OSINT

ОСНОВИ ЗБОРУ РОЗВІДУВАЛЬНИХ ДАНИХ

- 1. Людські джерела інформації (HUMINT)
- Найстаріша форма збору розвідувальних даних, яка до технічної революції XX століття була основним методом розвідки.
- Особливості: Пряме спілкування з людьми, контроль теми обговорення та керування діями джерел.Доступ до інформації, яку неможливо отримати іншими способами.Приклад: Згідно з публікацією «Національна розвідка США. Огляд за 2013 рік», HUMINT є унікальним завдяки прямій взаємодії з джерелами.

2. ГЕОПРОСТОРОВА РОЗВІДКА (GEOINT)

- Використання та аналіз зображень і геопросторових даних для опису, оцінки та візуалізації фізичних об’єктів і діяльності з географічною прив’язкою.
- Компоненти GEOINT: Зображення (отримані з супутників, безпілотників, літаків-розвідників).Розвідка зображень (IMINT).
- Геопросторові дані (картографія, геодезія, дистанційне зондування).Інструменти: Географічні інформаційні системи (ГІС) для збору, обробки та візуалізації даних.
- Приклад використання: Геолокація користувачів соцмереж для створення карти переміщення біженців із Сирії.
- Примітка: Термін IMINT вважається застарілим, оскільки GEOINT охоплює ширший спектр даних, включаючи візуальну фотографію, радіолокаційні та інфрачервоні датчики, лазери й електрооптику.

3. ВЗАЄМОДІЯ ЕЛЕМЕНТІВ GEOINT

Ключові елементи:

- Зображення.
- Розвідка зображень (IMINT).
- Геопросторові дані.

Переваги: Поєднання цих елементів забезпечує комплексне розуміння оперативної обстановки та підтримку прийняття рішень.

Застосування: Збір, управління, аналіз, генерація, візуалізація та доставка геопросторової інформації.

4. РАДІОЕЛЕКТРОННА РОЗВІДКА

- Збір інформації за допомогою засобів зв’язку, радарів та вимірювальних приладів.
- Категорії:
- Комунікаційна розвідка (COMINT):
  - Перехоплення електромагнітних комунікацій (телефонні дзвінки, електронна пошта, миттєві повідомлення).
  - Аналіз трафіку (геопросторові метадані): ідентифікація сторін, визначення їхнього місця розташування, пристроїв, технічних параметрів.
- Радіотехнічна розвідка (ELINT): Збір даних із радарів та інших систем.

5. РОЗВІДКА ВИМІРЮВАНЬ І СИГНАТУР (MASINT)

- Науково-технічна розвідка, що аналізує фізичні атрибути цілей і подій для їхньої ідентифікації.
- Характеристики:
  - Кількісний і якісний аналіз даних, отриманих від приладів зондування.
  - Виявлення унікальних особливостей джерел, випромінювачів або відправників.
- Приклади:
  - Радіолокаційні сигнатури авіаційних систем.
  - Хімічний склад проб повітря або води.
- Значення: Забезпечує технічну розвідку для точної ідентифікації об’єктів і подій.

6. РОЗВІДКА ЗА ВІДКРИТИМИ ДЖЕРЕЛАМИ (OSINT)

- Розвідка за відкритими джерелами (OSINT) – це збір інформації з несекретних, загальнодоступних джерел.
- Значення: Є ключовим елементом збору розвідувальних даних.За оцінками, OSINT становить ~80% інформації для розвідувальних аналітиків і ~95% економічно значущої інформації.

КАТЕГОРІЇ OSINT

OSINT поділяється на чотири основні категорії:

- Широкодоступні дані та інформація: Загальнодоступні матеріали, які не мають обмежень.
- Цільові комерційні дані: Інформація, отримана з комерційних джерел.
- Думки публічних експертів: Аналітика та оцінки від відомих фахівців.
- "Сіра література": Матеріали з обмеженим доступом, доступні лише певній аудиторії (наукові статті, препринти, технічні звіти).

ДЖЕРЕЛА ІНФОРМАЦІЇ ДЛЯ OSINT

- Засоби масової інформації: Телебачення, газети, інтернет-видання.
- Публічні дані:
  - Урядові звіти, дані про бюджети, демографію.
  - Слухання, законодавчі дебати, прес-конференції, публічні виступи.
- "Сіра література":
  - Наукові, політичні, соціально-економічні, військові матеріали.
  - Дослідження, дисертації, неофіційні урядові документи, технічні звіти.
- Спостереження та звіти:
  - Інформація від спостерігачів за літаками (плейнспоттери), радіолюбителів, спостерігачів за супутниками чи суднами.

«OSINT»

- «**OSINT**» (Open Source INTelligence) – це збір, аналіз, обробка даних які знаходяться у загальному доступі, але ці данні завжди специфічні, тобто зібрані та структуровані особливим способом, задля відповіді на конкретне питання.
- У 1947 році аналітик ЦРУ Кен Шерман зазначив, що держава отримує з відкритих джерел інформації майже 80%, пізніше генерал-лейтенант, керівник Розвідувального управління міністерства оборони США Самуель Уілсон стверджував що 90% всієї розвідувальної інформації надходить з відкритих джерел, а лише 10 % – з роботи агентури

НАЙШИРШЕ ВИКОРИСТАННЯ «OSINT» ЗДОБУВ У США.

Можна навести перелік організацій які користуються цим методом:

- Рада із захисту відкритих джерел (DOSC);
- Командування розвідки і безпеки ЗС США (INSCOM);
- Служба розвідувальної інформації Департаменту сухопутних військ (DA IIS);
- Національна розвідка центру відкритих джерел (DNI OSC);
- Академія відкритих джерел;
- Департамент передових систем (ASD);
- ФБР;
- Дослідницька служба бібліотеки Конгресу (Congressional Research Service)

- США використовує інформацію, отриману за допомогою «OSINT», в більшій мірі для планування бойових дій, організації та проведення військових операцій, запобігання терористичним актам. На думку аналітиків розвідки США найбільшою проблемою методу «OSINT» на даний момент є неперевірені джерела інформації, провокуючі ресурси, недостовірна інформація. Для отримання найбільш актуальної та якісної інформації користувач повинен обробити багато інформації з різних джерел та узагальнити її так, як вимагає мета та завдання дослідження.

