роби пошук.
- Спитай: я дивлюся чи торкаюся? Якщо будь-який крок потребує пароля, входу чи обходу замка — зупинися. Крапка. Знайди інший, відкритий шлях або не йди туди.
- Спитай: чого ця людина очікувала? Поважай початковий контекст. Публічний допис усьому світу — чесна гра. Приватний закуток — ні, навіть якщо ти можеш до нього дотягтися.
- Бери тільки те, що потрібно. Не висмоктуй усе життя людини. Збери кілька фактів, що відповідають на твоє справжнє питання. Решту пропусти.
- Ніколи не вдавай, не обманюй, не контактуй під фальшивою личиною. Жодної брехні заради даних. Жодних фейкових акаунтів, щоб заприятелювати з

об'єктом.

- Веди чесні нотатки по ходу. Збережи посилання, збережи дату, збережи те, що бачив, — точно як бачив. (Про це трохи згодом.)
- Перевіряй усе важливе двічі. Одне джерело — це чутка. Два незалежні джерела починають бути фактом.

Проженеш ці сім перевірок — і ти майже ніколи не ступиш не туди.

Як тримати нотатки чесними

Тут варто затриматися, бо саме на нотатках хороші слідчі відділяються від недбалих — і це теж частина того, щоб лишатися в межах закону. (Механіку — як саме вести файл справи — ми розберемо в розділі 3; тут важлива одна річ, юридична.)

Коли ти щось знаходиш, запиши, *де, коли і що воно насправді казало* — не те, що ти хотів би, щоб воно казало. Скріншот, точна веб-адреса, дата. І тримай факт окремо від твоєї *думки про факт*.

Чому це так важливо? Захист. Якщо твою роботу коли-небудь поставлять під сумнів — а одного дня це може статися, — твої чесні, датовані, підкріплені джерелами нотатки стануть щитом. Вони показують, що ти дивився на публічні речі, публічним способом, із справжньої причини. Це різниця між «я з'ясував це як належить» і «повідь на

слово». Завжди май змогу довести перше.

Коротка історія: де початківець зісковзує, а профі зупиняється

Пройдімо ситуацію, схожу на справжню. Усе й усі тут вигадані, але вибір — справжній. Слідкуй за мисленням.

Тебе попросили перевірити невеликого постачальника, перш ніж твоя компанія укладе з ним угоду. Контактну особу звати Daniela Voss, а її електронна адреса — daniela.voss@brightfield-supplies.com. Ось як це розгортається.

- Крок 1 — Відкритий погляд. Ти шукаєш назву компанії й знаходиш їхній сайт, дату реєстрації та кілька згадок у новинах. Усе публічне, усе чесне. Ти занотовуєш джерело й дату для кожного. Добре — ти твердо на безпечному боці.
- Крок 2 — Перевірка відкритого сліду. Ти проганяєш адресу Daniela через поважний сервіс перевірки брешів. Він каже тобі, що її адреса з'явилася у витоку два роки тому. Це *факт про відкритий слід*. Ти записуєш: «адресу відкрито у [назва витоку], 2024.» Досі безпечно. Ти дізнався лише *те*, що її було відкрито, а не щось таємне.
- Крок 3 — Спокуса. Той самий витік плаває онлайн, і він містить паролі. Початківець думає: «Я міг би просто перевірити, чи її старий пароль досі впускає в її пошту. Це

б стільки мені сказало.» Ось ця мить. Це вхідні двері з ключем під килимком.

- Крок 4 — Де профі зупиняється. Професіонал навіть не тягнеться до ручки дверей. Вхід із тим паролем був би несанкціонованим доступом — злочином — і отруїв би всю роботу. Навіть якби ти щось знайшов, це було б непридатне й незаконне. Тож ти зупиняєшся, занотовуєш відкритий слід як *факт* і рухаєшся далі — без драми.

- Крок 5 — Чисте завершення. Замість цього ти продовжуєш працювати *відкритими* слідами: звіряєш реєстрацію компанії з офіційним публічним реєстром, шукаєш публічні відгуки та судові записи, підтверджуєш усе тривожне другим джерелом. Тоді пишеш спокійний, чесний звіт: факти в одній колонці, твоя оцінка — в іншій, кожне твердження датоване й підкріплене джерелом.

Те, що ти лишився в межах закону, у жодну мить не зробило тебе *менш* ефективним. Воно зробило твою роботу *сильнішою*, бо все у твоєму звіті може витримати денне світло.

Спосіб мислення: профі знає, де зупинитися

Я хочу лишити тобі єдину ідею, що зв'яже весь цей розділ до купи.

Початківець питає: «Чи можу я це дістати?»

Професіонал питає: «Чи варто, і як далеко я

заходжу?»

Знати, де зупинитися, — це не обмеження твоєї майстерності. Це *і є* майстерність. Безрозсудним може бути будь-хто. Треба справжній професіонал, щоб потужно рухатися крізь публічну інформацію, а тоді, точно в потрібну мить, засунути руки в кишені й відступити від замкнених дверей.

Ця стриманість — те, що змушує людей довіряти тобі серйозну роботу. Це те, що дозволяє тобі добре спати. І це те, що робить тебе *хорошим* — не просто здатним, а хорошим у повному сенсі слова.

Я досі пам'ятаю той перший раз, коли слід повів туди, де мені було нічого робити. Питання, яке мені поставили, було маленьким і чесним. Але шлях усе відкривався далі — дім, родина, щоденний розпорядок, — і я відчував, як легко було б зробити наступний крок. Я закрив справу. Не тому, що не міг зробити той крок, а тому, що зробити його означало б перетворити чесний запит на стеження за чийось життям. Відступити відчувалося як програш. Це була найпрофесійніша річ, яку я зробив за весь той рік.

Тепер у тебе є компас. Решта цієї книги — про те, як навчитися ходити. Почнімо.

Вправа

Безпечна, законна вправа, щоб зробити яскраву лінію відчутною.

- Обери *велику публічну компанію*, яку ти вже знаєш, — відомий бренд, а не приватну особу. Компанії — публічні суб'єкти, тож це тримає тебе далеко від будь-яких питань приватності.
- Проведи п'ятнадцять хвилин, збираючи лише *публічні* факти: коли її засновано, де її штаб-квартира, її офіційний сайт, одну-дві свіжі новини. Для кожного пункту запиши точну веб-адресу й дату, коли ти дивився.
- Тепер напиши два короткі списки поруч. Ліворуч: «Факти, які я знайшов.» Праворуч: «Моя думка про те, що вони означають.» Тримай їх суворо нарізно. Відчуй, наскільки різні ці дві колонки.
- Насамкінець напиши одне чесне речення вгорі сторінки: твою *причину* дивитися. Практикуй звичку ніколи не починати без неї.

Ти щойно проганяв весь метод — спершу причина, тільки публічне, чесні підкріплені джерелами нотатки, факти нарізно з думкою — на цілі, де ти ніяк не можеш завдати шкоди. Саме так профі й розігріваються.

Підсумок

- Яскрава лінія — це дивитися чи торкатися. Читати те, що публічне, — нормально; входити в будь-що замкнене

чи використовувати вкрадений пароль — заборонено завжди.

- Публічне не означає «можна все». Поважай, чому і де чимось поділилися, бери тільки те, що потрібно, і пам'ятай, що на тому кінці — реальна людина.
- Профі знає, де зупинитися. Веди чесні, датовані, підкріплені джерелами нотатки, перевіряй важливі речі двічі й стався до зупинки перед замкненими дверима як до навички — бо це саме та навичка, що робить тебе тим, кому довіряють.

РОЗДІЛ ТРЕТІЙ

Спершу захисти себе

OPSEC і сокпанет

Дозволь почати з невеличкого зізнання. Найпершого разу, коли я шукав когось в інтернеті, я зробив це неправильно.

Я користувався власним акаунтом. Своїм справжнім іменем. Своїм справжнім фото. Я відкрив профіль людини, покопирсався там і відчув себе розумником. А потім, за кілька днів, ця людина з'явилася в моєму списку «Люди, яких ви можете знати». Платформа тихенько помітила, що я раз по раз переглядаю цей профіль. Вона запропонувала нас одне одному. Моє прикриття — таке, яке було, — зникло раніше, ніж я взагалі усвідомив, що мені є що втрачати.

Того разу ніхто не постраждав. Але це навчило мене найважливішого уроку цієї книги, і я хочу дати його тобі, перш ніж переходити до всього іншого.

Перш ніж дивитися на будь-кого, захисти себе.
Розслідування — це другий крок. Безпека —
перший.

Цей розділ про OPSEC. Це слово прийшло з військової сфери. Воно означає *операційну безпеку* — гарний спосіб сказати «не залишай слідів, які ведуть назад до тебе». Для

нас воно означає одну просту річ: ти можеш дивитися на відкритий інтернет так, щоб відкритий інтернет не дивився на тебе.

Я триматиму кожную думку простою і покажу тобі налаштування, яке ти зможеш зібрати на звичайному ноутбучі вже сьогодні по обіді. Ніяких шпигунських гаджетів. Ніяких витрат, окрім хіба що вартості чашки кави.

Чому ти ніколи не розслідуєш зі своїх власних акаунтів

Головна ідея — скажи її вголос, якщо це допоможе.

Твої справжні акаунти прив'язані до твого справжнього життя. Тієї миті, коли ти скористаєшся ними, щоб подивитися, ти ризикуєш показати своє обличчя тому, на кого дивишся.

Сучасні платформи — Facebook, Instagram, LinkedIn, TikTok, усі вони — стежать за *твоєю* поведінкою не менше, ніж за поведінкою всіх інших. Коли ти переглядаєш профіль знову і знову, платформа це помічає. Вона може запропонувати тебе й ту людину одне одному. У LinkedIn людина часто може побачити *точно*, хто її переглядав. Один необережний клік — і твоє ім'я потрапляє в її сповіщення.

Є й друга небезпека, тихіша, але така ж реальна. Твій власний акаунт повний *тебе*. Твоїх друзів. Твоїх фото. Твого місця роботи. Твоїх звичок. Якщо людина, яку ти досліджуєш, бодай трохи цікава чи трохи небезпечна, твій акаунт — це карта прямо до твоїх дверей. В OSINT людина, яку ти вивчаєш, іноді може вивчати тебе у відповідь. Ніколи не давай їй карту.

Тож ми будуємо стіну між «тобою-людиною» і «тобою-дослідником». Ця стіна називається сокпапет.

Що таке сокпапет (і чим він не є)

Сокпапет — це чистий, суто дослідницький (фейковий) акаунт. Уяви його як робочу рукавицю. Ти надягаєш її, щоб брати речі, до яких не хочеш торкатися голою рукою. Він не має жодного зв'язку з твоїм справжнім іменем, справжнім email, справжнім фото чи справжнім телефоном. Він існує заради однієї роботи: дивитися, тихо.

Назва походить від старого фокусу: надіти на руку шкарпетку й удавати, що це інший персонаж. Та сама ідея. Це окреме обличчя, яке ти надягаєш для досліджень.

Тепер дуже чітко про те, чим сокпапет не є, бо саме тут новачки потрапляють у халепу.

- Він не для того, щоб хитрощами змусити людей заговорити з тобою. Ми не пишемо об'єкту. Ми не

додаємо його в друзі. Ми не вступаємо непрохано в його приватні групи. Це перехід від *спостереження* до *взаємодії*, а взаємодія — це там, де етика й закон стають серйозними.

- Він не фейкова особистість для шахрайства, кетфішингу чи цькування. Ніколи. Якщо мета в цьому — закрий цю книгу.
- Він не чарівний плащ-невидимка. Він приховує твоє ім'я. Але сам собою він не приховує ні твого місцезнаходження, ні твого комп'ютера. Це ми полагодимо окремо.

Найкращі сокпапети в етичному OSINT дотримуються того, що слідчі у справах про зниклих людей називають правилом «не торкатися»: тільки спостерігати. Ніяких лайків. Ніяких коментарів. Ніяких запитів у друзі. Ніяких спроб скинути пароль. Ти муха на публічній стіні, не більше.

Сокпапет — це суто дослідницький акаунт для спостереження за відкритою мережею — ніколи для того, щоб зв'язуватися з кимось, обманювати чи взаємодіяти.

Будуємо безпечне налаштування, крок за кроком
Зберемо все це. Я піду по порядку. Зроби це один раз,
збережи — і матимеш чистий дослідницький набір
назавжди.

- Крок 1 — Створи окремий профіль браузера. Тобі не потрібен другий комп'ютер. Більшість браузерів (Firefox, Chrome, Brave) дозволяють створити свіжий профіль — цілком окремий простір браузера зі своєю історією, куками й логінами. Створи такий і назви його чимось нудним на кшталт «Дослідження». Ніколи не відкривай у ньому свої особисті акаунти й ніколи не відкривай свої дослідницькі акаунти поза ним. Ця одна звичка робить більшу частину важкої роботи.

- Крок 2 — Трохи зміцни цей браузер. У дослідницькому профілі вимкни телеметрію (коли браузер «дзвонить додому», повідомляючи, що ти робиш). Заблокуй сторонні куки. Встанови хороший блокувальник реклами й трекерів, як-от uBlock Origin. Це безкоштовно, займає п'ять хвилин і зупиняє більшість невидимого стеження, яке ходить за людьми по мережі. (Назви інструментів із роками змінюються — *ідея* полягає в тому, щоб «блокувати трекери, вбивати міжсайтові куки». Обери будь-який авторитетний інструмент, що це робить, коли читатимеш ці рядки.)

- Крок 3 — Зрозумій, що зливає браузер. Навіть із увімкненим блокувальником твій браузер тихо показує чимало: твою операційну систему, розмір екрана, шрифти, графічний чип. Разом вони утворюють відбиток — візерунок, майже такий же унікальний, як справжній відбиток пальця. VPN цього *не* приховує (про VPN трохи

згодом). Тобі не треба ставати експертом сьогодні. Просто знай, що воно існує, і тримай усі свої дослідження в цьому одному профілі браузера, щоб твоє «дослідницьке я» завжди виглядало однаково. Тут послідовність безпечніша за хаос.

- Крок 4 — Створи цілком нову пошту. Заведи свіжу поштову скриньку (Gmail, Proton, Outlook — будь-яку авторитетну). Використовуй її *ні для чого*, крім досліджень. Ця пошта ніколи не повинна торкатися твого справжнього імені, справжнього телефона відновлення чи справжніх акаунтів. Це корінь твого сокпапет. Стався до неї як до ключа від усього, бо вона ним і є.

- Крок 5 — Спочатку продумай персону на папері. Перш ніж створювати будь-який соціальний акаунт, виріши, ким цей сокпапет є. Правдоподібне ім'я. Вік. Місто. Нудна робота. Пара невинних захоплень. Запиши це й тримай послідовно. Інструмент, що генерує випадкові, але реалістичні особистості, може дати тобі старт. Мета — *непримітний і звичайний*, той, на кого ніхто не гляне двічі.

- Крок 6 — Розберися з підтвердженням телефона чесно. Деякі платформи вимагають номер телефона для реєстрації. Не використовуй свій особистий номер — це миттєво прив'яже сокпапет до тебе. Якщо ти робитимеш це регулярно, дешева окрема дослідницька SIM (одноразовий номер, який тримається лише для цього) —

це чиста відповідь. Безкоштовні інтернет-номери часто відхиляють, тож справжня SIM економить нерви.

- Крок 7 — Обирай фото профілю обережно. Ніколи не бери стокове фото чи знаменитість — швидкий зворотний пошук за зображенням спалить тебе за секунди. Багато людей використовують згенероване ШІ обличчя, але спершу обріж його й зітри приховані дані (метадані) з файлу, бо ці дані можуть тихо видати, де й як було зроблено зображення. Чесно кажучи, для чистого пасивного спостереження часто цілком нормально взагалі без фото.

- Крок 8 — «Витримай» акаунт, перш ніж ним користуватися. Цілком новий акаунт — це червоний прапорець і для платформ, і для людей. Заходь у нього протягом кількох днів. Підпиши на кілька нейтральних сторінок — спортивну команду, новинний сайт, кулінарну групу. Нехай він виглядає обжитим. Тоді, і тільки тоді, підходь до свого справжнього дослідження. Нові акаунти швидко блокують; розігрітий виживає.

- Крок 9 — Ніколи нічого не змішуй. Це золота нитка через усе це. Одна пошта на один сокпапет. Один телефон на один сокпапет. Ніколи не використовуй повторно фото, пароль чи навіть улюблений зворот мови між сокпапетами або зі своїм справжнім я. Повторне використання — це те, як дослідників зв'язують — одне з одним і назад до справжнього імені. Тримай усе на

окремих смугах.

Ось увесь набір: окремий профіль браузера, заблоковані трекери, свіжа пошта, продумана персона, чистий телефон за потреби, обережне фото і розігрітий акаунт. На звичайному ноутбукі. Сьогодні.

Що робить VPN — і чесна суперечка навколо нього

Ти всюди в цьому світі чутимеш слово VPN, тож дозволь мені зробити його простим.

VPN (віртуальна приватна мережа) приховує твою справжню інтернет-адресу — твою IP-адресу, яка приблизно є зворотною адресою, яку твоє з'єднання ставить на всьому, що ти робиш. Без VPN сайт, який ти відвідуєш, бачить адресу, що вказує на твоє рідне місто і твого інтернет-провайдера. З VPN сайт бачить натомість адресу VPN. Це наче надіслати листа через пересилковий офіс, щоб ніхто не прочитав назви твоєї домашньої вулиці.

Кілька простих правил:

- Використовуй платний, авторитетний VPN без логів. «Без логів» означає, що вони не зберігають записів про те, що ти робив. Безкоштовні VPN заробляють, продаючи твої дані — саме те, що ти намагаєшся захистити. Оминай їх.

- VPN приховує твою адресу, а не твій відбиток. Це один шар, а не вся стіна. Ось чому ми морочилися з профілем браузера.

А тепер чесна частина. Досвідчені дослідники *не погоджуються* між собою щодо VPN, і я хочу, щоб ти почув обидві сторони, а не гасло.