- У США сформована розгалужена мережа центрів і пунктів, що ведуть OSINT-розвідку та надають відомості більш ніж 7 тис. споживачам розвідувальних даних. І це не що інше, як результат скоординованих дій законодавчої і виконавчої влади, спрямованих на проведення цілеспрямованої політики в галузі забезпечення національної безпеки. Подібні структури є на всіх рівнях

- Ізраїль також використовує «OSINT» в першу чергу для аналізу військової спроможності противника. В структурі військової розвідки існує окремий спеціальний підрозділ для аналізу відкритих джерел інформації «Hatsaf», який збирає інформацію лише для військових цілей.
- У Великобританії за допомогою «OSINT» цивільні журналісти служби BBC Monitoring здійснюють первинний збір інформації, яка в подальшому потрапляє до співробітників спецслужб для її використання за конкретними напрямами досліджень.

- Зважаючи на міжнародний досвід використання «OSINT» можна зазначити, що для отримання якісної та актуальної інформації необхідно опрацьовувати велику кількість інформаційних джерел. Для правильної та продуктивної роботи цього методу не достатньо лише знаходити інформацію, її треба обробляти, аналізувати, знаходити підтвердження досліджуваних фактів, подій та явищ, адже багато інформації створюється саме для дезінформації.

- На сьогоднішній день в провідних країнах світу «OSINT» активно та успішно використовується інформаційно-аналітичними підрозділами; дані відсоткового співвідношення продуктивності відкритих джерел інформації підтверджують необхідність та актуальність використання досвіду США та країн Європи для вирішення оперативних, тактичних та стратегічних завдань силових структур

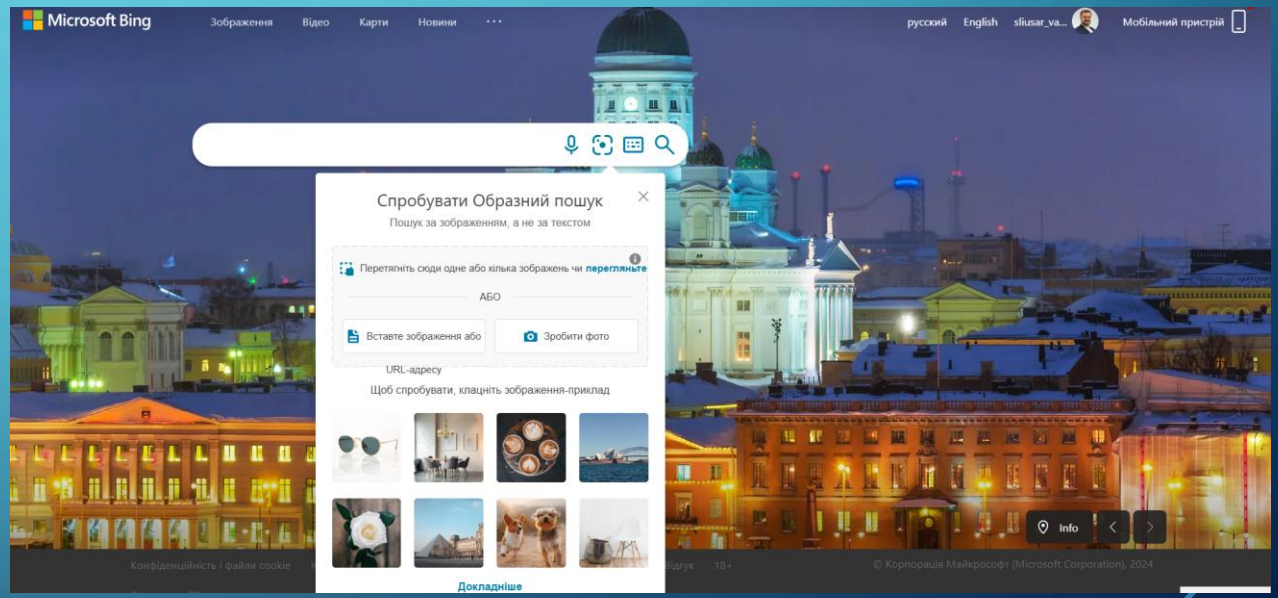
- Оскільки різниця між новачком, який шукає в Інтернеті інформацію і OSINT-професіоналом, який обізнаний з методикою пошуку та аналізу, має певні навички у цій сфері, колосальна: там, де новачок побачить фото, кількість репостів, групи і сторінки, на які підписана людина, профіль особи у соціальних мережах, – професіонал побачить активність, дати публікацій, фон на фотографіях, можливі причини підписки на певні групи, виділить кола спілкування (побудує схему зв'язків особи/осіб) тощо.

ОТЖЕ КЛЮЧОВИМИ ФАКТОРАМИ ДЛЯ УСПІШНОГО АНАЛІЗУ Є:

- чітке розуміння цілей аналізу;
- неупередженість (максимальна об’єктивність аналітика);
- збір інформації з максимально можливої кількості відкритих джерел;
- застосування «коефіцієнтів ваги» до кожної інформації;
- чіткість представлення даних;
- грамотний аналіз отриманої інформації.

ПОШИРЕНІ МЕТОДИ OSINT

- **Пошукові системи**: такі пошукові системи, як Google, Bing і Yahoo, є цінними інструментами для збору OSINT. Використовуючи оператори розширеного пошуку, аналітики можуть швидко фільтрувати й уточнювати результати пошуку, щоб знайти відповідну інформацію.



ПОШИРЕНІ МЕТОДИ OSINT

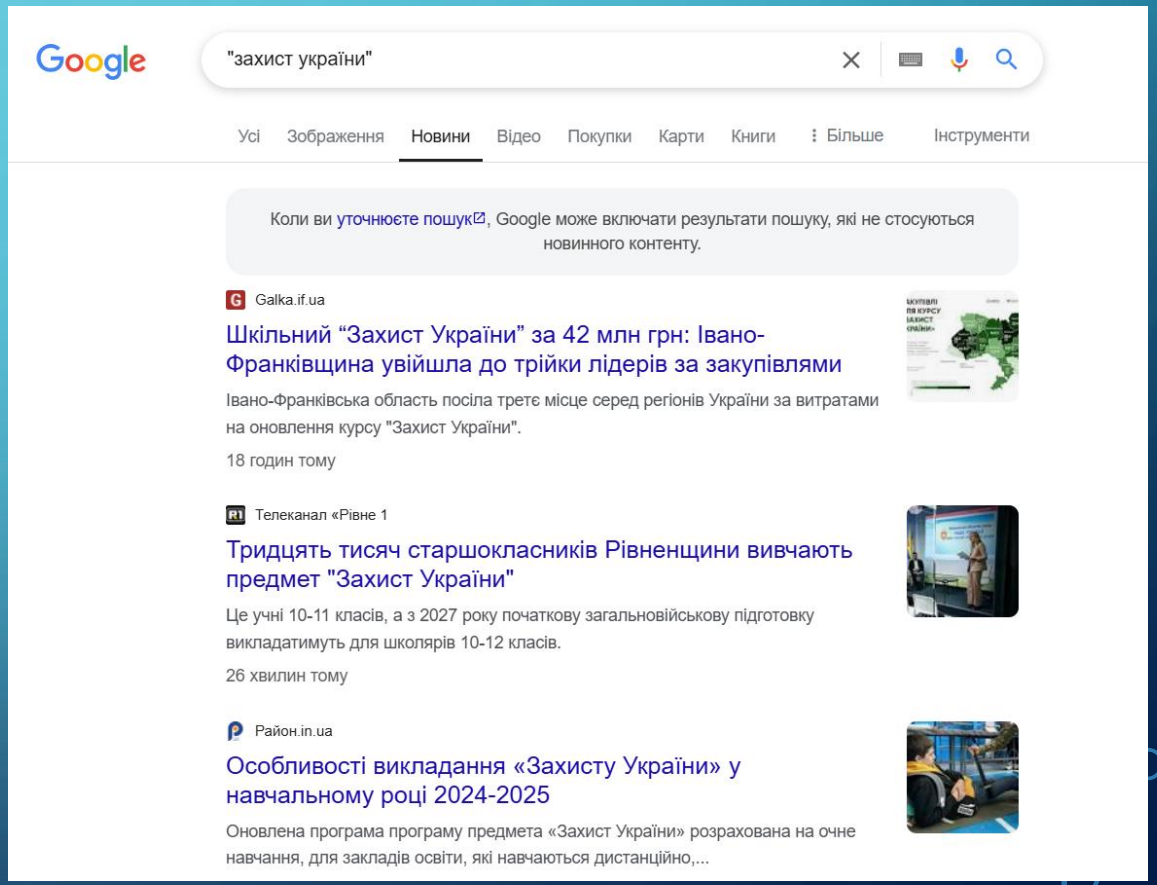
- **Соціальні медіа:** Платформи соціальних мереж, такі як Twitter, Facebook і LinkedIn, є цінними джерелами OSINT. Відстежуючи та аналізуючи активність у соціальних мережах, аналітики можуть отримати уявлення про тенденції, настрої та потенційні загрози.

ПОШИРЕНІ МЕТОДИ OSINT

- **Публічні документи:** публічні документи, такі як судові документи, записи про майно та бізнес-файли, є цінними джерелами OSINT. Отримавши доступ до цих записів, аналітики можуть збирати інформацію про окремих осіб, організації та інші організації.

ПОШИРЕНІ МЕТОДИ OSINT

- **Джерела новин**: такі джерела новин, як газети, журнали та онлайн-видання новин, є цінними джерелами OSINT. Відстежуючи та аналізуючи новинні статті, аналітики можуть отримати уявлення про поточні події, тенденції та потенційні загрози.



ПОШИРЕНІ МЕТОДИ OSINT

- **Веб-збирання**: веб-збирання передбачає використання програмних засобів для вилучення даних із веб-сайтів. Збираючи дані з кількох веб-сайтів, аналітики можуть швидко й ефективно збирати великі обсяги даних.

- Веб-скрепінг (також відомий як веб-збирання або вилучення даних) - це процес автоматичного вилучення даних з веб-сайтів, веб-сервісів і веб-додатків.
- Веб-скрепінг допомагає позбавити нас від необхідності заходити на кожен веб-сайт і вручну витягувати дані - довгого і неефективного процесу. Процес передбачає використання автоматизованих скриптів або програм. Скрипт або програма отримує доступ до HTML-структури веб-сторінки, аналізує дані і витягує конкретні необхідні елементи сторінки для подальшого аналізу.

ПОШИРЕНІ МЕТОДИ OSINT

- **Інструменти аналізу даних:** такі інструменти аналізу даних, як Excel, Tableau та R, є цінними для аналізу великих наборів даних. Використовуючи ці інструменти, аналітики можуть визначити закономірності, тенденції та зв’язки в даних.

9. Tableau

Tableau з першого погляду:

Тип інструменту: Інструмент візуалізації даних.
Доступність: Комерційна.
Найчастіше використовується для: Створення інформаційних панелей та робочих аркушів.
Переваги: Чудова візуалізація, швидкість, інтерактивність, підтримка мобільних пристроїв.
Мінуси: Поганий контроль версій, відсутність попередньої обробки даних.