Один табір каже: завжди використовуй VPN. Самої лише чистої адреси недостатньо проти зняття відбитків і геопідказок, тож тримай його ввімкненим для всього.

Другий табір каже: вимикай VPN на ту одну мить, коли створюєш акаунт. Чому? Бо деякі платформи розпізнають адреси VPN і ставляться до них як до підозрілих *під час реєстрації* — вони підкидають головоломки, вимагають номер телефона або відразу банять новий акаунт.

Обидва табори праві, залежно від контексту. Ось як я примирюю це простими словами:

Використовуй свій VPN для повсякденного перегляду й збору. Але для делікатної миті створення сокпапета на прискіпливій платформі чисте, звичайне на вигляд домашнє з'єднання часто працює краще, ніж адреса VPN, якій платформа не довіряє.

Не запам'ятовуй правило. Зрозумій компроміс: VPN захищає тебе, але *позначена* адреса VPN може вбити твій новий акаунт з першого погляду. Оцінюй кожну мить.

Як чесно зберігати докази

Знайти щось — це лише половина роботи. Якщо ти не можеш *довести*, що знайшов, і довести, що не підробив цього, воно з тим самим успіхом могло б і не існувати. Це вдвічі важливіше, якщо твоя робота колись може опинитися у звіті, у спорі чи в суді.

Дружня до новачка версія того, як робити це правильно:

- Захоплюй усю сторінку, а не крихітний фрагмент. Зберігай повну сторінку з видимою вебадресою (URL) і датою на екрані. Самотній обрізаний скриншот без контексту легко відкинути.
- Записуй коли і де. Точну дату й час, коли ти це побачив, URL і як ти туди потрапив (що шукав, на якій платформі). «Я знайшов це десь у Facebook» нічого не варте. «Переглянуто за цим URL цієї дати о цій годині» — це надійно.
- Зберігай, а не просто дивися. Контент видаляють. Збережи сторінку і подумай про використання публічного вебархіву, щоб існувала незалежна, датована копія, яку ти не контролював.

- Тримай оригінал недоторканим. Не обрізай, не освітлюй і не «прибирай» збережені докази. Якщо тобі потрібна відредагована версія для звіту, збережи й недоторканий оригінал теж, і зазнач, що ти редагував копію.
- Зберігай і промахи так само, як влучання. Якщо ти шукав і не знайшов *нічого* — запиши й це. Це доводить, що ти шукав, і не дає тобі втоптувати ту саму землю знову.

Коли зростатимеш, є належні інструменти, які захоплюють сторінки автоматично й ставлять на кожну захищену від підробки печатку та довірену позначку часу — щоб ніхто не міг звинуватити тебе в тому, що ти потім тихенько змінив скриншот. У перший день вони тобі не потрібні. А от звички, наведені вище, тобі *потрібні* з найпершого пошуку.

Прості нотатки, щоб ти ніколи не загубив нитку

Розслідування — це ланцюг маленьких відкриттів, і загубити своє місце в ньому напрочуд легко. Нотатки — це те, як ти тримаєш нитку.

Я засвоїв це важким шляхом — не роблячи цього. Якось я заглибився в справу з висновком, у якому був упевнений, і без жодного спогаду про те, як я до нього дійшов. Я не міг відтворити ані кроку, тож мусив викинути все і починати спочатку. Знахідка, крізь яку ти не можеш провести когось іншого, — це не знахідка, це відчуття. Відтоді я записую

кожен клік, по порядку, перш ніж дозволити собі бодай у щось повірити.

Тримай усе гранично просто. Один файл нотаток на одну справу. Для кожної знахідки занотуй чотири речі: що ти знайшов, де (URL чи джерело), коли ти це знайшов і як (пошук чи інструмент). І тримай один рядок священним:

Відділяй те, що ти побачив, від того, що ти думаєш, що це означає. Факти в одному стовпці, твої здогади — в іншому. Ніколи не давай їм змішатися.

Ця остання звичка — різниця між професіоналом і тим, хто дурить сам себе. «У його профілі вказано Київ» — це факт. «Отже, він, мабуть, живе в Києві» — це здогад. Пиши обидва, але ніколи їх не плутай. Також записуй свої глухі кути й причини, з яких ти покинув слід — майбутнє-ти подякує теперішньому-тобі.

Помилка новачка і як її виправити

Ось коротка, вигадана історія, яка могла б статися з будь-ким.

Знайомтеся: Дарія Коваленко, новачок, допитлива й завзята. Подруга просить її перевірити, чи можна довіряти продавцю на маркетплейсі на ім'я Роман Петренко.

- Крок 1 — Помилка. Дарія відкриває Instagram у своєму звичайному браузері, залогінена як своє справжнє я, і переглядає профіль Романа. Двічі. Вона також клікає на посилання, яке він опублікував, і воно завантажує сторінку, що тихо записує відвідувачів. Вона почувається продуктивною.
- Крок 2 — Викриття. Наступного дня акаунт Романа з'являється як запропонований друг для Дарії — а її для нього. Оскільки вона була залогінена як вона сама, її справжнє ім'я й фото були тим «відвідувачем», якого платформа прив'язала до цих переглядів профілю. Тепер Роман знає, що жінка на ім'я Дарія Коваленко за ним стежить. Її справжнє обличчя. Її справжній список друзів, за один клік.
- Крок 3 — виправлення, частина перша. Дарія зупиняється. Вона створює окремий профіль браузера «Дослідження» й ніколи не торкається в ньому своїх особистих акаунтів. Вона встановлює блокувальник трекерів. Відтепер її спостереження і її справжнє життя живуть у різних кімнатах.
- Крок 4 — виправлення, частина друга. Вона заводить свіжу пошту, вигадує просту, нудну персону на ім'я Олена Марчук і будує легкий акаунт-сокпапет. Вона розігрує його кілька днів нейтральними підписками. Для перегляду вона тримає VPN увімкненим.

- Крок 5 — Виправлення, частина третя. Тепер вона переглядає публічний профіль Романа через сокпапет, у дослідницькому браузері. Вона зберігає повну сторінку з URL і датою, занотовує, що вона знайшла проти того, що вона підозрює, і — головне — ніколи йому не пише. Тільки спостерігати.

Те саме завдання. Той самий ноутбук. Різниця в стіні між Дарією-людиною і очима, які дивляться. Ця стіна — і є весь цей розділ.

Вправа

Збери свій набір, перш ніж він тобі знадобиться. Це має зайняти менше години й не коштує нічого, окрім свіжої пошти.

1. Створи окремий профіль браузера лише для досліджень. Назви його просто.
2. У ньому встанови авторитетний блокувальник трекерів і вимкни телеметрію та сторонні куки.
3. Створи цілком нову пошту, яка ніколи не торкалася твоєї справжньої особи.
4. На папері продумай одну звичайну персону: ім'я, вік, місто, нудну роботу, два невинних захоплення. Тримай її непримітною.
5. Відвідай тестову сторінку «що видає мій браузер» і просто *прочитай*, що зливає твій дослідницький браузер. Поки що нічого не виправляй — просто подивися, щоб ідея відбитка стала відчутною.
6. Відкрий простий файл нотаток і потренуйся занотовувати одну нешкідливу, публічну річ

(скажімо, години роботи музею), використовуючи чотири поля: що, де, коли, як — і додай один рядок, що відділяє факт від здогаду.

Тепер ти збудував стіну й записник. Усе інше в цій книзі стоїть на них.

Підсумок

- Безпека передусім, завжди. Ніколи не розслідуй зі своїх власних акаунтів — збудуй стіну між тобою-людиною і тобою-дослідником за допомогою окремого профілю браузера й суто дослідницького сокпапета.
- Сокпапет — щоб спостерігати, а не торкатися. Свіжа пошта, проста персона, чистий телефон за потреби, обережне фото, розігрітий акаунт — і ніколи нічого не використовуй повторно між сокпапетами чи зі своїм справжнім я.
- Працюй чесно й тримай нитку. Використовуй авторитетний VPN (але розумій суперечку про реєстрацію), зберігай докази повною сторінкою з URL і датою, тримай оригінали недоторканими й веді прості нотатки, що відділяють те, що ти *побачив*, від того, що ти *думаєш*.

РОЗДІЛ ЧЕТВЕРТИЙ

Шукай як профі

Оператори і дорки

Більшість людей шукають погано. Це не образа. Це просто правда, і я включаю сюди себе молодшого. Ми вбиваємо кілька слів у рядок пошуку, кидаємо погляд на першу сторінку і здаємося, якщо відповідь не дивиться на нас у відповідь. Пошуковик зробив саме те, про що ми попросили. Ми просто поставили розпливчате питання, тож отримали розпливчасту відповідь.

Цей розділ це виправляє. До кінця його ти шукатимеш свідомо. Ти казатимеш пошуковику точно, чого хочеш, і, що не менш важливо, чого ти *не* хочеш. Ти вивчиш невеликий набір команд — ми називаємо їх **операторами** — які перетворюють широкий, хаотичний пошук на вузький і гострий. І ти вивчиш «доркінг», слово, яке звучить загадково, але таким не є. Воно просто означає уважний пошук.

Усе тут законне й відкрите — публічні пошуковики, вжиті так, як їх задумали. Лише навичка, без трюків.

Одна велика ідея: точність перемагає обсяг

Ось помилка, якої припускається майже кожен. Люди думають, що більше результатів — краще. Вони думають, що пошук, який повертає два мільйони сторінок, — це успіх.

Усе навпаки. Два мільйони результатів означають, що пошуковик тебе не зрозумів. Він скинув усе бодай віддалено пов'язане в купу й залишив тебе копати. Чудовий пошук часто повертає *п'ять* результатів — і відповідь у першому з них.

Твоя мета — не більше результатів. Твоя мета — правильні результати.

Уяви це як рибалку. Новачок тягне величезну сітку через увесь океан і виловлює здебільшого водорості. Професіонал знає точне місце, точну наживку, точну глибину — і ловить ту одну рибину, по яку прийшов. Оператори — це твоя наживка й твій глибиномір.

Визначмо зараз ключовий термін, бо я користуватимуся ним постійно. **Оператор** — це особливе слово чи символ, який ти додаєш до пошуку і який дає пошуковику додаткову вказівку. Звичайні слова кажуть, *що* шукати. Оператори кажуть, *як* і *де* шукати. У цьому весь секрет.

Оператори, по одному

Я навчу кожного на крихітному прикладі. Читай їх повільно і, якщо можеш, вбивай кожен приклад у пошуковик по ходу.

Ти вчиш це пальцями, а не лише очима. Усюди я використовуватиму вигадані імена, ніки й сайти, тож ніщо тут не вказує на реальну людину.

Точний збіг — лапки

Постав слова в "лапки" — і пошуковик мусить знайти саме ці слова, саме в тому порядку. Без лапок пошуковик вільний перетасовувати твої слова, підставляти синоніми й викидати слова, які вважає неважливими.

- Marina Delcroix — пошуковик може показати сторінки зі словом «Marina», сторінки зі словом «Delcroix» і сторінки, що лише приблизно збігаються.
- "Marina Delcroix" — лише сторінки з цим повним іменем, написаним саме так, поруч.

Це найкорисніша окрема звичка в пошуку. Імена, фрази, повідомлення про помилки, цитати з промови — обгорни їх у лапки й дивися, як шум відпадає.

Пошук усередині одного сайту — site:

Оператор site: каже пошуковику дивитися *лише* всередині одного сайту. Пишеш site:, тоді вебадресу, без пробілу.

- site:linkedin.com "Marina Delcroix" — знайти це ім'я лише в LinkedIn.
- site:reddit.com stolen bicycle Copenhagen — шукати тільки в Reddit.

Це потужно з двох причин. По-перше, власний пошук сайту часто слабкий, тоді як пошуковик уже проіндексував увесь цей сайт значно краще. По-друге, ти можеш прицілитися саме в той куток інтернету, де твоя відповідь, найпевніше, живе.

Ти навіть можеш націлити site: на цілий *тип* сайтів, використовуючи закінчення адреси:

- site:gov.uk — лише сторінки британського уряду.
- site:.edu — лише навчальні заклади, здебільшого університети. (Зверни увагу на крапку на початку: site:.edu збігається з усією родиною .edu, а не з одним сайтом.)

Знайти конкретні типи файлів — filetype:

Не все в інтернеті — звичайна вебсторінка. Звіти, таблиці, презентації й форми часто є документами. Оператор filetype: знаходить їх.

- filetype:pdf "annual report" Meridian Logistics — знайти PDF-звіти для вигаданої компанії.
- filetype:xlsx budget 2024 site:gov.uk — знайти таблиці (xlsx — це файл Excel) на сайтах уряду Великої Британії.
- filetype:pptx "Meridian Logistics" — знайти презентації PowerPoint, у яких названо компанію.

Документи — це золото. Люди обережні з тим, що викладають на вебсторінку, але часто забувають про те, що

поховане в старому PDF чи таблиці, яку виклали роки тому. Список телефонів, довідник співробітників, протокол наради — це ховається в документах.

Дивитися в заголовку чи вебадресі — `intitle: i inurl:`

Кожна вебсторінка має *заголовок* (той рядок, що показується у вкладці браузера) і *адресу* (URL, той рядок `www...` угорі). Два оператори дозволяють шукати лише в цих частинах.

- `intitle:"staff directory" Meridian Logistics` — сторінки, чий *заголовок* містить «*staff directory*». Сторінка, яка не полінувалася так себе назвати, дуже ймовірно і є справжньою, а не сторінкою, що лише мимохідь про це згадує.
- `inurl:careers site:meridianlogistics.example` — сторінки, чия *адреса* містить слово «*careers*».

Чому це важливо? Бо ключове слово в заголовку чи адресі — сильний сигнал, що сторінка *про* цю річ, а не просто побіжно її зачіпає. Це спосіб знайти сторінки, які влучають у ціль, а не дотичні до неї.

Прибрати те, чого ти не хочеш — знак мінус

Постав знак мінус - прямо перед словом (без пробілу) — і пошуковик викине кожен сторінку, що містить це слово. Ось як ти прибираєш хаотичний пошук.

- jaguar -car -animal — тобі потрібен гітарний підсилювач або спортивна команда, а не машина й не великий кіт.
- "Marina Delcroix" -obituary — ти шукаєш живу людину, а весь час натрапляєш на некролог тезки. Прибери його.
- Meridian Logistics -jobs -careers — тобі потрібні новини й записи про компанію, а не нескінченні вакансії.

Знак мінус тихий, але могутній. Більшість поганих пошуків не позбавлені правильних сторінок — вони топлять їх під неправильними. Відніми неправильні.

Розширити сітку свідомо — OR

Іноді тобі потрібне *будь-яке* з двох. Пиши OR великими літерами між ними. (Регістр важливий; «or» малими літерами трактується як звичайне слово.)

- "Marina Delcroix" OR "M. Delcroix" — злови і повне ім'я, і скорочену форму.
- Meridian Logistics (invoice OR receipt OR statement) — круглі дужки акуратно групують варіанти.

Використовуй OR, коли твою ціль можуть записувати більш ніж одним способом — прізвисько, скорочення, дівоче прізвище, варіант написання. Ти кажеш пошуковику: «підійде будь-який із цих».

Заповнити пропуск — символ підстановки

Зірочка * — це символ підстановки. Він означає «сюди щось підходить, я точно не знаю що». Найкраще працює всередині фрази в лапках.

- "Marina * Delcroix" — знаходить «Marina Anne Delcroix», «Marina J. Delcroix» і так далі. * стоїть замість пропущеного середнього імені.
- "chief * officer" site:meridianlogistics.example — знаходить «chief executive officer», «chief financial officer», «chief technology officer», усе одразу.

Символ підстановки — твій друг, коли ти знаєш форму фрази, але не кожне слово в ній.

Звзити за часом — фільтри дати

Старі результати можуть ховати свіжі, а іноді тобі потрібні саме *старі*. Кожен великий пошуковик має фільтр дати, зазвичай захований під кнопкою «Інструменти» чи «Фільтри» під рядком пошуку. Постав його на останній рік, останній місяць чи власний діапазон.

У деяких пошуковиках можна також фільтрувати за датою прямо в запиті за допомогою before: і after: у форматі рік-місяць-день:

- Meridian Logistics after:2023-01-01 before:2023-12-31 — лише результати за 2023 рік.

Дати важать більше, ніж очікують новачки. Злиття, зміна назви, скандал — знання, *коли* щось сталося, дозволяє відразу відрізати репортажі з того вікна часу.

Використовуй більш ніж один пошуковик

Ось звичка, яка відділяє профі від усіх інших: вони ніколи не довіряють одному пошуковику.

Google, Bing і Yandex не показують однакових результатів. Кожен по-своєму сканує мережу, по-своєму ранжує сторінки і — головне — по-різному цензурує й розставляє пріоритети залежно від того, де сидить його компанія.

- Google найширший для більшості світу і той, який знають найбільше людей.
- Bing (пошуковик Microsoft) часто виводить сторінки, які Google ховає, а його пошук за зображеннями поводить інакше, що іноді допомагає.
- Yandex — російський пошуковик, і він значно сильніший для контенту російською і для багатьох речей у Східній Європі та Центральній Азії. Він також славиться зворотним пошуком за зображеннями — але це вже пізніший розділ.

Різні пошуковики бачать різні інтернети. Якщо один не показує тобі нічого, інший може показати все.

Хороша новина: ключові оператори — лапки, `site:`, `filetype:`, знак мінус — працюють в усіх трьох, лише з невеликими відмінностями. Тож навичка, яку ти щойно опанував, подорожує з тобою. Коли пошук у Google повертається порожнім, не роби висновку, що відповіді немає. Прожени той самий запит у Bing і Yandex, перш ніж здатися. Я розкрив не одну справу, просто перенісши точно той самий пошук в інший пошуковик.

То що таке «Google-доркінг»?

Ти, мабуть, чув фразу «Google-доркінг» і, можливо, вона звучала як хакерство. Це не так. Дозволь пояснити це просто.

«Дорк» — це просто точний пошук, що складає кілька операторів разом. От і все. Слово прийшло від дослідників безпеки, але техніка — не що інше, як те, що ти вже вивчив у цьому розділі, поєднане до купи. Коли хтось пише розумний запит на кшталт `site:meridianlogistics.example filetype:pdf "employee handbook"` — це «дорк». Це вправний пошук, а не проникнення.

Хочу бути дуже чітким щодо межі, бо це межа, варта поваги. Знайти документ, який сайт виклав у відкритий інтернет, — законно й нормально. Пошуковики існують, щоб індексувати публічні сторінки. Якщо компанія викладає файл там, де будь-хто може до нього дістатися, а пошуковик

його індексує, читати його — те саме, що читати будь-яку іншу публічну вебсторінку.

Що *не* нормально — це полювати такими пошуками на те, що, як ти знаєш, мало бути приватним (паролі, чужі сторінки входу, помилково оприлюднені персональні дані), а потім цим скористатися, щоб кудись проникнути чи комусь зашкодити. Оператор нейтральний; значення мають твій намір і твої дії — та сама яскрава лінія з розділу 2. Якщо пошук випадково виявляє щось явно чутливе, оприлюднене через помилку, правильний хід — занотувати, а не експлуатувати, і, де доречно, повідомити.

Дорк — це точне питання. Поставити точне питання — ніколи не злочин. Злочином може бути те, що ти робиш з відповіддю.

Розібрана справа: пошук однієї людини, професійно

Дозволь показати, як оператори поєднуються в щось справжнє. Уяви вигаданий запит: колега просить мене підтвердити теперішнього роботодавця й професійне минуле людини, яку вони знають лише як Marina Delcroix і яка, на їхню думку, працює десь у логістичній галузі в Європі. Це все, що ми маємо. Дивись, як кожен оператор розсіює туман.

- Крок 1 — Зафіксувати ім'я. Я ніколи не шукаю ім'я без лапок. Я починаю з "Marina Delcroix" у Google.

Повертається купа приблизно пов'язаних результатів, зокрема, як не прикро, некролог іншої Marina Delcroix і десятки не пов'язаних соцпостів. Ця купа каже мені, що ім'я існує і не є вкрай рідкісним. Достатньо, щоб почати.

"Marina Delcroix"

- 1 Obituary: Marina Delcroix, 1948-2022
 - 2 Marina Delcroix (@delcroix_art) photos
 - 3 Delcroix family reunion – guestbook
 - 4 Marina Delcroix logistics – LinkedIn
- 3 з топ-4 — шум; тільки №4 по темі

- Крок 2 — Зрізати шум. Я прибираю неправильну людину й неправильний контекст: "Marina Delcroix" -obituary -funeral. Некролог зникає. Результати вже чистіші. Точність — це здебільшого віднімання.
- Крок 3 — Іти туди, де живуть професіонали. Логістика — це кар'єра, тож я цілюся в професійну мережу: [site:linkedin.com "Marina Delcroix" logistics](https://www.linkedin.com/company/marina-delcroix-logistics/). Тепер я отримую невелику жменьку профілів замість усього інтернету. Верхній профіль виглядає ідеально — Marina Delcroix, і слово «logistics» просто тут. Було б легко зупинитися й назвати це збігом. Але я читаю далі заголовка, і виринає тертя: ця Marina Delcroix займається *продажем програмного забезпечення для ланцюгів поставок*, базується в Монреалі, а «logistics» — просто ключове слово в її самопрезентації. Не та людина.

Пошуковик збіг з моїми словами, а не з моєю ціллю. Результат на першій сторінці, що підходить твоєму запиту, — не те саме, що результат, який підходить твоїй справі.

- Крок 4 — Переформулювати, тоді підтвердити другим джерелом. Тож я перестаю довіряти верхньому влученню й затакую запит однією деталлю, яку насправді маю, — Європою: `site:linkedin.com "Marina Delcroix" logistics (Europe OR Rotterdam OR Antwerp)`. Цього разу спливає інший профіль: Marina Delcroix в операційному відділі фірми, яку я назву Meridian Logistics, розташованої в правильній частині світу. Це зачіпка, а не факт — тож я підтверджую її, перш ніж повірити. Я ніколи не довіряю одній сторінці, тож шукаю її ім'я на власному сайті компанії: `site:meridianlogistics.example "Marina Delcroix"`. Сторінка команди й пресреліз обидва називають її регіональною менеджеркою з операцій. Тепер незалежне джерело погоджується з профілем, а хибне монреальське влучання позаду мене.

- Крок 5 — Потягнутися до документів. Вебсторінки вичищають; документи забувають. Я запускаю `"Marina Delcroix" Meridian filetype:pdf`. Програма конференції 2023 року вказує її як спікерку з короткою професійною біографією — саме та деталь минулого, про яку просив мій колега. Ця біографія також згадує *попереднього* роботодавця, а це свіжа нитка, яку я міг би потягнути, якби знадобилося.

- Крок 6 — Перевірити другий пошуковик. Перш ніж щось записувати, я знову проганяю два найкращі запити в Bing і Yandex. Bing виводить статтю місцевих новин, яку Google поховав, і в ній її названо на ім'я й посаду. Тепер три окремі, публічні джерела погоджуються щодо роботодавця й ролі. Я зупиняюся тут, бо питання отримало відповідь і все веде назад до публічної сторінки, на яку я можу послатися.

Зверни увагу, що сталося. Я жодного разу не вгадував. Кожен крок використовував простий оператор, який ти тепер знаєш, і кожен крок або звужував пошук, або додавав незалежне підтвердження. Ось і все ремесло в мініатюрі.

І зверни увагу на глибший урок: хороший пошук сам по собі — це перший півот. В OSINT «півот» означає використання одного факту, який ти знайшов, щоб дістатися наступного факту. Точний пошук не просто відповідає на твоє питання — він вручає тобі нові нитки (попереднього роботодавця, співавтора, стару адресу), які стають відправною точкою твого наступного пошуку. Ти не просто знаходиш відповідь. Ти відчиняєш двері.

Вправа

Обери вигадану ціль, з якою можеш безпечно погратися, або візьми публічну особу, яку ти маєш дозвіл і причину шукати заради практики — скажімо, відомого автора. Тоді зроби ось що, записуючи запит і кількість результатів на кожному

кроці, щоб *побачити* точність у дії:

1. Пошукай його повне ім'я без лапок. Занотуй приблизно, скільки результатів повертається. 2. Пошукай те саме ім'я в лапках. Кількість впала? Верхні результати стали доречнішими? 3. Додай оператор `site:`, щоб шукати лише на одній платформі, де він, найпевніше, з'явиться. 4. Додай знак мінус, щоб прибрати один вид результатів, який тобі заважає. 5. Запусти пошук `filetype:pdf` для його імені й подивися, чи спливають документи, яких не показали звичайні вебсторінки. 6. Насамкінець візьми свій єдиний найкращий запит і запусти його, без змін, у **Bing** і **Yandex**, а також у **Google**. Запиши один результат, що з'явився в одному пошуковику, але не в інших.

Якщо ти закінчиш і твій останній пошук поверне менше, гостріших результатів, ніж перший, — вітаю. Ти перестав тягти сітку через океан.

Підсумок

- Точність перемагає обсяг. Пошук, який повертає п'ять правильних сторінок, перемагає той, що повертає два мільйони неправильних. Оператори — лапки, `site:`, `filetype:`, `intitle:/inurl:`, знак мінус, **OR**, символ підстановки `*` і фільтри дати — це те, як ти туди дістаєшся.
- Складай оператори й перемикай пошуковики. «Дорк» — не що інше, як кілька операторів, поєднаних в

одне точне, законне питання. А оскільки Google, Bing і Yandex бачать різні інтернети, запуск того самого запиту в усіх трьох часто є різницею між «з порожніми руками» й «з відповіддю».

- **Хороший пошук** — це перший півот. Кожен гострий пошук не лише відповідає на сьогоднішнє питання, а й вручає тобі наступну нитку, яку потягнути — завжди підтверджену другим незалежним публічним джерелом, перш ніж ти повіриш.

РОЗДІЛ П'ЯТИЙ

Нікнейми

Перша нитка

Розкажу тобі про день, коли нікнейм розплутав ціле життя.

Одного разу я мав майже нічого, з чим працювати. Один нік. Сім маленьких літер, які людина колись роками раніше вбила в поле реєстрації і забула про них. Ні справжнього імені. Ні фото, якому я довіряв би. Ні місцезнаходження. Лише цей рядок.

За дві години я мав повне ім'я, три email-адреси, рідне місто й обличчя. Я нічого не зламував. Я не порушив жодного закону. Я просто потягнув за одну нитку, і весь світ розпустився.

Тією ниткою був нікнейм. І в цьому розділі я навчу тебе, як за нього тягнути.

Що таке нікнейм насправді

Нікнейм (юзернейм) — це ім'я, яке людина обирає собі в інтернеті. Його також називають ніком. Це @щось у Twitter чи Instagram. Це ім'я перед акаунтом у Reddit. Це частина email до знака @.

Люди обирають ці імена один раз, коли вони молоді чи поспішають, а потім тримаються за них. Назавжди. Ось у чому секрет. Нікнейм здається дрібним і одноразовим. Це не так. Це одна з найсильніших відправних зачіпок у всій розвідці з відкритих джерел.

Розвідка з відкритих джерел, або OSINT, просто означає з'ясовувати речі, використовуючи інформацію, яка вже публічна. Ніякого злому. Ніяких трюків, що порушують закон. Лише те, що люди залишили на видноті, де будь-кому дозволено дивитися. Ми збираємо це, ми з'єднуємо це і ми обережно міркуємо про те, що воно означає.

Нікнейм — ідеальна перша нитка з однієї простої причини.

Люди ліниві з іменами. Вони повторно використовують той самий нік усюди.

Подумай про власне життя. Ти, ймовірно, маєш одне-два прізвиська, які вбивав у сотню форм реєстрації. Може, це дитяче прізвисько. Може, це твоє ім'я плюс улюблене число. Може, це слово, яке тобі подобалося в чотирнадцять. І ти використовував його на ігрових сайтах, форумах, у шопінг-акаунтах і соцмережах, знову і знову, роками.

Так робить кожен. Це по-людськи. Вигадувати свіже розумне ім'я щоразу — виснажливо, а люди втомлені. Тож вони повторюють. І це повторення — слід.

Головна ідея

Ось весь розділ в одному реченні.

Якщо людина використовує той самий рідкісний нікнейм у багатьох місцях, ти можеш крокувати від одного місця до наступного й поволі складати картину того, хто вона.

Ось і все. Один нік стає картою. Кожна зупинка на карті дає тобі щось нове: фото, справжнє ім'я, прив'язаний email, ще один нік, місто. І кожна нова річ дозволяє тобі зробити ще один крок.

Але є правило, яке ти маєш назавжди закарбувати в пам'яті, перш ніж ми просунемося бодай на дюйм далі. Це найважливіше речення в цій книзі.

Збіг імен НЕ доводить, що це та сама людина.

Два акаунти з однаковим ніком можуть бути однією людиною. Або можуть бути двома незнайомцями, які випадково обрали те саме слово. Або ім'ям, яке хтось покинув, а незнайомиць пізніше схопив. Збіг — це зачіпка, а не висновок. Зачіпка — це натяк, що вказує кудись. Висновок — це те, що ти насправді довів. Ніколи не плутай ці дві речі. Це помилка, що губить новачків, і це єдине речення, яке треба винести з цього розділу.

Я засвоїв це в неприємний спосіб. На початку я був певен, що взяв свого чоловіка. Той самий рідкісний нік, те саме

місто, хронологія збігалася. Я вписав його ім'я вгорі своїх нотаток і почувався розумним. Я помилявся. Це був незнайомець, який просто випадково поділяв той нік, — слід роздвоївся на два профілі раніше, а я пройшов повз, бо хотів мати рацію. Той промах навчив мене більше, ніж будь-яке чисте влучання: тієї миті, коли ти починаєш сподіватися, що зачіпка вказує на твою ціль, ти перестав розслідувати й почав вгадувати.

Шкала впевненості

Оскільки збіг імен не доводить особи, нам потрібен спосіб говорити про те, *наскільки* ми впевнені. Я користуюся простою шкалою. Кожна зачіпка, яку ти знаходиш, перебуває на одному з цих щаблів.

- **Слабкий.** Один спільний нік. Поширений аватар. Загальне біо. Саме собою це майже нічого не доводить. Особливо якщо нік короткий чи звичайний, як-от john чи mike88.
- **Помірний.** Рідкісний, незвичайний нік, ужитий повторно, плюс іще щось, що пасує. Однаковий вік акаунта. Кілька спільних друзів. Тепер ти вже кудись рухаєшся.
- **Сильний.** Збігається справді рідкісний сигнал. Точно той самий незвичайний файл фото профілю. Точно та сама дивна фраза у двох біо. Підказка для відновлення, що

збігається. Дві такі речі разом — і ти майже на місці.

- Підтверджено. Об'єкт сам зв'язує акаунти («знайдіть мене в Х»). Або жорсткий ідентифікатор, як-от фрагмент email відновлення, вказує на одну-єдину людину.

Твоя робота як дослідника — підійматися цією шкалою. Ти починаєш унизу зі слабкої зачіпки. Ти збираєш більше підказок. Кожна підказка, що пасує, підтягує тебе на щабель вище. Ти не називаєш справжню людину, поки не будеш близько до вершини.

Що рідкісніша підказка, то швидше ти піднімаєшся. Поширений нік ледь тебе зрушує. Унікальний нік плюс унікальне фото можуть пронести тебе більшу частину шляху за два кроки.

Метод, крок за кроком

Так я опрацьовую нікнейм з нуля. Дотримуйся цього порядку.

- Отримай своє насіння. Той один нік, з якого ти починаєш, — це твоє насіння (seed). Запиши його точно, літера за літерою. Регістр зазвичай не має значення, а от написання — завжди.
- Перевір, де він існує. Візьми насіння й пошукай його на багатьох платформах одразу. Це називається енумерація — велике слово, яке просто означає «перевірка списку». Ти запитуєш: на яких сайтах цей точний нік розв'язується

в справжній, живий профіль? Є безкоштовні інструменти, що перевіряють сотні сайтів за секунди — добре відомі приклади це Sherlock, Maigret і WhatsMyName (назви інструментів з часом змінюються, тож стався до них як до прикладів, а не як до істини в останній інстанції). Але пам'ятай: інструмент лише каже тобі, що сторінка існує. Він не каже тобі, що ця сторінка — твоя людина. Ти все одно дивишся власними очима.

- **Сортуй влучання вручну.** Тріаж означає сортування результатів за тим, що важливо. Відкрий кожне живе влучання. Це справжній профіль зі справжньою активністю чи порожня заглушка? Деякі сайти показують сторінку «зайнято» для імені, яким ніхто насправді не користується. Це хибне влучання. Викинь його.
- **Збери нові нитки.** На кожному справжньому профілі збирай усе нове: справжнє ім'я, біо, прив'язаний сайт, фото, ще один нік, який вони згадують, місто. Кожна нова річ — свіжа нитка, яку потягнути.
- **Іди за нитками.** Годуй нові ніки назад в енумерацію. Годуй справжнє ім'я в наступний крок — перестановки. Годуй фото в пошук за зображенням. Знову і знову, картина росте.
- **Оцінюй кожен зв'язок на шкалі.** По ходу постійно запитуй: наскільки я впевнений, що цей акаунт — та сама людина? Записуй щабель. Слабкий, помірний, сильний, підтверджено. Не давай слабкій зачіпці тихо

перетворитися на факт у твоїй голові.

Тепер розкрию три з цих кроків детальніше, бо саме там новачки знаходять справжнє золото.

Вгадування варіацій

Люди не завжди повторюють нік точно. Іноді вони трохи його змінюють. firecat стає fire_cat стає firecat88 стає thefirecat. Фокус у тому, що кожна людина змінює його *своїм власним послідовним способом*. Це її особиста граматики імен — її приватний звід правил для творення ніків.

Щойно ти помітиш звід правил, ти можеш передбачати ніки, яких ще навіть не знайшов.

Щоб згенерувати варіації, візьми частини, які знаєш, і змішай їх:

- Ім'я і прізвище в різному порядку: annalee, anna.lee, leeanna, a_lee.
- Додай число, яке їм, схоже, подобається, або рік народження: annalee92, anna_lee_1992.
- Заміни літери на схожі, це називається літспік (leetspeak): е на 3, о на 0, тож annalee стає ann4l33.
- Додай маленькі слова, яким вони віддають перевагу: theannalee, realannalee, annaleexo.

Тоді прожени ці здогади назад через енумерацію, щоб побачити, які з них справжні. Передбачити нік — приємно й

розумно, але передбачення перебуває на слабкому щаблі, поки живий профіль не доведе, що воно справжнє.

Перетворення нікнейма на email і назад

Частина email до знака @ називається локальною частиною (local-part). У annalee92@gmail.com локальна частина — annalee92. Помітив дещо? Це нік. Тож email і нікнейми перетікають одне в одне.

- **Email на нікнейм.** Якщо знаходиш email, відріж локальну частину й прожени її через енумерацію, як будь-який інший нік. annalee92 може бути на десяти сайтах.
- **Нікнейм на email.** Якщо маєш нік, вгадуй email з нього. Спробуй annalee92@gmail.com, annalee92@outlook.com, annalee92@proton.me. Тоді підтверди, які скриньки насправді існують, за допомогою перевірки існування.

Перевірка існування запитує сайт, лагідним і публічним способом: «чи існує тут акаунт із цим email?». Багато сайтів відповідають на це тихо, ні на мить не турбуючи власника акаунта. Безкоштовні інструменти роблять це за тебе на десятках сервісів. Слово обережності: кілька сайтів надішлють власнику сповіщення, якщо ти їх поштрикаєш. Оминай такі, інакше ти сполохаєш свій об'єкт і переступиш межу, яку не варто переступати. Тримайся публічного, тихого боку паркана.

Наскільки добре працює цей півот, повністю залежить від того, наскільки рідкісна локальна частина. annalee92 дає чудовий півот. info, чи contact, чи admin не кажуть тобі нічого, бо ними користується мільйон людей.