Якщо ви хочете створювати інтерактивні візуалізації та дашборди без значних навичок програмування, Tableau – один з найкращих комерційних інструментів для аналізу даних. Цей пакет обробляє великі обсяги даних краще, ніж багато інших BI-інструментів, і він дуже простий у використанні. Він має візуальний інтерфейс перетягування (ще одна безперечна перевага над багатьма іншими інструментами аналізу даних). Однак, оскільки він не має шару сценаріїв, існує межа того, що може зробити Tableau. Наприклад, він не дуже добре підходить для попередньої обробки даних або побудови більш складних розрахунків.

Хоча він і містить функції для маніпулювання даними, вони не дуже зручні. Як правило, перед імпортом даних до Tableau вам потрібно буде виконати скриптові функції за допомогою Python або R. Але його візуалізація є досить першокласною, що робить його дуже популярним, незважаючи на його недоліки. Крім того, він готовий для мобільних пристроїв. Як аналітик даних, мобільність може не бути вашим пріоритетом, але вона стане у нагоді, якщо ви захочете погратися з даними на ходу!

ІНСТРУМЕНТИ OSINT МОЖНА РОЗДІЛИТИ НА ТРИ ОСНОВНІ КАТЕГОРІЇ У ЗАЛЕЖНОСТІ ВІД ТОГО, НА ЯКУ ДІЯЛЬНІСТЬ ВОНИ НАЦІЛЕНІ:

- Інструменти виявлення: інструменти, які дозволяють шукати дані, які вже перебувають у мережі. Найкращим прикладом є пошукова система Google. Хоча може здатися, що це проста пошукова система, але насправді Google індексує і сканує безліч веб-сайтів, що, у свою чергу, дає величезний потенціал для виявлення нової інформації. Хорошим прикладом постає інструмент Shodan, який нижче буде описано.
- Інструменти вилучення: після виявлення дані необхідно вилучити і зібрати в безпечному місці. Ці інструменти гарантують, що тільки необхідні дані будуть відфільтровані для вилучення, щоб уникнути об'ємних передач (які можуть «насторожити» ціль), а також уникнути непотрібних даних, які можуть зіпсувати інформацію.
- Інструменти агрегації: після того, як були зібрані всі релевантні дані, є потреба у їх подальшому співвіднесенні та компіляції у функціональний, легко засвоюваний формат.

ПОШУКОВІ СИСТЕМИ ДЛЯ OSINT

- 1. Google Search

Особливості:

- Найпопулярніша пошукова система з потужними алгоритмами індексації.
- Підтримує розширений пошук (оператори: site:, filetype:, inurl: тощо).
- Доступ до широкого спектра даних: вебсайти, зображення, новини, відео.

Потенціал для OSINT:

- Ефективний для пошуку відкритої інформації, включаючи соціальні мережі, публічні документи та архіви.
- Можливість використання Google Dorks для точкового пошуку (наприклад, конфіденційних документів).

Обмеження: фільтрація результатів може залежати від регіону чи персоналізації.

2. BİNG

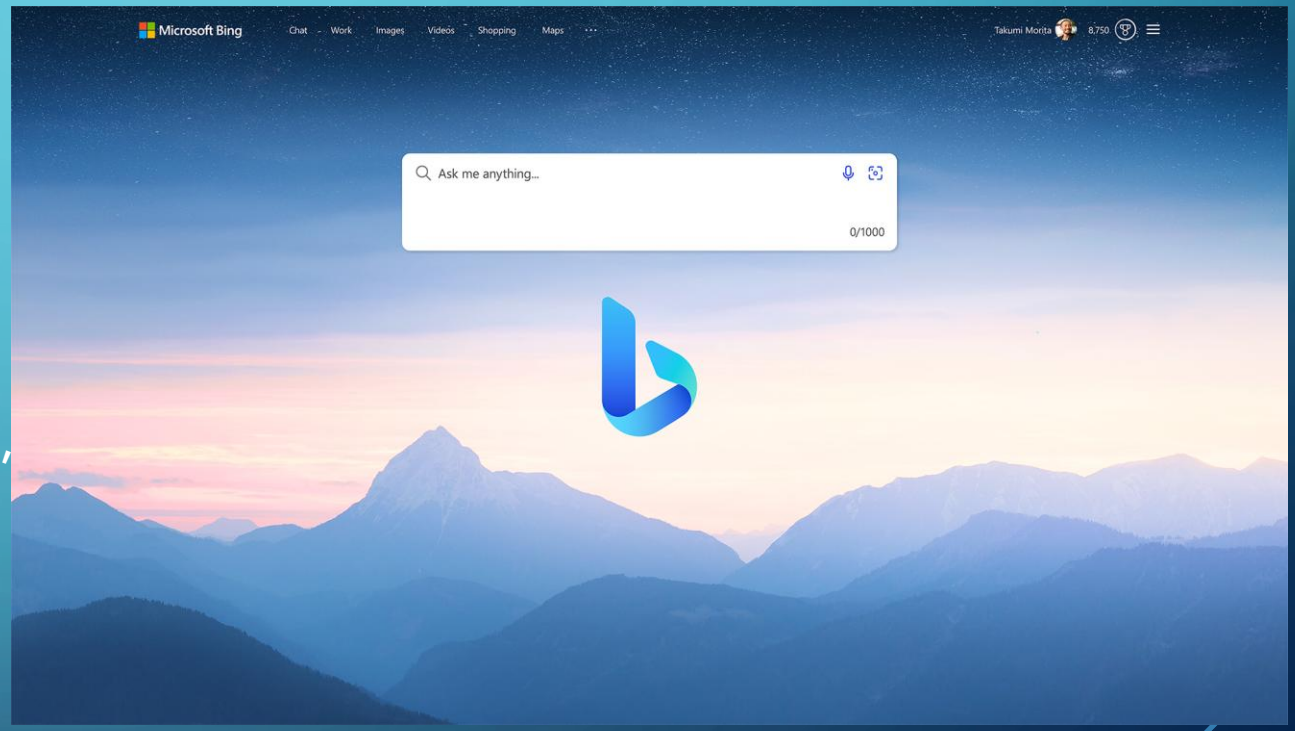
Особливості:

- Пошукова система від Microsoft із підтримкою пошуку вебсайтів, зображень, відео та новин.
- Менш популярна, ніж Google, але має унікальний алгоритм ранжування.