Фото — друга нитка

Нікнейм — нитка номер один. Фото профілю, аватар, — нитка номер два. І часто вона сильніша, бо люди повторно використовують зображення ще недбаліше, ніж імена.

Два способи потягнути за цю нитку:

- Зворотний пошук за зображенням. Ти даєш пошуковику картинку замість слів, і він знаходить інші місця, де з'являється саме ця картинка. Якщо те саме дивне фото спливає на трьох акаунтах із трьома різними ніками — це сильна ознака, що всіма трьома керує одна людина.
- Пошук обличчя. Деякі пошуковики знаходять те саме обличчя на різних фото. Це ще потужніше, бо може зв'язати людину навіть тоді, коли вона щоразу використовувала іншу картинку.

Але тримай шкалу в думці й тут теж.

- Схоже — не те саме, що ідентичне. Результат, який лише *схожий* на твоє фото, може бути іншим кадруванням, репостом чи справжнім двійником. Перш ніж довіритися збігу, підтверди, що це *те саме*

зображення, а не просто схоже.

- Рідкісне, оригінальне фото, яке людина зробила сама, — сильний сигнал.
- Стокове фото, знаменитість чи картинка, якою користуються тисячі людей, нічого не варта для встановлення особи.
- Згенероване ШІ обличчя — фейкове обличчя, зроблене комп'ютером, — не поверне жодних збігів узагалі. І ця тиша — сама собою сигнал. Обличчя, якого немає більше ніде, часто є вигаданою персоною.

Не використовуй інструменти пошуку облич без письмового дозволу й правової перевірки.

Пошук облич напругу зачіпає приватність людей, і в багатьох місцях він обмежений чи прямо незаконний. Знай правила там, де ти є, отримай дозвіл письмово й май чітку законну причину, перш ніж хоч раз його запустити. Це не опція — це той один пілот у цьому розділі, що може поставити *тебе* по неправильний бік закону.

Одна справа, від початку до кінця

Ось як усе це працює на вигаданій людині. Усі й усе тут вигадане. Іди за тягами.

- Крок 1 — Насіння. Невеликий онлайн-магазин отримує фейкові п'ятизіркові відгуки. Кожен фейковий

відгук приходить з акаунта з ніком mossyfern. Це все, що я маю. Один нік, сім літер, більше нічого. Я записую його: mossyfern.

- Крок 2 — Енумерація. Я проганяю mossyfern по кількох сотнях сайтів. Інструмент не вручає мені чистий список. Ось приблизно те, що він насправді друкує:

```
[*] Checking: mossyfern
[+] found    photo-site.example/mossyfern
[+] found    gaming-forum.example/u/mossyfern
[+] found    recipe-site.example/mossyfern
[+] found    twitter.example/mossyfern
[-] 404      instagram.example/mossyfern
[!] unknown recipe-site (page loaded, empty?)
4 found, 1 not found, 1 flagged
```

Читай це чесно. Інструмент схиляється до *оптимізму* — він рахує сторінку як «found» тієї миті, коли вона завантажується, навіть заглушку, тож ті зелені рядки — це влучання, які треба перевірити, а не зачіпки, яким варто довіряти. Instagram, та одна платформа, яку я найбільше хотів, не має жодного mossyfern узагалі. Це не баг; ніка там просто немає, і я це записую. Просто зараз увесь цей запуск — *слабка* зачіпка.

- Крок 3 — Тріаж і збір. Я відкриваю кожне влучання власними очима, бо інструмент лише довів, що сторінка завантажується. Кулінарний сайт — порожня заглушка: ім'я зайняте, але немає ні постів, ні аватара, нічого. Це хибне влучання; інструмент назвав його «found», а

насправді це просто припаркована, загальна сторінка. Я викидаю його. Влучання в Twitter — небезпечне: це справжній, активний акаунт, але він належить хлопцю-підлітку в іншій країні, який постить про футбол. Ті самі сім літер, зовсім інша людина. Це класичний хибнопозитив — хтось інший схопив ідентичний нік. Я ловлю це не за ім'ям (ім'я збіглося ідеально), а за *контентом, фото й датами*: ніщо там не торкається рослин, будинків чи дощового міста, а акаунт на три роки молодший за інші. Геть його. Два влучання виживають. Фотосайт справжній і активний: десятки знімків кімнатних рослин і біо, що читається «plant mom in the rainy city, she/her». Ігровий форум теж справжній, а профіль веде на особистий блог. Два справжні профілі. Я збираю: хобі (рослини), натяк на місцезнаходження (дощове місто), прив'язаний блог.

Ті самі сім літер, інша людина. Ось пастка тезок у плоті.

• Крок 4 — Тяг за аватар. Обидва справжні профілі використовують те саме фото: жінка тримає папороть біля вікна. Я роблю зворотний пошук за цим зображенням. Точно те саме фото з'являється на сторінці невеликого місцевого клубу любителів рослин, з підписом «our volunteer Deborah Ashworth». Тепер я маю можливе справжнє ім'я. Це сильний сигнал — рідкісне, оригінальне фото, що прив'язує нік до імені. Я піднявся на

два шаблі одразу.

- Крок 5 — Перестановки з імені. Маючи в руках «Deborah Ashworth», я будував варіації: deborahashworth, dashworth, deb_ashworth, debashworth. Я проганяю їх назад через енумерацію. deb_ashworth живий на професійній мережі, вказано роботу в розсаднику рослин у місті Elmbrook. «Дощове місто», і «Elmbrook», і «рослини» — усе пасує. Помірний сигнал сам собою, але він акуратно складається на те, що я вже маю.

- Крок 6 — Півот на email. З блога, який я знайшов на Кроці 3, сторінка «contact» показує deb.ashworth.ferns@gmail.com. Я не пишу туди. Я роблю тиху перевірку існування. Ця адреса зареєстрована на фотосайті й ігровому форумі — точно ті два акаунти, з яких я почав. Це сильний сигнал, але я себе стримую: це *одна* перевірка. Один позитивний результат, хоч який чистий, заслуговує на сильний і не вище. Він лишається сильним, поки друге, незалежне джерело не погодиться. Тож я тримаю його там і йду шукати те друге джерело.

- Крок 7 — Підтвердити й зупинитися. Я вже маю це. Рідкісне оригінальне фото прив'язало нік до імені Deborah Ashworth на сторінці клубу рослин (Крок 4). Перевірка email тепер прив'язує той самий нік до того самого імені другим, незалежним способом (Крок 6). Два окремі джерела, здобуті двома окремими шляхами, вказують на одну людину. *Ось* що піднімає мене від

сильного до підтверджено — не сам email, а email плюс фото, що погоджуються між собою. Я оформляю знахідку, виклавши кожен щабель доказів просто й ясно, щоб будь-хто міг перевірити мою роботу. А тоді зупиняюся. Я не переслідую її приватне життя далі за питання, яке мені поставили. Ця стриманість — частина ремесла.

Озирнися на те, що сталося. Кожен крок вручав наступному кроку його пальне. Нік привів до профілів. Профілі привели до фото. Фото привело до імені. Ім'я привело до нових ніків. Ніки привели до email. Email замкнув коло. Жодна окрема підказка нічого не довела. Усі разом — довели.

І зверни увагу на безлад, який я *не* проскочив. Інструмент назвав припарковану кулінарну сторінку «found», тож я відкрив її й викинув. Він збігся з незнайомцем у Twitter, тож я вбив хибнопозитив, читаючи контент і дати, а не ім'я.

Справжня робота виглядає ось так.

Пастки, що ловлять новачків

Перш ніж підеш практикуватися, вивчи помилки, щоб могли їх обходити.

- Пастка тезок. Дві різні людини, той самий нік. Це найпоширеніша невдача з усіх. Короткі й поширені ніки майже нічого не варті, бо стільки людей їх поділяють. Довіряй рідкісним рядкам, сумнівайся в поширених.

- **Перевикористане ім'я.** Хтось покидає нік; незнайомець хапає його пізніше. Старі пости й нові пости — це дві різні людини в одному імені. Переконайся, що продовжилася *людина*, а не просто рядок.
- **Інструмент, що бреше.** Інструменти енумерації ламаються, коли сайти змінюються. Вони повідомляють про влучання, яких немає, і пропускають ті, що є. Завжди дивись власними очима й запускай більш ніж один інструмент, бо кожен перевіряє інший список сайтів.
- **Фейкове обличчя.** Стокове фото чи обличчя від ІІІ ні з чим не зв'язує реальної особи. Не будуй справу на картинці, якою міг би скористатися будь-хто.

У кожної з цих пасток ті самі ліки: піднімайся шкалою і збирай незалежні підказки.

Вправа

Зроби це на собі. Це найбезпечніший і найповчальніший спосіб навчитися.

- Запиши найстаріший нікнейм, який можеш пригадати, — той з підліткових років, який ти вбивав усюди не думаючи.
- Прожени його через безкоштовний крос-платформний чекер нікнеймів. (Примітка про інструменти: деякі — це просто сайти, які ти відкриваєш; інші — маленькі безкоштовні програми, які ти встановлюєш, іноді

запускаєш з термінала. Якщо термінал для тебе новий, почни з чекера в браузері — метод ідентичний, і тобі ніколи не треба платити, щоб щось відпрацьовувати в цій книзі.) Подивися, у скількох місцях він досі живе.

- Відкрий кожне справжнє влучання. Запитай: що незнайомиць міг би дізнатися про мене з одного лише цього? Хобі? Місто? Справжнє ім'я? Старе фото?
- Тепер спробуй три варіації того ніка, використовуючи власну граматику імен. Скільки з них — теж ти?
- Насамкінець візьми найстаріше своє фото, яке можеш знайти, і зроби зворотний пошук за зображенням. Де ще воно з'являється?

Посидь із тим, що знайдеш. Це точно те, що хтось зробив би з ціллю. Відчути це зсередини навчає тебе і того, як працює метод, і того, чому ми ставимосся до нього з такою обережністю.

*Оберни це проти себе. Ліки від усього, що ти щойно знайшов на собі: перестань повторно використовувати один нік усюди, спиши старі акаунти, яких більше не торкаєшся, і тримай справжнє ім'я подалі від одноразових профілів. Той один перевикористаний нікнейм — нитка, що зв'язує все твоє життя докупи, — переріж її.
(Повний чекліст: Додаток D, «Поверни собі*

контроль».)

Підсумок

- Нікнейм часто є єдиною найкращою відправною ниткою, бо люди повторно використовують той самий нік на багатьох сайтах роками, а один нік веде до іншого, тоді до фото, імен і email.
- Опрацьовуй нитку по порядку: енумеруй, де існує нік, тріажуй справжні влучання на око, збирай нові підказки, вгадує варіації й переходь ниткою між нікнеймом та email — із фото профілю як сильною другою ниткою.
- Збіг імен ніколи не доводить, що це та сама людина. Піднімайся шкалою впевненості від слабкого до підтверджено, складай незалежні підказки, стеж за тезками й перевикористаними іменами і тримайся суворо законного й відкритого.

РОЗДІЛ ШОСТИЙ

Email

Головний ключ

Візьми на секунду власну email-адресу. У скількох місцях ти вбивав її цього року? Шопінг-сайт. Розсилка. Новий застосунок. Робочий логін. Гра, яку захотіла твоя дитина. Форма запису до стоматолога.

Тепер подумай, як довго ти маєш цю адресу. Багато людей тримають ту саму пошту десять років, дехто — двадцять. Ми міняємо номер телефона, коли переходимо до іншого оператора. Ми переїжджаємо. Ми міняємо роботу. Але пошта лишається.

Ось чому в OSINT email-адреса — головний ключ.

Швидке нагадування слова. OSINT означає *розвідку з відкритих джерел* (Open-Source Intelligence). Це ремесло знаходити факти про людину чи річ, використовуючи лише інформацію, яка вже публічна — відкриту мережу, публічні записи, речі, які люди опублікували самі. Ніякого злому. Ніяких трюків, що порушують закон. Лише уважний погляд.

Email-адреса — це один маленький рядок тексту. Але це *стабільна, унікальна* мітка однієї людини. Стабільна означає, що вона рідко змінюється. Унікальна означає, що

нею користується лише одна людина. Склади ці дві речі разом — і матимеш щось рідкісне: єдину крапку, що з'єднується з десятками інших крапок. Де людина робить покупки. Якими застосунками користується. Яке її справжнє ім'я. Іноді її фото. Іноді стару звичку з пароллями, яку вона так і не виправила.

У цьому розділі я покажу тобі, як тягнути за цей рядок — лагідно, законно й крок за кроком.

Email-адреса — це та одна мітка, яку людина несе роками через увесь інтернет. Знайди її — і двері починають відчинятися.

Чому email зв'язує так багато докупи

Кожен акаунт, який ти створюєш, просить email. Мусить. Саме так сайт каже «ти — це ти», коли ти знову входиш. Саме так він надсилає тобі чек чи посилання для скидання.

Тож твоя пошта тихо стає списком усіх місць, де ти був. Не навмисне. Воно просто так виходить.

Для дослідника це означає, що один email може відповісти на питання на кшталт:

- На яких сайтах і в яких застосунках зареєстрована ця людина?
- Яке її справжнє ім'я?

- Який нікнейм вона любить використовувати?
- Чи потрапляли її дані колись у злом — і якщо так, то з якого сервісу?
- Це *та сама* людина, що й той інший акаунт, який я знайшов?

Ми візьмемо їх по черзі. Але спершу — правило, що тримає тебе в безпеці й чесності.

Межа, яку ти ніколи не переступаєш

В email-OSINT є яскрава, чітка межа. Вивчи її зараз — і вона захищатиме тебе всю кар'єру.

Ти можеш перевірити, чи існує акаунт. Ти ніколи не можеш торкатися акаунта.

Перевіряти — нормально. Запитати сайт «чи є тут акаунт для цього email?» — це публічне питання, яке будь-хто може поставити. Читати те, що сайт *виришує* тобі показати, — нормально.

Торкатися — не нормально. Входити — не нормально. Вгадувати пароль — не нормально. Використовувати злитий пароль, щоб потрапити всередину акаунта — навіть щоб «просто подивитися», — не нормально. Це не OSINT. Це проникнення, і в більшості країн це злочин.

Ось найпростіший спосіб тримати це в голові. Ти стоїш на тротуарі перед будинком. Тобі дозволено помітити, що

світло горить, машина на під'їзді, на поштовій скриньці написано «Karas». Тобі *не* дозволено відчиняти двері. Та сама вулиця, інша дія.

Підтверди, що акаунт існує. Прочитай те, що сайт пропонує добровільно. Тоді зупинися. Ніколи не входи, ніколи не вгадує, ніколи не використовуй злитий пароль.

Ми повернемося до цієї межі не раз, бо вона важить найбільше там, де спокуса найсильніша.

Метод 1 — Де використовується цей email?

Найперше, чого ти хочеш від email, — це карта. Де ця людина зареєстрована?

Є розумний, лагідний спосіб з'ясувати, і він використовує функцію, яку кожен сайт уже має: форми «забули пароль» і «реєстрація».

Ідея проста. Коли ти заходиш на сайт і починаєш процес «забули пароль», сайт мусить запитати себе: *чи маємо ми акаунт для цього email?* І тоді він зазвичай каже тобі відповідь, просто там, на екрані, перш ніж ти щось довів.

- Якщо він каже «ми надіслали посилання для скидання на вашу пошту» чи «цей email уже використовується» — акаунт існує.

- Якщо він каже «ми не знайшли акаунта з цим email» — акаунта немає.

Ця різниця у формулюванні називається диференціал (differential). Це просто гарне слово для «сайт дає дві різні відповіді, і відповідь каже тобі те, що ти хочеш знати».

Зверни увагу, чого ти *не* зробив. Ти не увійшов. Ти не отримав посилання для скидання (воно йде в поштову скриньку об'єкта, не твою). Ти нічого не торкнувся. Ти поставив публічне питання й прочитав відповідь. Ось чому ця техніка на безпечному боці межі. Але будь чесним щодо того, що означає «пасивний»: це означає, що ти не увійшов — а не те, що ти невидимий. Сайт може обмежити частоту цих перевірок, залогувати спробу чи порахувати її як порушення умов користування. Тихо — не те саме, що невиявно.

Ти міг би робити це вручну, один сайт за раз — клікнути «забули пароль», вбити email, прочитати відповідь, записати. Зробивши це кілька разів вручну, ти навчишся, як виглядають відповіді.

Є також інструменти, що перевіряють багато сайтів одразу й вручають тобі список. Їхні назви приходять і йдуть, тож я не прив'язуватиму тебе до жодного. Добре відомим безкоштовним був *Holehe*, який перевіряє понад сотню сайтів і повідомляє, чи зареєстрований email на кожному;

хостований сервіс під назвою *Erieos* робить щось схоже у твоєму браузері. Стався до них як до *прикладів методу*, а не як до істини. Email-інструменти псуються швидко — вони залежать від форм інших сайтів, а ці форми змінюються щомісяця. Завжди перехресно перевіряй несподіване «не знайдено» другим інструментом, перш ніж повірити.

Те, що отримуєш у кінці, — золото: слід. «Цей email є на GitHub, Spotify і старому форумі.» Кожне — нова нитка, яку потягнути.

Метод 2 — Перетворення імені на email (трюк із шаблоном)

Іноді ти маєш протилежну проблему. Ти знаєш ім'я людини й де вона працює, але не маєш її email. Ти хочеш *вирахувати* його.

Ось ключовий факт, що робить це можливим. Компанії майже завжди дотримуються одного шаблону для всіх. Вони не вигадують новий стиль для кожного співробітника — це був би хаос для їхнього ІТ-відділу. Тож вони обирають один рецепт і штампують його на всю компанію.

Поширені рецепти виглядають ось так. Скажімо, домен компанії — `brightmail.com`, а співробітник — Jason Karas:

- `first.last` → `jason.karas@brightmail.com`

- flast (перша літера імені + прізвище) → jkaras@brightmail.com
- first → jason@brightmail.com
- f.last → j.karas@brightmail.com
- firstl → jasonk@brightmail.com

А тепер прекрасна частина, і її варто сказати вголос:

Знайди один підтверджений email у компанії — і ти зламав шаблон для всіх там.

Якщо можеш підтвердити — з публічного джерела — що maria.velez@brightmail.com справжній, ти тепер знаєш, що рецепт — first.last. Тож бос, якого ти шукаєш, Jason Karas, — це сильне передбачення: jason.karas@brightmail.com.

Де знайти ту одну підтверджену адресу? У публічних місцях, усі відкриті:

- Пресреліз компанії чи PDF-звіт (спробуй пошук на кшталт "@brightmail.com" filetype:pdf).
- Сторінка «контакти» зі співробітниками.
- Публічний репозиторій коду, де email розробників сидять в історії комітів.
- Інструменти пошуку за доменом, що вже каталогізували формат email компанії.

Невелике застереження, щоб ти виглядав професіоналом, а не спамером. Щойно маєш передбачену адресу, не надсилай на неї лист, щоб «протестувати». Надсилання пошти каже людині, що хтось нишпорить навколо, а це перекреслює всю твою мету. Є способи перевірити, чи адреса справжня, без надсилання чого-небудь, і інструменти, збудовані саме для цього — але для новачка чесний хід такий: знайди одну підтверджену адресу, застосуй шаблон і став до результату як до сильного, а не підтверджено.

Ще одна примітка. Цей трюк із шаблоном найчистіший для *робочих місць*. Для особистих адрес у стилі Gmail люди підмішують прізвиська, роки народження й випадкові числа, тож варіантів стає надто багато. Тримай його для доменів компаній, де панує дисципліна.

Метод 3 — Чи був цей email у зломі? (тільки відкритий слід)

Великі компанії зламують. Це сумно, але звично. Коли це стається, списки email їхніх користувачів — іноді з паролями, датами народження чи адресами — витікають в інтернет. Кожну таку подію ми називаємо зломом (breach).

Для дослідника *відкритий слід* злому — корисний, обережний сигнал. Зверни увагу на слово: відкритий слід. Ми перевіряємо, *чи* email з'явився у відомому зливі і в яких зливах. Ми не йдемо полювати на вкрадені паролі й уже

точно ними не користуємося.

Золотий стандарт безкоштовного інструменту тут — Have I Been Pwned (часто пишуть HIBP). Ти вбиваєш email, і він дає простий список: ця адреса з'явилася в зломі LinkedIn такого-то року, у зломі Dropbox іншого й так далі. Він *не* показує тобі паролів. Він показує *присутність* — сам факт відкритого сліду та назви й дати зливів.

Чому це корисно OSINT-досліднику? Дві причини, обидві чисті:

- Це підтверджує, що людина мала десь акаунт. Якщо email спливає в зломі «MyFitnessPal», то ця людина користувалася MyFitnessPal — ще один сайт на твоїй карті сліду, іноді для сервісу, який відтоді закритися.
- Це натякає на час. Злом має дату, яка каже тобі, що акаунт існував *до того часу*. Це накидає грубу хронологію онлайн-життя людини.

Межа діє й тут. Перевірка *відкритого сліду* — «так, у цих зломах» — це публічне знання про публічну подію, тож це безпечно. Читати чи використовувати злиті паролі за ним — це ті двері, які ти вже знаєш, що ніколи не відчиняєш.

Дані зломів також *брудні*. Зливи маркують неправильно. Старі дані переробляють і перепродають під новими назвами. Тож стався до будь-якого влучання в зломі як до зачіпки, а не факту. Воно вказує тобі кудись. Саме собою

воно нічого не доводить.

А ось частина, яку новачки розуміють неправильно, тож вивчи її раз і носи всюди: нульовий результат не означає, що адреса безпечна, фейкова чи невживана. Він означає, що інструмент не проіндексував злом, який її містить — не більше. Купа справжніх, активно вживаних адрес повертаються порожніми: їхні зломи так і не додали, або адреса новіша за зливи. «Нуль зломів» читається як *тут не знайдено*, ніколи як *чисто* — відсутність позитиву, а не присутність негативу. Стався до цього як до маленького поштовху, ніколи як до вироку.

Ось як ці перевірки насправді виглядають на екрані — одне влучання, одне порожнє:

```
t.orsini@northvale-labs.com
Breaches: 1 (PixelForge Design, 2019)
Pastes: 0
---
info@northvale-labs.com
Breaches: 0 Pastes: 0
"0" != "safe" -- може бути просто непроіндексовано
```

*Перевірка злomu каже тобі, де і приблизно коли
хтось мав акаунти. Вона ніколи не дає тобі дозволу
відчинити хоч один.*

Метод 4 — Півот через Gravatar

Є маловідомий трюк, який відчувається як магія, коли спрацьовує вперше.

Є сервіс під назвою **Gravatar** — скорочення від «globally recognized avatar» (глобально впізнаваний аватар). *Аватар* — це просто маленька картинка профілю поруч із твоїм іменем. Багато сайтів (секції коментарів, сайти для розробників, блоги) використовують Gravatar, щоб одне фото ходило за тобою всюди. Ти встановлюєш його раз, і воно з'являється на всіх них.

А ось особливість, якою можна скористатися. Gravatar прив'язує твоє фото — а іноді й цілий маленький профіль — до твого email. Тож якщо маєш чийсь email, ти можеш іноді витягти назад його фото, обраний нікнейм, справжнє ім'я, місцезнаходження й посилання на його інші акаунти. З нічого, крім рядка email.

Тобі не треба розуміти математику, щоб цим користуватися. Простими словами: береш email у нижньому регістрі, проганяєш через стандартний відбиток (званий хеш — код фіксованої довжини, зроблений з тексту) і запитуєш публічну адресу Gravatar по картинку й профіль, що збігаються. Багато інструментів роблять цей крок за тебе, тож ти просто вставляєш email і читаєш результат.

Що отримуєш, коли спрацьовує: обличчя до імені, нікнейм, щоб згодувати у свої інші пошуки, а іноді й

місцезнаходження. Не в кожного є Gravatar, і багато хто ставить лише фото. Але коли влучає, влучає сильно — фото й нікнейм з одного email — це чудова нитка, щоб потягнути.

Метод 5 — Півот: email на нікнейм на ім'я і назад

Усе вище має одну форму. Ти починаєш з одного шматка інформації, і він вручає тобі інший, який вручає ще один. Це називається півот — розгойдування від одного факту до наступного, наче переходиш річку камінь за каменем.

Три камені, між якими ти стрибатимеш найчастіше, — це email, нікнейм і ім'я. Ось як вони живлять одне одного:

- Email → нікнейм. Перевірка злому чи профіль Gravatar вручає тобі нікнейм, який людина любить використовувати, скажімо jkaras_dev.
- Нікнейм → ім'я. Ти шукаєш цей нікнейм по соцсайтах і форумах (для цього є цілі інструменти, розглянуті в іншому розділі) і знаходиш профіль, що показує справжнє ім'я: Jason Karas.
- Ім'я → email. Тепер ти застосовуєш трюк із шаблоном компанії з Методу 2 і передбачаєш jason.karas@brightmail.com — і підтверджуєш, що він існує, лагідною перевіркою «забули пароль» з Методу 1.

Бачиш коло? Кожен факт затуляє картину навколо наступного. Це справжнє серцебиття OSINT. Жоден окремий пошук не «розв'язує» людину. Ти будуєш її, один

підтверджений камінь за раз, звіряючи кожен новий факт з іншим джерелом, перш ніж довіритися.

Розібрана справа: один email відкриває картину

Ось усе це як одна маленька, *вигадана* історія. Кожне ім'я й адреса тут вигадані — іди за ходами, а не за деталями.

Тобі вручають одну email-адресу: t.orsini@northvale-labs.com.

Це все. Твоя робота — з'ясувати, хто це.

- Крок 1 — Прочитай саму адресу. Перш ніж будь-який інструмент, просто подивися. Домен — northvale-labs.com, компанія. Локальна частина — [t.orsini](mailto:t.orsini@northvale-labs.com), що пахне шаблоном [f.last](mailto:f.last@northvale-labs.com) — перша літера імені [t](mailto:t.orsini@northvale-labs.com), прізвище [orsini](mailto:t.orsini@northvale-labs.com). Тож ти шукаєш когось на ім'я Т-щось Orsini в Northvale Labs — слабке прочитання поки що, але безкоштовне, і ти дістав його просто подивившись.
- Крок 2 — Склади карту сліду. Ти проганяєш email через лагідну перевірку «забули пароль» по поширених сайтах, використовуючи метод з раніше. Сайт хостингу коду каже «ми надіслали посилання для скидання» — чисте «так, існує». Але професійна мережа дає тобі *те саме ввічливе повідомлення, хоч би що ти вбив*: «якщо акаунт існує, ми надішлемо посилання на пошту». Це навмисно. Багато великих сайтів тепер приховують диференціал саме для того, щоб люди не могли робити те, що ти робиш. Тож ти не можеш зробити висновок «вона в цій мережі». Ти позначаєш це *невідомо*, а не *так* —

жодного перерахування повідомлення, яке сайт сконструював, щоб не сказати тобі нічого.

- Крок 3 — Перевір відкритий слід. Ти шукаєш email на Have I Been Pwned. Він з'являється в одному зломі, від сервісу дизайн-інструментів, датованому кількома роками тому (рядок PixelForge Design, 2019 у боксі вище). Це підтверджує старий акаунт деінде й грубо датує їхнє онлайн-життя. Ти записуєш це як *зачіпку* — не більше. Ти не йдеш шукати жодного пароля. За звичкою ти також перевіряєш загальну info@northvale-labs.com компанії — і вона повертається нуль зломів, нуль публічних вставок (*pastes*). Ти позначаєш це як не-результат, а не як довідку про чистоту — знову: порожнеча не «чисто».

- Крок 4 — Спробуй півот через Gravatar. Ти згодуєш email у пошук Gravatar. Повертається профіль: фото, нікнейм *torsini* і вказане місто. Тепер ти маєш обличчя й нік з однієї адреси.

- Крок 5 — Півот нікнейма на ім'я. Ти береш email у лапки й шукаєш: "t.orsini@northvale-labs.com". Перша сторінка — здебільшого шум: ті сірі сайти «пошук за email» і «знайти будь-кого», що зішкрябують адресу, обгортають її в рекламу й не знають нічого, чого не знаєш ти. Ти пропускаєш кожен з них; це сміття, вбране як результати. Під шумом сидить одне справжнє влучання: список учасників конференції (публічний PDF), що називає *Teresa Orsini*, Northvale Labs. Тоді ти робиш півот

на нік натомість — *torsini* по соц- і форум-сайтах — і другий профіль підтверджує те саме ім'я й роботодавця. Два незалежні джерела, тож тепер ти віриш. Це збігається з твоїм здогадом з Кроку 1. Камені з'єднуються.

- Крок 6 — Підтверди шаблон. Просто щоб бути певним рецепту, ти знаходиш одну *іншу* адресу Northvale Labs у публічному PDF на їхньому сайті:

m.dubois@northvale-labs.com. Та сама форма *f.last*. Тож шаблон компанії підтверджено, і *t.orsini@northvale-labs.com* акуратно сидить усередині нього — твій початковий email перевірено з другого напрямку.

- Заминка, що не розв'язується. На тій самій сторінці ти також помітив *orders@northvale-labs.com* і *orsini.family@example-mail.com*. Жодна з них не належить *одній* людині. Перша — рольова скринька (*role mailbox*), спільна скринька, яку читає ціла команда. Друга — сімейний акаунт, спільний для пари чи родини. Прожени її через Gravatar і отримай назад одне фото — чиє це обличчя? Ти не можеш сказати. Це може бути Teresa, партнер чи доросла дитина, що завела акаунт роками тому. Адреса відображає *домогосподарство*, а не *людину*, і жодна кількість півотів не розділить це назад. Тож ти записуєш те, що чесно правдиве, і не більше: *спільна адреса — може бути власником чи членом родини — звідси розділити неможливо*. Ось де ця нитка закінчується. Не

чиста відповідь. Часткова, позначена як часткова.

З одного рядка тексту ти тепер маєш ім'я, обличчя, місто, роботодавця, грубу хронологію й два підтверджені акаунти — плюс один канал, позначений *невідомо*, і дві адреси, які ти відмовився приписати одній людині. Кожен крок публічний, кожен крок лагідний, жодного разу не торкаючись акаунта. Деякі з твоїх найгостріших ходів були тими, де ти *не* робив висновку: прихований диференціал, порожній злом, спільна скринька.

Негативний чи неоднозначний результат — це справжні дані. «Невідомо», записане чесно, б'є «так», угадане неправильно, щоразу.

Вправа: перевір власний відкритий слід

Зроби це на власному email — тому, що належить тобі. Це найбезпечніша можлива практика, бо ти сам об'єкт і маєш повне право.

1. Відкрий Have I Been Pwned у своєму браузері. 2. Вбий власну email-адресу й запусти перевірку. 3. Прочитай список зломів, з яким вона повертається. Для кожного помічай дві речі: *який сервіс* злили і *якого року*. 4. Напиши собі коротку хронологію: «Я мав акаунт на X до року Y». Зверни увагу, скільки твоєї власної онлайн-історії це накидає — з однієї адреси. 5. Як бонус, подивися, *який вид* даних оприлюднив кожен злом (деякі перелічують «passwords», деякі «dates of

birth»). Якщо якийсь злом оприлюднив пароль, яким ти досі десь користуєшся, — піди зміни його. Ти щойно перетворив урок OSINT на справжній самозахист.

Посидь із тим, скільки відкрив твій єдиний email. Це відчуття — «ого, усе пов'язане з цією однією річчю» — саме те, що ти тепер розумієш про email кожного іншого. Використовуй це обережно.

Підсумок

- Email-адреса — головний ключ, бо вона *стабільна й унікальна* — одна людина тримає її роками, тож вона тихо зв'язується з усім, де вона зареєструвалася, її справжнім іменем, фото й онлайн-історією.
- Ключові ходи лагідні й публічні: склади карту, де використовується email, за допомогою розкриття «забули пароль», вирахуй шаблон email компанії з однієї підтвердженої адреси, перевір *відкритий слід* злому на сервісі на кшталт Have I Been Pwned, спробуй фото-півот через Gravatar і розгойдайся між email, нікнеймом та ім'ям.
- Ніколи не переступай межу, яку ти встановив на початку: підтверди, що акаунт існує, і прочитай те, що сайт пропонує добровільно, тоді зупинися. Входити, вгадувати чи використовувати злитий пароль — це не OSINT, це злочин.

- Факти живлять одне одного: email, нікнейм та ім'я утворюють коло, і кожен новий факт вартий довіри лише тоді, коли друге джерело його підтвердить. Рольова скринька чи сімейна адреса відображає групу, а не людину — запиши те, що чесно правдиве, і не більше.
«Невідомо», записане чесно, б'є «так», досягнуте неправильно.

Оберни це проти себе. Перекрий цей півот на собі: використовуй унікальну адресу (чи псевдонім) на кожен сайт, увімкни двофакторну автентифікацію й не використовуй повторно один email як свій нікнейм усюди. Дивись Додаток D («Поверни собі контроль»).

РОЗДІЛ СЬОМИЙ

Номери телефонів

Особистий якір

Візьми на секунду власний номер телефону.

Він у тебе вже роками. Можливо, вже десятиліття. Ти дав його своєму банку. Ти дав його своєму лікарю. Ти вписав його в заявку на роботу. Ти набрав його в застосунку доставки їжі о 2-й ночі. Ти зберіг його в сотні телефонів друзів під своїм іменем.

Номер телефону — це один із найбільш особистих і найбільш стабільних слідів, які людина залишає по собі. Люди змінюють пошту. Люди видаляють старі акаунти в соцмережах. Але більшість людей тримає той самий номер телефону дуже довго. Саме тому я називаю його *особистим якорем*. Він утримує людину на місці.

Цей розділ — про те, як читати номер телефону і як безпечно побачити, що публічно з ним пов'язано. Ми рухатимемося повільно, і кожен термін пояснюється тієї ж миті, коли з'являється. Залишайся спокійним і обережним увесь шлях: номер телефону — це не просто дані. Він належить справжній людині.

Що таке номер телефону насправді

Спершу проясню одну заплутану річ.

Не існує єдиної офіційної «зворотної телефонної книги» на весь світ. Ти не можеш ввести номер в один чарівний сайт і отримати ім'я власника — перевірене й правдиве. Хто каже інакше, той щось продає, і часто продає крадені дані.

Те, що ми робимо насправді, менше й чесніше. Ми читаємо *структуру* номера. Ми перевіряємо, де він *з'являється* публічно. І ми перевіряємо, у яких *застосунках* цей номер зареєстровано. Кожне з цього — маленький слід. Ми складаємо сліди до купи. Оце і вся гра.

*Номер телефону — це зачіпка, ніколи не висновок.
Одне попадання кудись вказує. Саме по собі воно
нічого не доводить.*

Читаємо сам номер

Перш ніж щось шукати, ти читаєш номер. Ця частина цілком безпечна. Ти не торкаєшся жодної мережі. Ти нікого не пінгуєш. Ти просто дивишся на цифри так, як картограф дивиться на координати.

Спершу приведи номер до чистого міжнародного вигляду. Слідчі називають це E.164 — це просто назва стандартного формату. Виглядає він так:

+, потім код країни, потім решта номера, без пробілів і дефісів.

Наприклад, вигаданий номер зі США, записаний чисто, це +1 202 555 0134. Вигаданий номер зі Сполученого Королівства — +44 20 7946 0958. + означає «міжнародний». Перші цифри після нього говорять, яка це країна.

- Код країни — провідні цифри говорять, яка це держава. +1 — це США й Канада. +44 — Велика Британія. +380 — Україна. +49 — Німеччина. Це найкорисніша річ, яку ти дізнаєшся, бо вона говорить, *правила якої країни застосовуються* до всього, що ти робиш далі.
- Префікс зони чи регіону — наступний блок часто вказує на місто чи регіон, особливо для стаціонарних номерів (стаціонарний — це фіксований домашній чи офісний телефон, не мобільний). Для мобільних цей блок вказує на оператора, який *першим* видав номер.
- Тип лінії — багато безкоштовних інструментів також вгадають, мобільний це номер, стаціонарний чи VoIP. VoIP означає «голос через інтернет» — номер телефону, який живе в інтернеті, як Google Voice чи безкоштовний застосунок для повідомлень. Це дуже важливо. VoIP-номер дешевий і анонімний. Він не належить жодній фіксованій людині чи місцю. Якщо номер, який видає себе за чийсь особистий мобільний, виявляється VoIP, будь особливо обережним.