Потенціал для OSINT:

- Корисна для перевірки альтернативних результатів, які можуть не відображатися в Google.
- Ефективна для пошуку мультимедійного контенту (зображень, відео).

Обмеження: менший обсяг індексованої інформації порівняно з Google.



3. YAHOO! SEARCH

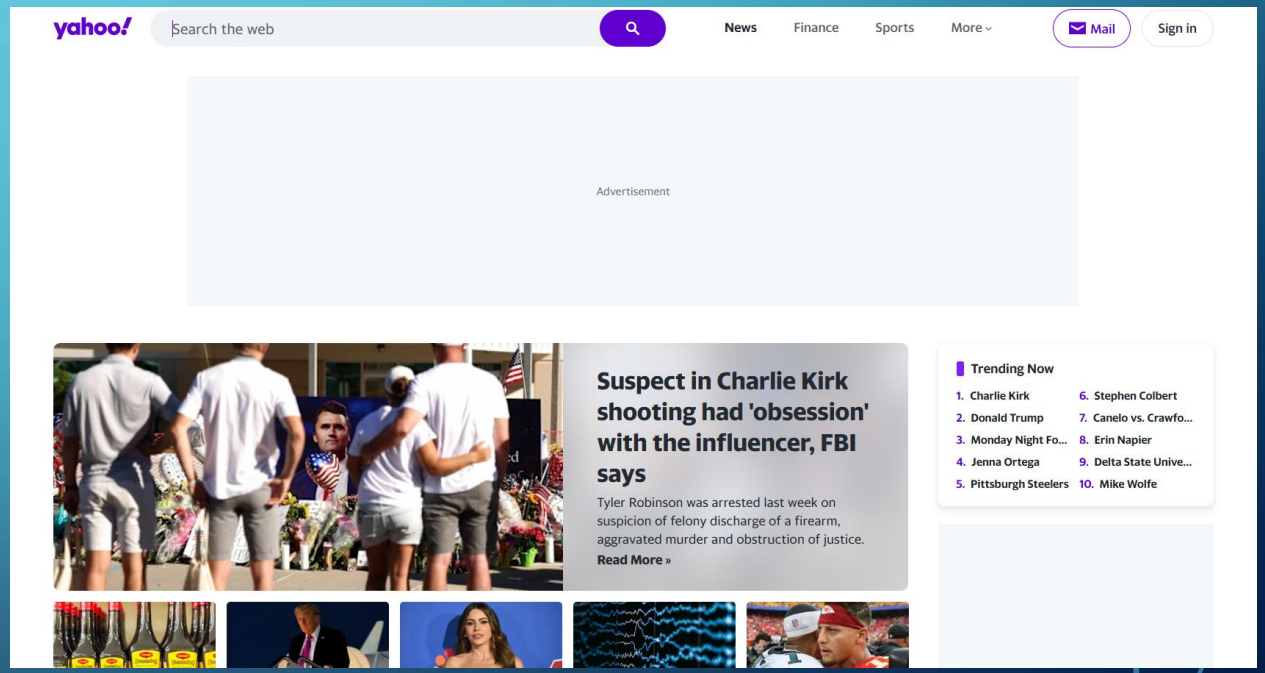
Особливості:

- Пошукова система, що інтегрує результати з різних джерел.
- Надає доступ до новин, зображень і вебсайтів.

Потенціал для OSINT:

- Корисна для пошуку застарілої інформації або даних із соціальних мереж, які можуть бути недоступні в інших системах.
- Підходить для крос-перевірки результатів із Google та Bing.

Обмеження: менш розвинений функціонал порівняно з Google.



4. BRAVE SEARCH

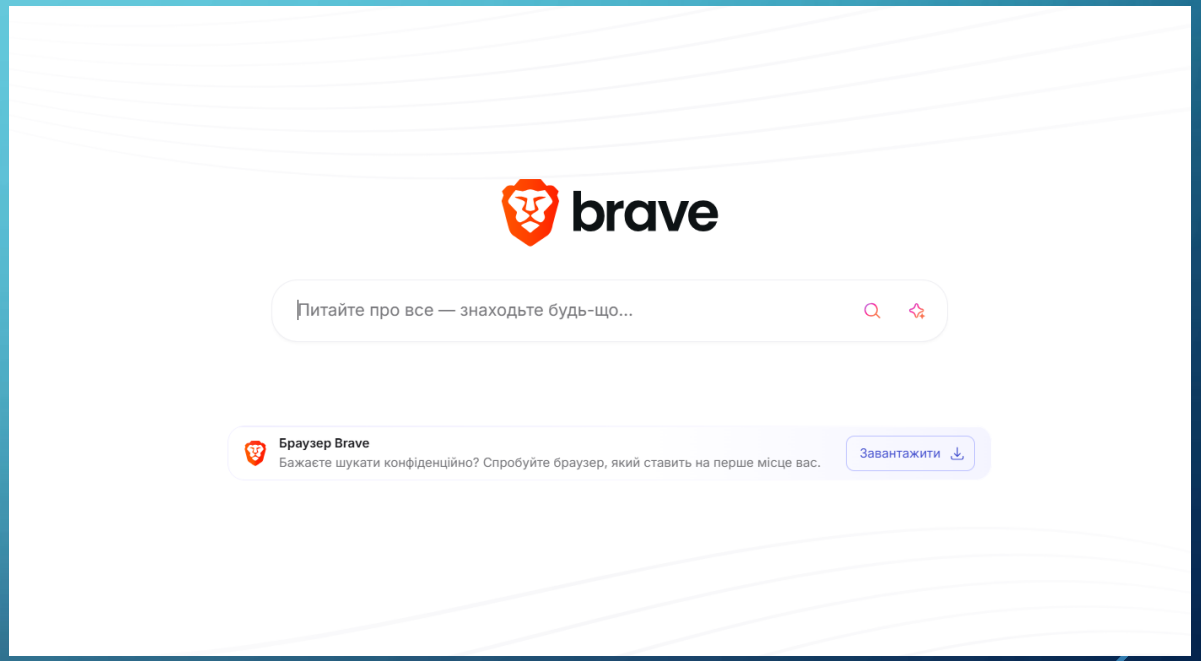
Особливості:

- Незалежна пошукова система, орієнтована на конфіденційність і відсутність трекінгу.
- Пропонує прозорий алгоритм без персоналізації результатів.

Потенціал для OSINT:

- Ідеальна для анонімного збору даних, що зменшує ризик виявлення.
- Корисна для пошуку інформації в середовищах, де потрібна приватність.

Обмеження: менший індекс порівняно з Google, що може обмежувати результати.



5. WOLFRAM ALPHA

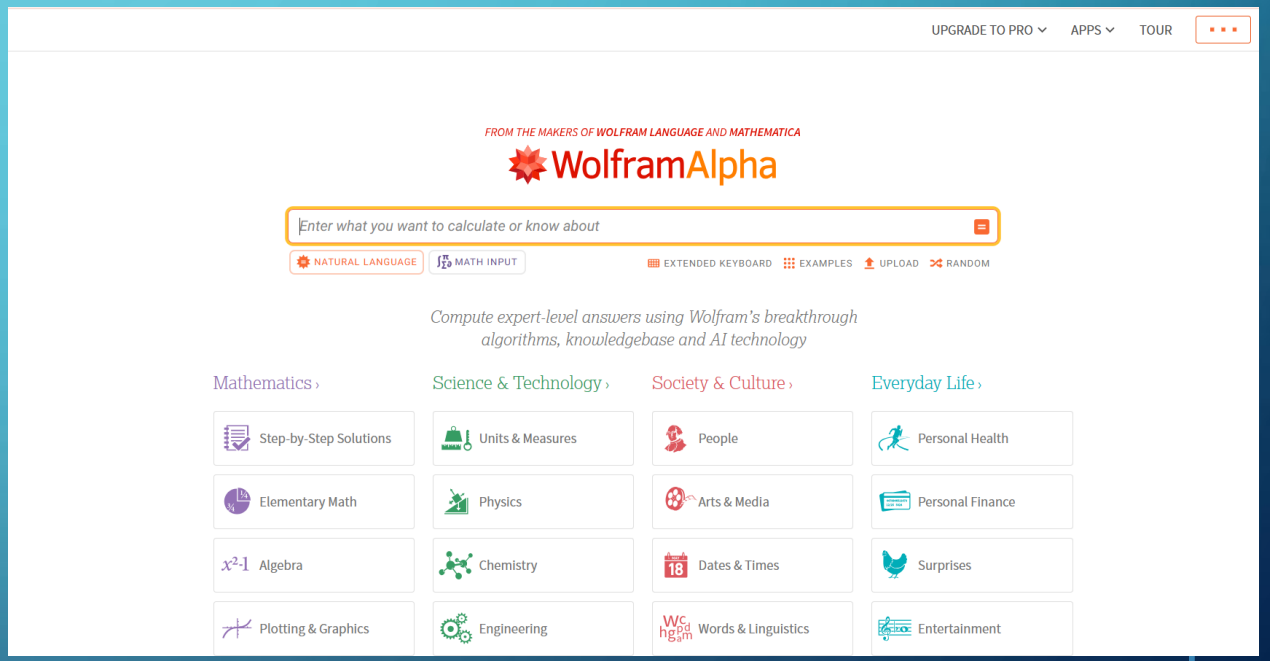
Особливості:

- Обчислювальна пошукова система, що надає відповіді на основі алгоритмів, баз знань і штучного інтелекту.
- Спеціалізується на аналізі структурованих даних (статистика, математика, наукові дані).

Потенціал для OSINT:

- Ефективна для аналізу числових даних, демографічної статистики чи наукової інформації.
- Корисна для перевірки фактів і обчислень на основі відкритих джерел.

Обмеження: обмежена підтримка пошуку текстової чи мультимедійної інформації.



6. MOJEEK

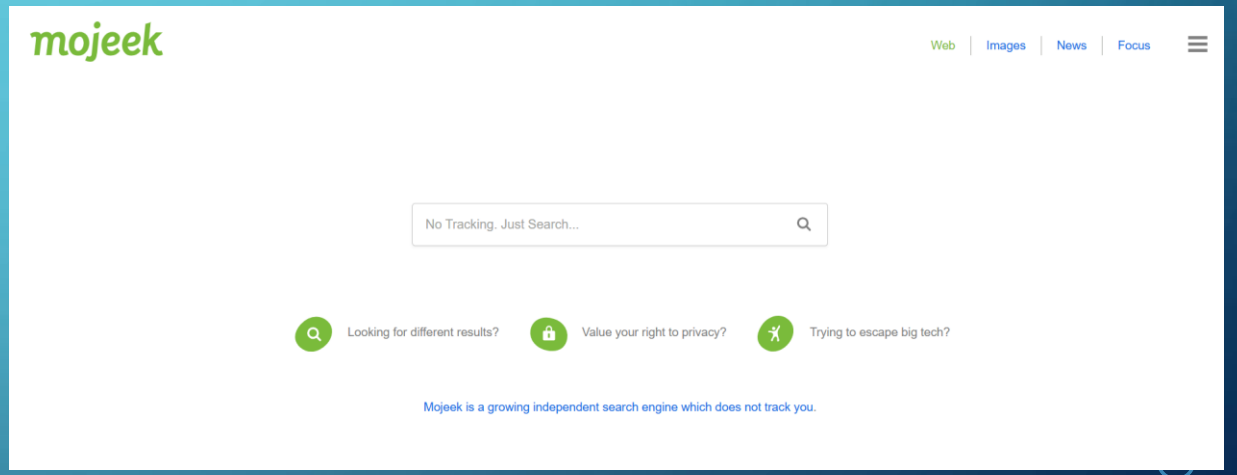
Особливості:

- Незалежна пошукова система, що не відстежує користувачів.
- Фокусується на створенні власного індексу вебсайтів.