Тут є одна пастка, про яку я мушу попередити тебе одразу.

Оператор, якого показує інструмент, зазвичай початковий — компанія, яка вперше видала номер. Але люди можуть *зберегти свій номер і змінити компанію*. Це називається **переносимість номера**. Тож номер може казати «Оператор Х», хоча людина насправді роками тому перейшла до Оператора Y. Ніколи не записуй «ця людина користується Оператором Х» лише зі статичного читання. Це слабкий висновок, а не факт. Це єдине місце в книзі, за яким закріплена переносимість — коли вона зринатиме далі, я просто вказуватиму сюди.

Офлайн-читання номера говорить тобі країну, регіон і тип лінії. Воно ніколи не говорить, хто теперішній власник.

Інструменти для цієї частини з'являються й зникають, і їхні назви зміняться після того, як цю книгу надрукують — більшість обгортає той самий рушій з відкритим кодом, що валідуює номери. Не запам'ятовуй жодного інструмента. Пам'ятай *кроки*: приведи до +код країни номер, потім читай країну, регіон і тип лінії.

Дивимось, з чим номер публічно пов'язаний
Тепер ідемо шукати. Безпечно.

Пошук номера в лапках по всьому вебу

Це найпростіший хід, і часто це найшвидший шлях від голого номера до справжнього імені чи бізнесу. Люди викладають свій номер по всьому відкритому вебу — в оголошеннях, бізнес-каталогах, підписах на форумах, старих резюме, дописах на маркетплейсах.

Введи номер у пошуковик у лапках. Лапки кажуть пошуковик: «знайди саме це». Тож ти шукаєш "555 0134".

Ось важлива частина. Люди записують свій номер десятком різних способів. Тож ти теж шукаєш його кількома різними способами:

- З кодом країни: "+1 202 555 0134"
- У локальному стилі: "(555) 0134"
- З дефісами: "555-0134"
- З пробілами чи крапками

Якийсь один формат влучить у сторінку, яку решта пропустить. Коли ти знаходиш сторінку, де вказано номер, поруч із ним майже завжди вказано щось *іще* — ім'я, пошту, крамницю, нікнейм. Цей сусід — твій наступний крок.

Спробуй більш ніж один пошуковик. Google — це не весь інтернет. Bing і Yandex індексують різні регіональні сторінки. Для номерів зі Східної Європи й довколишнього регіону Yandex часто сильніший.

Пастка тут: повторне використання номерів. Номери телефонів переробляють. Коли людина покидає номер, оператор пізніше віддає його комусь новому. Тож стара сторінка може показувати *попереднього* власника. А бізнеси часто ділять один номер між багатьма співробітниками. Ніколи не припускай, що сторінка й людина — ідеальний збіг. Шукай друге джерело, що погоджується.

Краудсорсні застосунки «хто мені дзвонив»

Ти напевно бачив застосунки, що обіцяють сказати, хто тобі телефонує. Truecaller, GetContact і подібні застосунки — відомі приклади. Ось як саме вони працюють, бо розуміння цього вбереже тебе від великої помилки.

Ці застосунки не мають таємного офіційного довідника. Вони показують, як інші люди зберегли цей номер у власних телефонах. Коли багато користувачів дозволяють застосунку читати їхній список контактів, застосунок дізнається, що безліч людей зберегли +1 202 555 0134 як, скажімо, «Mike Plumber». Тож коли ти пробиваєш номер, він показує «Mike Plumber».

Ці застосунки ріжуть в обидва боки. Тієї миті, коли ти встановлюєш такий і даєш йому читати контакти, ти віддаєш усіх у своєму телефоні — а твій власний номер стає доступним для пошуку іншим.

Іноді це справді корисно. Один застосунок, GetContact, цікавий тим, що показує тобі *кілька* імен, які різні люди зберегли для одного номера. Ти можеш побачити «Mike Plumber», «Mike Landlord» і «SPAM». Цей кластер імен — маленька історія. Він розповідає про ролі людини й про те, як її бачать інші, а не просто дає одну наліпку.

Але тепер попередження, і це найважливіше попередження в усьому розділі.

*Краудсорсні застосунки з іменами тих, хто
дзвонить, можуть брехати, і брешуть постійно.
Ім'я в такому застосунку — це чулка, а не факт.*

Чому вони можуть брехати? Бо імена вписують випадкові незнайомці. Хтось може зберегти твій номер під жартівливим ім'ям. Хтось може зберегти його неправильно. Старий контакт може роками бути неактуальним. Номер міг змінити власника. Застосунок просто повторює те, що люди вписали. Слідчі спільноти на кшталт Bellingcat наголошують, що точність таких імен непостійна й залежить від того, як номер виглядає в чужих телефонних книгах.

Тож стався до кожного повернутого імені як до *окремого маленького сліду*. Ім'я означає набагато більше, якщо воно з'являється незалежно у двох різних застосунках чи джерелах. Одне ім'я з одного застосунку не доводить нічого.

Ще одне, для твоєї власної безпеки. Багато цих застосунків тихо вивантажують *твій* список контактів, коли ти ними користуєшся. Якщо ти когось пробиваєш, ти можеш віддати номери всіх своїх друзів, і сам можеш стати доступним для пошуку.

Найсильніший хід для новачка: номер → месенджер → нікнейм

Тепер я навчу тебе найпродуктивнішого шляху в роботі з номерами. Це хід, який перетворює самотній номер на справжній слід.

Ось основна ідея, простими словами.

Номер телефону часто є *ключем* до акаунта в месенджері. Месенджери на кшталт WhatsApp, Telegram, Signal і Viber дозволяють знаходити людей за номером телефону — це нормальна вбудована функція, щоб друзі могли знаходити одне одного. Коли ти перевіряєш номер в одному з цих застосунків, ти можеш побачити **профіль**: фото, відображуване ім'я, короткий опис, а іноді й **нікнейм**.

Цей нікнейм — скарб.

Бо щойно в тебе є нікнейм, ти знову на знайомій території. У попередньому розділі ми дізналися, що люди повторно використовують той самий нікнейм на багатьох сайтах. Тож нікнейм, який ти витягнув із месенджера, стає пошуком,

який можна запустити всюди інде. Ланцюжок виглядає так:
номер → профіль у месенджері → нікнейм → решта
онлайн-життя цієї людини.

З усіх шляхів у цьому розділі Telegram часто найбагатший, бо він може показати справжній @username, навіть коли ховає сам номер телефону. А @username — це саме той тип сліду, який робить півот через увесь веб.

М'яка, але тверда загорода. Перевірка номера в месенджері зазвичай означає збереження його як контакту, а збереження контакту може сповістити людину — вона може побачити, як з'являється новий контакт, або ти можеш зринутися в її списку «контакти, що приєдналися». Тож, як розглядалося в розділі 3, роби це з чистого дослідницького акаунта, ніколи не зі свого. І пам'ятай про налаштування приватності: якщо хтось поставив у застосунку «ніхто не може знайти мене за номером», перевірка просто нічого не дасть. Це нормально.

Номер часто відмикає нікнейм у месенджері.

Нікнейм відмикає все, що ти вже вмієш шукати.

Розібраний кейс: від номера до імені

Пройдімо один вигаданий приклад, від початку до кінця, щоб ти побачив, як складаються сліди. Кожне ім'я й номер тут вигадані.

Ти намагаєшся встановити, хто розмістив підозріле оголошення «продам авто». Єдина контактна деталь в оголошенні — номер телефону: +1 202 555 0177.

- Крок 1 — Прочитай номер офлайн. Ти приводиш його до +1 202 555 0177. +1 говорить тобі, що це номер зі США чи Канади. Безкоштовний офлайн-парсер дає тобі ось це:

```
+1 202 555 0177
valid:      yes
line type:  mobile
region:     Washington DC (origin only)
carrier:    "Verizon" (original issuer)
```

Офлайн-парсер повертає лише ці чотири речі — країну, регіон, тип лінії, початкового оператора — ніколи ім'я. Регіон — це лише те, де номер *народився*, а не де людина живе тепер. І застосовується засторога про оператора: це *початковий* видавець, тож ти ніде не пишеш «користується Verizon». Записуй лише те, що безпечно: «країна = США, мобільний, регіон = походження, а не дім, оператор = ненадійно (переносимість)». Тепер ти знаєш, на веб і пошуковики якої країни спиратися.

- Крок 2 — Пошукай номер у лапках. Ти шукаєш "202-555-0177", потім "+1 202 555 0177", потім "(202) 555-0177" більш ніж в одному пошуковнику. Версія з дефісами влучає в старий допис на хобі-форумі, де користувач підписався цим номером і нікнеймом

desertdrew. Цікаво. Але це одна сторінка, тож це лише слабка зачіпка. (Якби парсер позначив це як VoIP — номер Google Voice чи безкоштовного застосунку — він не розмістив би *нікого* ніде: ані домашнього регіону, ані справжнього оператора. Ти оцінив би весь ракурс локації як слабкий і не будував би на ньому. Мертвий сигнал — це нормально; вдавати, що він сильний, — ні.)

• Крок 3 — Перевір краудсорсні застосунки з іменами, обережно. Ось де перший застосунок намагається тебе обдурити. Він повертає одне гучне ім'я:

```
+1 202 555 0177  
saved by others as: "Mike Plumber"  
(crowd label from strangers' address books)
```

Якби ти був недбалий, ти написав би «продавець — це Mike Plumber, сантехнік» і пішов би додому з помилкою. Але стій. Одне краудсорсне ім'я саме по собі слабке — чутка, вписана незнайомцями, а не факт. «Mike Plumber» узагалі не збігається з форумним нікнеймом desertdrew.

Найімовірніше, номер переробили, і «Mike Plumber» — це попередній власник, який досі живе в адресних книгах незнайомців роками після того, як він покинув номер, — класична неправильна відповідь, яку наївний читач приймає й на цьому зупиняється. Тож ти тримаєш «Mike Plumber» як слабку, ймовірно мертву зачіпку. Потім ти перевіряєш *другий* застосунок: він повертає «Drew» і «Drew

Marketplace». Третій застосунок теж повертає «Drew».

Тепер *два незалежні застосунки* погоджуються на «Drew», і це збігається з форумним нікнеймом *desertdrew*.

Підтвердження піднімає «Drew» зі слабкого до помірного — але лише тому, що ти відмовився довіряти першому самотньому імені.

- **Крок 4 — Перевір месенджери.** Ти зберігаєш номер як контакт і відкриваєш Telegram. За ним стоїть акаунт, де показано фото, відображуване ім'я «Drew» і нікнейм *@desertdrew*. Обережно тут — власник *сам задав* це ім'я й нікнейм, тож вони не є незалежним джерелом. Одна й та сама людина контролює і номер, і ім'я; самообране ім'я лише підтверджує, що цей акаунт використовує нікнейм *desertdrew*, воно не може підтвердити, хто ця людина.

Тож це не піднімає «Drew». Воно лишається на помірному, утримуване там двома незалежними застосунками й форумним дописом — джерелами, які власник не писав.

- **Крок 5 — Зроби півот на нікнеймі.** Ти береш *@desertdrew* і шукаєш його на інших платформах, точно як ми практикували в розділі про нікнейми. Він з'являється на сайті обміну фото й сайті відгуків, обидва під тим самим нікнеймом, обидва показують те саме середнє за розміром місто зі США з Кроку 1. *Ці* — незалежні: власник не контролював, що каже сайт відгуків чи чиясь чужа сторінка — і їхня згода — це те, що нарешті піднімає

«Drew» до сильного. Тепер у тебе цілісна картина: одна людина, один нікнейм, один регіон, доступна за одним номером.

Зверни увагу, чого ти не робив. Ти не дзвонив людині. Ти не обманював сторінку входу. Ти не купував крадені дані. Ти прочитав публічну структуру, шукав публічні сторінки, скористався нормальною функцією застосунку й зробив півот на публічному нікнеймі — підтверджуючи кожну заціпку незалежним джерелом, перш ніж їй довіритися.

Один просунутий трюк, і чому новачкам його варто оминати

Ти з часом можеш прочитати про хитру техніку, де слідчий запускає процес «забув пароль» на сайті, бачить підказку на кшталт «ми надіслали код на номер, що закінчується на 77», і зшиває багато таких підказок з багатьох сайтів, щоб відновити повний прихований номер.

Я називаю її, щоб ти впізнав. Я також кажу тобі поки що її не чіпати.

Копирсання в живій системі входу чи відновлення акаунта, щоб вичавити з неї інформацію про акаунт, лежить у правовій сірій зоні. Залежно від твоєї країни й наміру, воно може порушити закони про зловживання комп'ютером і правила застосунку. Воно також може надіслати сигнал безпеки справжньому власнику. Це не поле для новачка. Як

слідчий базового рівня, ти дуже далеко заходиш безпечними кроками вище і ніколи не потребуєш його торкатися. Якщо твоя робота колись справді цього вимагатиме — це момент для навчання, письмового дозволу й ретельної юридичної перевірки, а не для цікавості.

Якщо техніка змушує тебе взаємодіяти з чиеюсь системою входу чи відновлення, стався до неї як до чутливої і відступи. Спершу основи.

Вправа: безпечно пробий власний номер

Найбезпечніший номер у світі для практики — твій власний. Ти вже знаєш про нього правду, тож можеш *оцінити* те, що тобі кажуть інструменти. Це робить його ідеальним учителем.

Зроби ось що:

- Запиши свій номер у E.164. Приведи його до форми + код країни номер, без пробілів і дефісів. Переконайся, що правильно вгадав код країни.
- Прочитай його офлайн. Скористайся будь-яким безкоштовним читачем номерів, щоб перевірити країну, регіон і тип лінії. Це відповідає реальності? Якщо він вказує оператора, зверни увагу, це твій *теперішній* оператор чи старий — так ти відчуваєш переносимість власними очима.

- Пошукай його в лапках. Пошукай власний номер у кількох різних форматах, більш ніж в одному пошуковику. Де він з'являється? Ти можеш здивуватися, що є публічним. Усе, що ти знайдеш, зможе знайти й той, хто розслідує тебе.
- Перевір застосунків із іменами тих, хто дзвонить. Пробий себе в одному краудсорсному застосунку. Яке ім'я повертається? Воно правильне, неправильне, смішне чи порожнє? Посидь із думкою, наскільки *ненадійне* воно навіть для номера, який ти знаєш досконало.
- Напиши два-три речення про те, що було точним, що неправильним, і що здивувало.

Ця рефлексія і є справжнім уроком. Відчути, як інструменти помиляються щодо *тебе*, — найшвидший спосіб навчитися ніколи не довіряти їм наосліп щодо незнайомця.

Підсумок

- Номер телефону — це особистий, довготривалий якір. Ти читаєш його структуру офлайн (країна, регіон, тип лінії), шукаєш його в лапках у кількох форматах у кількох пошуковиках і перевіряєш, у яких застосунках він зареєстрований — кожне попадання є зачіпкою для підтвердження, ніколи не фактом.
- Краудсорсні застосунки «хто мені дзвонив» показують, як незнайомці зберегли номер, тож вони легко помиляються й легко підробляються. Ім'я враховується

лише тоді, коли погоджуються два незалежні джерела.

- Найсильніший хід для новачка — номер → профіль у месенджері → нікнейм, бо нікнейм повертає тебе в крос-платформний пошук, який ти вже знаєш. Роби це з чистого дослідницького акаунта, а трюки з входом-і-відновленням облиш як правову сіру зону.

Оберни це проти загрози

Усе в цьому розділі можна спрямувати на *тебе*. Вимкни «знайти мене за номером» у своїх соцзастосунках і месенджерах, видали будь-які застосунки з іменами тих, хто дзвонить — вони вивантажують твої контакти й роблять тебе доступним для пошуку — і розглянь окремий номер для реєстрацій. Додаток D (Поверни собі контроль) проводить через це.

Твоє перше справжнє розслідування

Складаємо все докупи

Це останній розділ книги. Тож зробимо те, заради чого була вся книга.

Ми проведемо одне справжнє розслідування, від початку до кінця. Одна зачіпка на вході. Один чесний маленький звіт на виході. Усе, що ти вивчив у попередніх розділах, тут знадобиться — навички пошуку, полювання на нікнейми, перевірки пошти, перевірки телефонів, шкала впевненості, звички OPSEC і етична межа, яку ти не переступаєш.

Я вигадав увесь цей кейс. Кожне ім'я, нікнейм, пошта й номер телефону нижче вигадані для навчання. Жоден із них не є справжньою людиною. Але *метод* — це точно те, як працює професіонал. Іди слідом повільно. Не поспішай до відповіді. У цій роботі те, як ти туди дістаєшся, важить не менше, ніж те, де ти опиняєшся.

Одна річ перед тим, як почнемо. Тримай нотатки відкритими весь час. Порожнього текстового файла достатньо. Записуй, що ти шукав, що знайшов, коли знайшов і *як* знайшов. Якщо ти не можеш простежити висновок

назад до нотатки, ти не зможеш його потім захистити. Тож ми ведемо нотатки з найпершого кліку.

І одна звичка, що рятує кейси: захопи сторінку тієї миті, коли ти її бачиш. Вебсторінки змінюються і видаляються — часто саме цікаві, часто одразу після того, як ти їх знайшов. Тож коли щось важливе, зроби скріншот, скопіюй точну веб адресу і збережи сторінку в публічний вебархів, щоб була заморожена, датована копія, на яку ти зможеш послатися потім. Нотатка, що посилається на живу сторінку, надійна лише настільки, наскільки надійна ця сторінка завтра. Нотатка, що посилається на архівну копію, — це доказ.

Знахідка, яку ти не можеш простежити назад до нотатки, — це не знахідка. Це здогад.

Постановка

Ось наша зачіпка. Лише одна.