Потенціал для OSINT:

- Підходить для анонімного пошуку інформації, що не залежить від великих корпорацій.
- Корисна для пошуку даних у менш популярних джерелах.

Обмеження: менший обсяг індексованої інформації порівняно з Google чи Bing.



7. SEARCH.COM

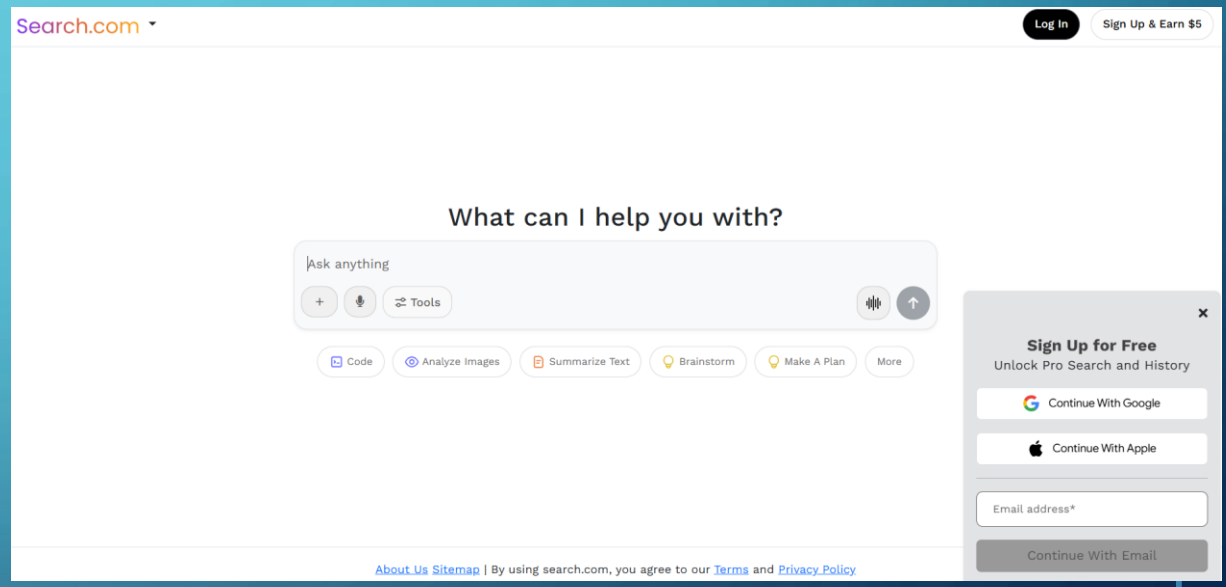
Особливості:

- Агрегатор, що комбінує результати з кількох пошукових систем.
- Надає доступ до вебсайтів, новин, зображень і продуктів.

Потенціал для OSINT:

- Ефективна для швидкого порівняння результатів із різних джерел.
- Корисна для пошуку інформації, що може бути пропущена однією системою.

Обмеження: результати залежать від якості джерел, що агрегуються.



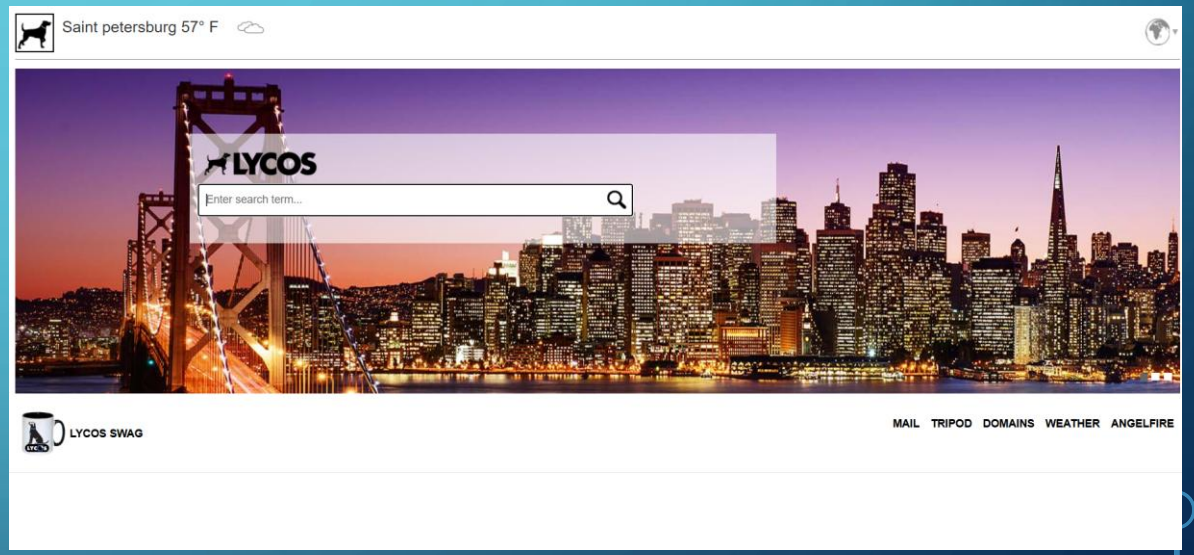
8. LYCOS

Особливості:

- Пошукова система з акцентом на мультимедійний контент (зображення, відео, новини, продукти).
- Має застарілий інтерфейс, але все ще функціонує.