Невеликий онлайн-маркетплейс ручних виробів отримав скаргу. Продавець там, під назвою крамниці «pinewicketcrafts», узяв гроші за замовлення і зник. Ані доставки. Ані відповідей. Покупець ставить просте, справедливе питання: *чи є справжня людина за цією крамницею, і чи пов'язана ця крамниця з іншими крамницями, які, можливо, роблять те саме?*

А ось наша мета. Зверни увагу, яка вона вузька. Ми не «досліджуємо людину». У нас є чітке питання з відповіддю. Ця сфокусованість — це вся робота. Розмите питання змушує блукати вічно. Тісне питання каже тобі, коли зупинитися.

Запиши мету на початку нотаток, слово в слово:

Мета: Чи є справжня, знаходжувана людина за крамницею «pinewicketcrafts», і чи пов'язана ця крамниця з іншими акаунтами продавців?

Усе, що ми тепер робимо, служить цьому реченню.

Розслідування

- Крок 1 — Налаштуй чисте, тоді дивися, перш ніж торкатися. Перш ніж щось шукати, я відкриваю дослідницький браузер, не особистий. Я вийшов зі своїх акаунтів. Я не збираюся входити, комусь писати чи натискати «зв'язатися з продавцем». Це *пасивна* робота — я лише дивлюся на те, що вже публічне. Це правило захищає кейс і захищає мене. Тоді я пишу першу нотатку: дата, час, мета й єдине зерно, що в мене є — назва крамниці pinewicketcrafts.
- Крок 2 — Почни з найпростішого пошуку, що є. Я вводжу назву крамниці в пошуковик, у лапках, точно: "pinewicketcrafts". Лапки змушують точний збіг, тож я не отримую сторінки про сосни й крикет. Повертаються дві

речі. Перша — сама сторінка крамниці на маркетплейсі. Друга — крихітний результат із форуму рукоділля, де хтось дописав під тим самим ім'ям. Обидва йдуть у нотатки з повними вебадресами й часом, коли я їх побачив. Я поки що не довіряю жодному. Наразі це *зачіпки*, не більше.

- Крок 3 — Читай сторінку крамниці як документ, а не як історію. Сторінка крамниці мізерна, але й мізерні сторінки протікають. У розділі «Про нас» продавець написав один дружній рядок: *«Зроблено з любов'ю в майстерні Джорданом.»* Ім'я. Добре, але слабко — саме лише ім'я вказує на мільйони людей. Я також зауважую, що крамниця відкрилася вісім місяців тому й вказує загальний регіон, а не адресу. Я записую кожен факт і, що не менш важливо, записую, чого *бракує*: немає повного імені, немає телефону, немає пошти на сторінці. Негативні результати — це справжні результати. Вони показують, як далеко я подивився.

- Крок 4 — Зроби півот на нікнеймі. Ось перший справжній півот. Люди повторно використовують нікнейми. Те саме ім'я, яке вони обрали на одному сайті, вони часто обирали на ще десяти, бо його легко запам'ятати. Тож я беру pinewicketcrafts і перевіряю його на багатьох платформах. (У попередньому розділі ти бачив безкоштовні інструменти пошуку нікнеймів, що це роблять — вони просто питають кожен сайт: «чи існує тут

це ім'я?») Результат — не охайний список. Він ніколи такий не буває. Деякі сайти кажуть «не знайдено», один обмежує мене за частотою, один вантажить порожню сторінку, а два виходять за час очікування — інструмент прямо попереджає мене, які з них він не зміг прочитати:

```
enum v1.4 · 312 sites · 14:22
[*] pinewicketcrafts
[+] found marketplace.example/shop/pinewicketcrafts
[+] found woodcraft-forum.example/u/pinewicketcrafts
[+] found photos.example/pinewicketcrafts
[-] 404 github.example/pinewicketcrafts
[!] 429 reddit (rate-limited, retry later)
[?] 200? blogs.example (page loads but blank)
[!] timeout 2 sites unreachable
3 found · 1 not found · 4 unclear
```

Тож у мене немає «акаунтів». У мене є три *кандидати* і сліпа пляма — сайт, обмежений за частотою, порожня сторінка, що може бути будь-чим, і два, що вийшли за час очікування. Чотири сайти, які я насправді не зміг прочитати. Я записую цю сліпу пляму, бо прогалина, про яку я знаю, безпечніша за чистий на вигляд список, якому я надто довіряю. Те саме ім'я — це *зачіпка*, а не доказ. Ця обережність і є різницею між слідчим і чуткою.

- Крок 5 — Підтверди кожного кандидата й одного викинь. Тепер я відкриваю трьох кандидатів і дивлюся, замість того щоб рахувати імена. Двоє швидко вишиковуються: профіль на столярному форумі говорить про шпаківні, крамниця на маркетплейсі *продает* шпаківні,

той самий стиль фото, дати перетинаються. Добре — це два незалежні місця, що погоджуються. Але третій, фотоакаунт, неправильний. Я його майже взяв — нікнейм збігався точно. Тоді я його справді прочитав: це підліток, що викладає селфі зі спортзалу й фото кросівок, востаннє активний роками тому, нічого про дерево взагалі. Хтось інший ухопив те саме слово першим. *Той самий нікнейм, інша людина.* Я викреслюю його з нотаток і пишу чому: *«photos.example/pinewicketcrafts — ВІДХИЛЕНО, непричетна людина, немає ремісничого контенту, збіг лише за ім'ям.»* Це відхилення не марна робота. Це і є робота. На шкалі впевненості два незалежні збіги, що вижили після справжнього перегляду, б'ють три, які я ніколи не перевіряв. Тепер я ставлю це на щабель помірний — крамниця на маркетплейсі й столярний профіль, імовірно, одна людина — і тримаю двері відчиненими, бо мені досі бракує тих двох недосяжних сайтів.

- Крок 6 — Зроби півот від нікнейма до пошти. На хобі-столярному профілі, у публічному дописі з проханням поради, людина підписалася контактною адресою, щоб покупці могли зв'язатися: *jordan.pinewicket@example-mail.com.* Це дарунок, і він публічний, тож мені дозволено його зазначити. Новий ідентифікатор означає нові двері. Я запускаю безпечні, стандартні перевірки пошти, яких ти навчився раніше — не щоб кудись зламатися, а щоб побачити, що *публічно* з

нею пов'язано. Я перевіряю, чи адреса зринає у відомих публічних списках витоків (легітимний сервіс «чи була ця пошта у витокі»), і роблю простий пошук самої адреси в лапках. Ось що повертає перевірка витоків — і зверни увагу на другий рядок, бо я також пробив загальну контактну адресу крамниці для порівняння:

```
jordan.pinewicket@example-mail.com
Breaches: 2    (Collection-2019, ForumX-2021)
Pastes:  0
---
info@pinewicketcrafts.example
Breaches: 0    Pastes: 0    (no records)
note: "0" is not "clean" – may be unindexed
(2nd lookup delayed – rate-limited 6s)
```

Дві речі треба прочитати уважно. Особиста адреса існує вже роками й зринає в старих витоків — тож це справжня, вживана поштова скринька, а не одноразова, зроблена вчора. *Крамнична* адреса не повертає нічого — і, точно як попереджав розділ 6, порожньо не означає «чисто», лише неіндексовано. Я зазначаю це й рухаюся далі. Пошук у лапках тоді дає ще одну справжню річ: особиста пошта роками тому залишила публічний відгук на *другій* крамниці маркетплейсу, крамниці під назвою «oakwicketgoods».

- Крок 7 — Йди за новою зачіпкою, обережно. «oakwicketgoods». Інше слово, той самий дивний середній шматок — *wicket*. Це відлуння цікаве, але відлуння — не доказ. Я не оголошую крамниці

пов'язаними, бо дві назви римуються. Я йду й дивлюся. Друга крамниця тепер закрита, але її стара публічна сторінка досі вказує той самий регіон і ті самі фото шпаківень. Та сама пошта у відгуку. Те саме ремесло. Той самий стиль. Тепер це дві крамниці, пов'язані поштовою адресою й контентом, що збігається — справжнє підтвердження, а не здогад. Я записую це прямо: *два акаунти продавця, пов'язані однією публічною поштою й фото товарів, що збігаються; помірний, що це той самий оператор — поки що дві незалежні нитки, і нічого проти них.*

• Крок 8 — Зроби півот до телефону й прочитай його чесно. Стара сторінка «oakwicketgoods» мала ще один клаптик: публічний допис роками тому, де продавець пропонував номер телефону для локального самовивозу — +1 202 555 0147. Я запускаю *пасивні* перевірки телефону з попереднього розділу. І цей пошук — гарне нагадування, що номер бреше так само часто, як і говорить:

```
+1 202 555 0147
valid:      yes (format only, not assignment)
line type:  VoIP (not a home carrier)
region:     Washington DC (number's origin)
carrier:    virtual / app-based
```

Прочитай це й охолонь. VoIP-номер — це застосунок, а не поріг дому — його «регіон» — це те, де номер *народився*, а

не де спить його власник. Тож це не розміщує Джордана нікуди. Це слабкий сигнал, і я оцінюю його слабо. Для чого він *справді* добрий — так це для однієї речі: простий пошук номера дає ті самі цифри на обох сторінках крамниць — тож він стає третьою незалежною ниткою між ними й піднімає зв'язок крамниця-крамниця з помірного до сильного, і це все, що я йому дозволяю. Сам номер лишається слабким — як спосіб розмістити людину він нічого не вартий. Тоді той самий пошук тихо виносить на поверхню ще щось — особистий соцпрофіль, на ім'я «Jordan Alvarez», із домашніми фото, позначеним партнером і тим, що схоже на будинок та вулицю на задньому плані. Я зазначаю це прізвище, але не спираюся на нього: воно висить на цьому одному слабкому VoIP-номері, і більше ніщо його не підтвердило. Одна слабка зачіпка не заслуговує місця в моєму висновку — тож «Alvarez» лишається позначеним, як непідтверджене припущення, а моя знахідка тримається того, за що я можу поручитися: продавець, який зветься Джордан. І тут я зупиняюся.

- Крок 9 — Зупинися на межі, навмисно. Зверни увагу, що щойно сталося. Моє питання було про *продавця* й про те, чи пов'язані крамниці. Воно було не про дім людини, її партнера чи де вона спить уночі. Слід *міг би* тривати — я міг би спробувати встановити точну адресу, партнера, щоденний розпорядок. Я цього не роблю. Не тому, що не міг би, а тому, що *не повинен*. Той матеріал поза моєю

метою, він нав'язливий, і гонитва за ним перетворила б справедливе розслідування на стеження за приватним життям. Тож я пишу нотатку — чесну: *«Слід тягнувся до домашньої адреси й родини; зупинився тут. Поза сферою й нав'язливо. Не зібрано.»* Знати, де зупинитися, — не слабкість. Це вся причина, чому люди взагалі можуть довіряти цьому ремеслу.

Навичка, що робить тебе професіоналом, — це не те, як далеко ти можеш зайти. Це знання, де зупинитися — і запис того, що ти зупинився.

Тепер відступи й подивися, що ми насправді збудували — і що викинули. З однієї назви крамниці ми дійшли до імені, двох підтверджених акаунтів (після того, як відкинули третій, що був незнайомцем із тим самим нікнеймом), публічної пошти, другої пов'язаної крамниці й номера телефону, який ми оцінили слабо, але який усе одно зв'язав дві крамниці. Імовірно, один оператор, що зветься Джордан — із прізвиськом, що зринуло раз і лишається непідтвердженим. Кожен крок був маленьким, перевірюваним півотом. Кожну знахідку зважували на шкалі впевненості, перш ніж вона заслужила наступний крок — і відхилений акаунт та порожнеча «немає записів» є частиною сліду, а не соромом, схованим від нього. І ми провели чисту межу там, де закінчився суспільний інтерес і почалося приватне життя.

Це петля з найпершого розділу, запущена по-справжньому: відкритий слід (публічні клаптики, залишені онлайн) → півот (перетворити кожен клаптик на наступні двері) → атрибуція (обережне рішення, що це одна людина) — усе в межах правил.

Звіт

Знахідка, яку ніхто не може прочитати, — це знахідка, що не рахується. Тож ми її оформлюємо. Коротко, просто й чесно. Добрий звіт новачка відповідає на чотири речі: про що мене питали, що я знайшов, наскільки я впевнений і чого я *не* робив. Ось наш.

Кейс: запит щодо недоставки pinewicketcrafts >

Дата: (сьогоднішня дата) > Мета: Встановити, чи є справжня, знаходжувана людина за крамницею «pinewicketcrafts», і чи пов'язана вона з іншими акаунтами продавців.

Що я знайшов. Крамницю «pinewicketcrafts», схоже, веде справжня особа, яка зветься на ім'я Джордан. (Прізвище «Alvarez» зринуло з однієї слабкої телефонної зачіпки; я позначаю його як непідтверджене й *не* трактую як встановлене.) Продавець пов'язаний — на щаблі сильний — із другою, тепер закритою крамницею маркетплейсу «oakwicketgoods», і, на щаблі помірний, зі столярно-хобійним профілем. Зв'язки спираються на

спільну публічну поштову адресу (jordan.pinewicket@example-mail.com), фото товарів, що збігаються, і повторно використані контактні дані.

Що я виключив. Фотоакаунт з ідентичним нікнеймом «pinewicketcrafts» виявився належним *іншій, непричетній людині* (немає ремісничого контенту, збіг лише за ім'ям). Я його відхилив. Два сайти були недосяжні під час моєї перевірки нікнейма, тож моя картина неповна, і я це кажу.

Наскільки я впевнений і чому. Зв'язок крамниця-крамниця сильний; прив'язка до столярного профілю лише помірна; і це *не* підтверджено — хочу бути щодо цього чітким.

Висновок не спирається на жодну окрему зачіпку; він спирається на кілька незалежних публічних джерел, що погоджуються — ремесло й фото, що збігаються, і повторно використана пошта на двох крамницях. Номер телефону я оцінив слабо навмисно: це VoIP/застосунковий номер, тож він підтверджує зв'язок крамниць, але нікого нікуди не розміщує. Якби пошта виявилася спільною для двох людей, моя впевненість упала б, тож я позначаю це як точку, що змінила б картину.

Чого я не робив і чого не зміг підтвердити. Я не зв'язувався з продавцем чи будь-яким акаунтом. Я ніде не входив і не взаємодіяв — увесь збір був пасивним і з публічних сторінок. Я зупинився, коли слід повів до домашньої адреси й членів родини, бо це поза цим розслідуванням і нав'язливо. Я *не*

зміг підтвердити точну юридичну особу продавця чи намір; «зник із замовленням» — це те, що повідомляє покупець, і я не знайшов незалежного доказу шахрайства — лише те, що два акаунти пов'язані й оператор, імовірно, знаходжуваний. Ця різниця важлива: я звітую про зв'язки, які я перевірів, а не про злочин, який я довів.

Джерела. (Короткий пронумерований список кожної сторінки з її вебадресою й часом, коли я її переглядав — включно з пошуками, що нічого не дали, і акаунтом, який я перевірів і відхилив.)

Прочитай цей звіт ще раз і зверни увагу на його тон. Він ніколи не перепродає. Він каже, наскільки впевнений, а не просто що. Він визнає прогалини. Він показує межу, яку я відмовився переступати. Такий звіт — це те, що ти можеш передати іншій людині, і вона зможе перевірити кожен крок. Ось мета. Не звучати розумно — бути *перевірюваним*.

Пиши знахідки, а не вирoki. Кажу, наскільки ти впевнений, показуй джерела й визнавай, чого ти не робив.

Другий кейс: той, що не закривається

Хочу показати тобі ще один, і він найважливіший у книзі — бо він *провалюється*. Справжня робота робить це набагато частіше, ніж охайна історія вище, і новачок, який ніколи цього не бачить, думатиме, що зробив щось не так, коли це

трапиться з ним. Він не зробив. Іноді чесна відповідь — «я не можу сказати», і дійти до цієї відповіді чисто — це професійна навичка, а не провал.

Запит: покупець залишив на маркетплейсі захопливий відгук, що читається як фейковий, підписаний лише «Rae M.» — це справжній клієнт чи продавець, що хвалить власну крамницю? Один фрагмент імені, більше нічого.

Я опрацьовую його тим самим дисциплінованим способом. Пошук нікнейма гаєт дає два живі акаунти, що *обидва* пасують. Один — це Rae Molina, активна в тій самій ремісничій сцені, приблизно в правильному регіоні — правдоподібно. Інший — Rae Mercer, який раніше взаємодіяв саме з цим продавцем — теж правдоподібно. Дві справжні людини. Обидві можуть бути «Rae M.». Я намагаюся розбити нічию. Півот на пошту заходить у глухий кут: немає публічної адреси для жодного. Півот на фото заходить у глухий кут: у жодного профілю немає придатного зображення. Пошук у лапках «Rae M.» плюс назва крамниці не дає нічого нового. У мене два кандидати, кожен на щаблі слабкий, і *нічого, що піднімає одного над іншим*.

Тож я зупиняюся — і пишу чесний фінал:

Знахідка: Не вдалося атрибутувати. Дві правдоподібні особи («Rae Molina», «Rae Mercer») пасують фрагменту «Rae M.»; немає публічного

доказу, що їх розділяє. Впевненість: слабкий, розщеплений між двома кандидатами. Я не можу сказати, чи відгук справжній, чи написаний самим продавцем. Рекомендую не діяти на цьому, доки не з'явиться сильніший ідентифікатор.

Придивися до цього фіналу. Він прямо називає глухий кут. Він відмовляється обрати зручнішу відповідь лише щоб вручити комусь ім'я. Ця відмова і є знахідкою. Слідчий, який видавлює впевнену відповідь зі слабого доказу, не корисніший за того, хто каже «я не можу сказати» — він небезпечніший, бо хтось може діяти на здогаді.

«Я не зміг цього підтвердити» — це теж знахідка. Пиши її щоразу, коли це правда.

Ще одна нотатка, перш ніж ти підеш — хто є суб'єктом, змінює правила. Обидва кейси вище були споживчими сценаріями: продавець-шахрай, підозрілий відгук. Якщо ж ти колись робиш це, щоб перевірити кандидата на роботу чи працівника, зупинися й згадай врізку з розділу 2: вмикаються додаткові закони (FCRA, антидискримінаційні правила, згода на біометрію). У тому світі дисципліна набуває ще одного правила — ти зупиняєшся й не записуєш речі, що не стосуються справи роботи (чиясь релігія, здоров'я, вагітність) точно так, як ми зупинилися на домашній адресі Джордана тут. А для формальних рішень

про наймання ця робота часто має проходити через ліцензованого перевіряльника, а не аматора. Інший суб'єкт, додаткові правила. Знай, у якому світі ти перебуваєш, перш ніж почати.

Де вчитися далі

Ти закінчив основи. Тепер єдиний шлях уперед — повторення. Ось як отримати їх безпечно й безкоштовно.

Практикуй спершу на собі. Ти — єдиний суб'єкт, якого тобі завжди дозволено досліджувати повністю. Пошукай власне ім'я, власні старі нікнейми, власну пошту в перевіряльнику витоків. Це відкриває очі — і трохи некомфортно — побачити власний слід так, як його бачив би незнайомиць. Бонус: усе, що ти знайдеш, ти потім можеш *прибрати*. Найкращий урок OPSEC, що є.

Роби OSINT-челенджі й CTF. «CTF» означає capture the flag (захопи прапор) — гра, де ти розв'язуєш загадки, щоб знайти приховану відповідь. Є OSINT-орієнтовані, де ти геолокуєш фото чи відстежуєш фейкову персону по сайтах. Вони безпечні («цілі» вигадані для гри), вони оцінюються, і вони будують саме ті м'язи півоту з цього розділу. Пошукай OSINT-CTF для початківців і вікторини; багато безкоштовні й браузерні.

Спробуй наглядову подію з пошуку зниклих людей — обережно. Групи на кшталт Trace Labs проводять

«пошукові загони», де волонтери використовують OSINT, щоб допомогти знайти справжніх зниклих людей, працюючи суворо в межах закону й твердого правила «жодних контактів». Це справжня, значуща робота, але це *не* вільне поле для новачка: ти дотримуєшся їхнього гайду з OPSEC, використовуєш дослідницький акаунт і ніколи ні з ким не взаємодієш. Заходь скромно, спершу прочитай їхній гайд для учасника й учися в людей, які роблять це роками.

Читай авторитетні гайди, а не випадкові блоги. Кілька джерел довіряються по всьому полю — наприклад, набір інструментів для онлайн-розслідувань від Bellingcat і їхні гайди з верифікації для початківців. Вони написані людьми, які роблять це на життя, і обережні щодо закону й етики. Додай хороші в закладки. Повертайся до них.

Тримай звички, а не лише інструменти. Інструменти зміняться. З'являються нові сайти, старі вмирають, застосунки перейменовують щороку. *Процес* не змінюється. Тісне питання, нотатки з дії номер один, півот із дисципліною, зваж кожну знахідку на шкалі впевненості, зупинися на етичній межі, оформ чесно. Вивчи це, і будь-який новий інструмент — це просто нові двері для того самого методу.

Міст до другого тому

Ця книга була основами: петля, правила, точний пошук, нікнейми, пошта, телефон, шкала впевненості й ази того, як лишатися безпечним і етичним.

Другий том іде глибше. Ми серйозно візьмемося за OPSEC — справжні дослідницькі акаунти, ізольовані середовища й контроль того, що *ти* сам протікаєш, поки дивишся. Ми перейдемо до зображень і місць: зворотний пошук зображень, зроблений правильно, і геолокація — з'ясування, звідки знято фото, за тим, що є в кадрі. Ми будуватимемо таймлайни й карти зв'язків і навчимося структурованих способів, якими професіонали борються з власним упередженням, щоб їхні висновки трималися. Усе там стоїть на тому, що ти щойно тут відпрацював.

Наразі ти зробив те, заради чого була ця книга. Ти провів розслідування, від однієї маленької зачіпки до чесного звіту, і ти знав, де зупинитися. Це все ремесло в мініатюрі. Тримай нотатки. Лишайся допитливим. Лишайся добрим. І я побачу тебе в другому томі.

— Yehor

Вправа

Проведи власний крихітний кейс, на собі, використовуючи лише кроки з цього розділу.

- **Обери зерно.** Обери один старий нікнейм, яким ти користувався роками тому. Запиши його на початку свіжого файла нотаток, із сьогоднішньою датою й цією метою: *«Знайти, які публічні акаунти й інформація досі ведуть назад до цього мого старого нікнейма.»*
- **Пошукай його точно.** Введи нікнейм у лапках у пошуковик. Зазнач кожен результат із його вебадресою й часом, коли ти дивився.
- **Зроби півот на ньому по платформах.** Скористайся безкоштовним перевіряльником нікнеймів, щоб побачити, де це ім'я досі існує. Зазнач кожне попадання як *зачіпку*, а не доказ.
- **Підтверди або відхили.** Для кожного попадання виріши: це справді я чи хтось, хто обрав те саме ім'я? Запиши свої міркування й рівень впевненості для кожного.
- **Знайди власну межу.** У якийсь момент ти можеш знайти щось приватне — стару адресу, члена родини. Практикуй зупинку. Напиши нотатку: *«Дійшов до приватної інформації; зупинився; поза сферою.»*
- **Напиши чотиричастинний звіт.** Про що тебе питали, що ти знайшов, наскільки ти впевнений і чого ти не робив. Тримай його в межах однієї сторінки.

Тоді зроби корисне: прибери те, що знайшов. Це твоє перше справжнє розслідування і твоя перша справжня перемога

OPSEC.

Підсумок

- Однієї зачіпки достатньо, щоб почати — один публічний клаптик, опрацьований із тісним питанням і дисциплінованими півотами, може довести тебе аж до відповіді.
- Безлад — це робота, а не помилка — справжні сліди мають неправильні попадання, глухі кути, порожні результати й інструменти, що виходять за час очікування. Прогін без відхилених зачіпок — це не чистий прогін; це недбалий. Записуй, що ти викинув і чому.
- Зваж, перш ніж крокувати — кожна знахідка отримує щабель на шкалі (слабкий → помірний → сильний → підтверджено), і ти ніколи не будеш наступний крок на непідтвердженій зачіпці; лише кілька незалежних джерел, що погоджуються, заслуговують підтверджено.
- Звіт і межа — це ремесло — професіонал пише знахідки чесно (наскільки впевнений, які джерела, чого він *не* робив) і точно знає, де закінчується суспільний інтерес і починається приватне життя.

Епілог

Що ти вмієш тепер — і що буде далі.

Озирнися на те, з чого ти починав цю книгу.

Нікнейм був просто нікнеймом. Пошта була просто адресою. Номер телефону був просто цифрами. Тепер ти знаєш правду: кожне з них — це нитка, і ти вмієш її тягнути — обережно, за порядком, підтверджуючи по ходу.

Ти вивчив одну петлю, на якій тримається все ремесло — відкритий слід → півот → атрибуція. Ти вивчив правила, що тримають тебе професіоналом, а не проблемою. Ти навчився захищати себе, перш ніж дивитися на когось іще. Ти навчився шукати як той, хто знає, що робить, і перетворювати нікнейм, пошту чи номер телефону на початок справжньої, чесної картини.

Це фундамент. Усе попереду збудовано на ньому.

Чесна частина

Тебе спокушатиме, тепер, коли ти можеш бачити, бачити все. Опирайся цьому. Навичка, яку ти почав будувати, — це тиха сила, а тиху силу судять цілком за тим, як ти нею користуєшся. Дивися лише тоді, коли маєш добру причину. Підтверджуй, перш ніж робити висновок. І коли слід веде туди, де тобі нема чого робити — зупинися. Цей інстинкт,

більше за будь-яку техніку в цій книзі, і робить когось гідним довіри в цій роботі.

Куди ти йдеш далі

Наступне, що треба зробити, просте: практикуй. Запускай петлю на собі. Запускай її на речах, якими володієш. Коли будеш готовий до справжньої, керованої практики, OSINT-спільнота проводить відкриті челенджі й події — безпечні, легальні місця, щоб відточити все, що ти щойно вивчив. (Стартовий список знайдеш у додатку.)

Тоді, коли поодинокі зачіпки почнуть здаватися легкими, ти будеш готовий до другого тому — «Крос-платформна атрибуція», де одна нитка стає багатьма, і ти вчишся стежити за людиною по всіх місцях, де вона існує одночасно.

Ти прийшов, уміючи шукати. Ти йдеш, уміючи *розслідувати*.

Кожна тінь має ім'я. Тепер ти знаєш, як почати читати одну з них.

— Yehor Selin

Додаток

Глосарій, метод на одній сторінці й де практикувати.

А — Глосарій простими словами

- OSINT — з'ясування речей із використанням лише публічної, відкритої інформації.
- Відкритий слід (Exposure) — слід, який хтось залишив на видноті (нікнейм, фото, номер, допис).
- Півот (Pivot) — використання однієї зачіпки, щоб знайти наступну.
- Атрибуція — впевненість, що зачіпки вказують на одну справжню особу.
- Сокпапет (sock puppet) — чистий, окремий дослідницький акаунт, ніколи не твій справжній.
- OPSEC — захист себе під час роботи, щоб твій перегляд не лишав сліду.
- Дорк (Dork) — точний пошук із операторами (як лапки чи site:), щоб вибрати кращі результати.
- Метадані — прихована інформація всередині файла (наприклад, коли й іноді де зроблено фото).
- Шкала впевненості — наскільки ти впевнений, у чотирьох фіксованих словах, вживаних по всій цій книзі:

слабкий (одна непідтверджена зачіпка), помірний (дві незалежні зачіпки погоджуються), сильний (три або більше незалежних погоджуються, ніщо не суперечить), підтверджено (незалежно встановлено й перевірено).

В — Метод на одній сторінці

1. Почни з однієї зачіпки. Запиши точно, що в тебе є. 2. Постав маленьке питання. «Що ця одна річ може мені дати?» 3. Зроби півот. Перетвори кожную відповідь на наступне питання. 4. Піднімайся шкалою впевненості. Ніколи не роби висновок на одній зачіпці — підтверджуй двома-трьома незалежними. 5. Записуй по ходу. Зберігай, що знайшов і де знайшов — зроби скріншот і збережи копію у вебархів, перш ніж сторінка встигне змінитися. 6. Знай, коли зупинитися. Немає доброї причини чи переступаєш межу? Зупинися. І якщо доказ ніколи не проходить далі за слабкий, «не зміг підтвердити» — це справжня, чесна відповідь.

Відкритий слід → півот → атрибуція.

Підтверджуй, перш ніж робити висновок.

С — Де практикувати (безпечно й легально)

- Спершу дослідуй себе. Це єдина ціль, яку тобі завжди дозволено дослідити повністю.
- OSINT-челенджі й CTF. Спільнота проводить відкриті, легальні події-загадки, збудовані саме для

навчання цих навичок.

- Події з пошуку зниклих людей (як-от ті, що проводить Trace Labs) дозволяють практикувати заради справді доброї справи, поряд із досвідченими людьми.
- Публічні гайди з розслідувань від поважних команд (наприклад, набір інструментів і вправи від Bellincat) дають тобі справжні задачі для розв'язання.

Починай з малого, лишайся легальним і тримай метод перед очима. Майстерність приходить із повторень, а не з інструментів.

Нотатка про інструменти у вправах. Вони бувають двох форм. Деякі — звичайні вебсайти — ти просто відкриваєш їх у браузері й друкуєш. Інші (багато перевіряльників нікнеймів і поштові інструменти) — це маленькі безкоштовні програми, які ти встановлюєш, і деякі з них працюють у *терміналі* — текстовому вікні, де ти вводиш команди — а не з кнопками. Жодне не краще; у них просто різні заїзди. Якщо інструмент хоче термінал, а це для тебе нове, не дай цьому себе зупинити: почни з браузерного еквівалента, вивчи метод, а термінальні освой пізніше. І тобі ніколи не треба витратити ні копійки, щоб практикувати будь-що в цій книзі.

D — Поверни собі контроль: зменшуємо власний слід

Щойно ти дослідив себе, у тебе є мапа власного відкритого сліду. Тепер скористайся нею. Кожна техніка в цій книзі працює на клаптиках, які ти залишив на видноті — тож захист простий: лишай менше клаптиків і забери назад ті, які можеш. Працюй за цим списком за порядком; перші пункти дають найбільше захисту за найменше зусиль.

- **Зміни паролі, що витекли.** Прогони свої пошти через перевіряльник витоків (розділ 6). Для кожної адреси, що зринає у витоку, зміни цей пароль і кожне інше місце, де ти його повторно використав. Це найцінніша річ на сторінці.
- **Увімкни двофакторку всюди, де це важливо.** Спершу пошта, потім усе, де є гроші чи повідомлення. Код із застосунку кращий за код в SMS. Самого лише витеклого пароля перестає бути достатньо, щоб зайти.
- **Розірви ниточку нікнейма.** Ти бачив у розділі 5, як один повторно використаний нікнейм зв'язує всі твої акаунти. Для всього, що хочеш тримати окремо, використовуй інше ім'я. Спиши старі нікнейми, якими більше не користуєшся.
- **Закрий і видали мертві акаунти.** Форум, яким ти скористався раз у 2016-му, досі протікає. Якщо не користуватимешся ним знову, видали його — не просто покидай. Менше дверей, менше півотів.

- Вимкни «знайти мене за номером / поштою». У соцзастосунках і месенджерах вимкни налаштування, що дають незнайомцю знайти твій профіль за номером телефону чи поштою. Це вбиває телефонний півот із розділу 7.
- Видали застосунки з іменами контактів і відклич доступ до контактів. Ті застосунки визначення номера вивантажили всю твою адресну книгу — і зробили твій номер доступним для пошуку іншим. Прибери їх і відклич дозвіл на контакти в застосунків, яким він не потрібен.
- Знімай геолокацію й метадані перед публікацією. Фото можуть нести місце, де їх зроблено. Вимкни теги локації в камері й перевір налаштування приватності, що геотегують твої дописи.
- Замкни те, що бачать незнайомці. Постав старі дописи й фотоальбоми на «лише друзі». Переглянь «публічний» бік кожного профілю так, наче ти незнайомиць, що зазирає — бо хтось буде.
- Використовуй наявні шляхи видалення. Пошукай своє ім'я; де брокер даних чи сайт «пошуку людей» тебе вказує, у більшості є форма відмови чи видалення. Це нудно, але працює. Перевіряй наново кожні кілька місяців — деякі повертають тебе в список.

- Перевіряй себе за розкладом. Відкритий слід відростає. Запускай самодослідження з розділу 8 двічі на рік і прибирай усе нове.

Коли той, хто дивиться, уже знає тебе. Уся ця книга спирається на одну втіху — що незнайомець мусить *вгадувати*, чи два акаунти належать одній людині, а здогади можуть бути хибними. Ця втіха зникає, коли шукач — це той, хто вже знає твої старі нікнейми, твій номер, твою пошту, твоє обличчя й імена твоєї родини — колишній, сталкер, переслідувач. Для них захист «те саме ім'я не означає ту саму людину» не діє; у них є істина. Якщо це твоя ситуація, зрозумій дві важкі речі. По-перше, справжнє фото, яке ти вже виклав, чи родич, що тебе позначив, іноді не можна повністю «розвистежити» — чесним рішенням може бути зміна самого нікнейма, номера чи пошти, а не просто їх приховування. По-друге, це більше, ніж чек-лист. Звернися по спеціалізовану допомогу: гаряча лінія проти домашнього насильства, програма конфіденційності адреси чи місцева поліція — люди, які роблять саме це на життя.

Захист родини. Кожен півот у цій книзі працює й на твоїх дітях і партнері. Замкни акаунти неповнолітніх жорстко: приватні за замовчуванням, без тегів локації, без пошуку за номером чи поштою, і поговори з ними про те, що незнайомець може відновити з допису з надлишком інформації. Зроби самодослідження *на публічному сліді*

твоєї родини, обережно, і приборіть разом.

*Найкращий захист — це та сама навичка, що й
найкраще розслідування: знати точно, що ти
лишаєш на видноті — а тоді вирішити, навмисно,
що лишається.*

Е — Шаблони, які можна скопіювати

Кради їх. Встав у файл нотаток і заповни пропуски. Вони перетворюють звички з цієї книги на щось, що ти справді запускаєш.

Чотиричастинний звіт. Кожна знахідка, яку ти комусь вручаєш, лягає в цей скелет:

КЕЙС:	(один рядок — що це)
ДАТА:	(коли)
МЕТА:	(одне питання, одним реченням)
ЩО ЗНАЙШОВ:	(відповідь, прямо)
ВПЕВНЕНІСТЬ:	(щабель: слаб/помір/сильн/підтв + незалежні джерела, на яких стоїть)
ЩО ВИКЛЮЧИВ:	(зачіпки перевірені й відхилені, чому)
ЧОГО НЕ РОБИВ:	(межі, лінія зупинки, чого не зміг підтвердити)
ДЖЕРЕЛА:	(нумеровано: URL + дата/час + архівна копія — з глухими кутами)

Робоча нотатка (один рядок на крок). Тримай її відкритою з першого кліку:

ЧАС | ДІЯ | ФАКТ (що я бачив) |
ДУМКА (що я думаю) | ДЖЕРЕЛО + АРХІВ

Шпаргалка шкали впевненості. Ніколи не пиши висновок без щабля — і ось що саме заслуговує кожен:

- **слабкий** — одна зачіпка, непідтверджена (ім'я-збіг, одна краудсорсна наліпка, VoIP-номер). Зачіпка, ніколи не висновок.
- **помірний** — два *незалежні* джерела погоджуються (напр. контент + дати, або два окремі застосунки). «Незалежні» означає, що вони не могли просто скопіювати одне одного.
- **сильний** — три або більше незалежних джерел погоджуються, і ніщо їм не суперечить.
- **підтверджено** — незалежно встановлено, і інша людина може перевірити кожен крок наново й дійти тієї самої відповіді.

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