Потенціал для OSINT:

- Корисна для пошуку архівного мультимедійного контенту.
- Підходить для крос-перевірки зображень і відео.
- Обмеження: обмежена популярність і менший індекс порівняно з Google.



AOL

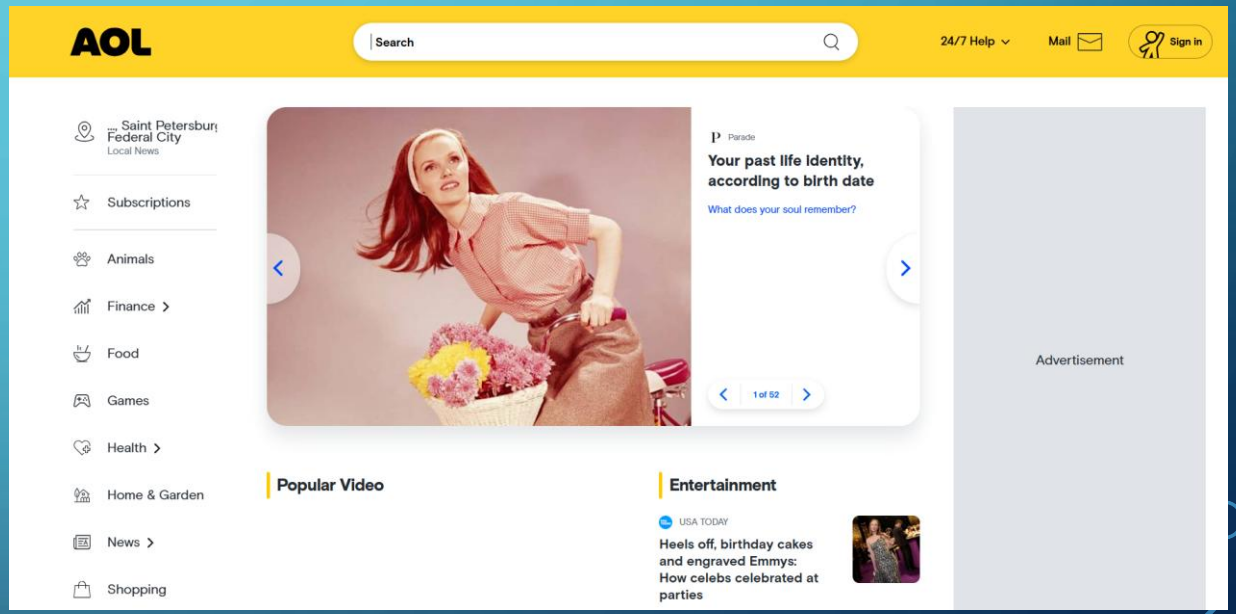
Особливості:

- Пошукова система, орієнтована на американську аудиторію.
- Надає результати з вебсайтів, новин і мультимедіа.

Потенціал для OSINT:

- Корисна для пошуку інформації, релевантної для США (новини, локальні звіти).
- Підходить для крос-перевірки з іншими системами.

Обмеження: обмежена глобальна індексація.



ЛОКАЛІЗОВАНІ ПОШУКОВІ СИСТЕМИ)

- Yandex (Росія)
- Особливості:
- Найпопулярніший пошуковик у Росії з часткою ринку понад 70%, також використовується в Білорусі, Казахстані та Туреччині.
- Підтримує понад 20 булевих операторів (наприклад, +, -, &&, ||, inurl:, title:), подібних до Google Dorks, для точного пошуку.
- Потужний пошук зображень з розпізнаванням обличчя та функцією пошуку подібних зображень (не тільки ідентичних, а й схожих об'єктів, наприклад, будівель).
- Адаптує результати за мовою та локацією, інтегрується з іншими сервісами Yandex (карти, пошта, браузер).

- Потенціалдля OSINT:
- Ідеальний для розслідувань у Східній Європі та російськомовному контенті, де дає результати, відмінні від західних пошуковиків.
- Використовується для реверсного пошуку зображень, геолокації та виявлення вразливостей; Bellingcat рекомендує для перевірки фактів.
- Ризики: Зв'язки з російським урядом, можливе відстеження; використовуйте з VPN для анонімності.
- Обмеження: Менш ефективний для глобального контенту, можлива цензура.

2. BAİDU (КИТАЙ)

Особливості:

- Домінуючий пошуковик у Китаї з часткою ринку ~65-80%, індексує переважно китайськомовний контент у спрощеній китайській.
- Підтримує пошук зображень, карт (Baidu Maps), соціальних мереж та бізнес-довідників; інтегрується з WeChat та Weibo.
- Алгоритми враховують локалізацію, але технологія відстає від Google (більше ваги старшим доменам, менше покарання за "чорне" SEO).
- Цензура контенту відповідно до вимог уряду КНР.

Потенціал для OSINT:

- Ключовий для аналізу китайського інтернету: індексує WeChat, Weibo, бізнес-реєстри (QCC.com, TianYanCha.com) для геолокації та перевірки компаній.
- Використовується для моніторингу загроз, витоків даних та соціальних мереж; комбінується з Google для повного охоплення.

Обмеження: Блокування Google в Китаї; потребує VPN та знання китайської; цензура обмежує доступ до чутливих тем

МЕТАПОШУКОВІ СИСТЕМИ

- All-in-One

Особливості:

- Мега-пошукова система, що агрегує результати з кількох основних пошуковиків (Google, Bing, Yahoo тощо).
- Підтримує пошук вебсторінок, зображень, новин та інших типів контенту в одному інтерфейсі.
- Швидкий доступ до результатів без дублювання, з акцентом на ефективність.

Потенціал для OSINT:

- Корисна для одночасного пошуку по кількох джерелах, що дозволяє виявляти унікальні результати, пропущені окремими пошуковими системами.
- Підходить для початкового сканування відкритих джерел, включаючи комерційні сайти як Amazon та eBay.
- Обмеження: Залежить від якості агрегованих джерел, може не охоплювати регіональний контент.

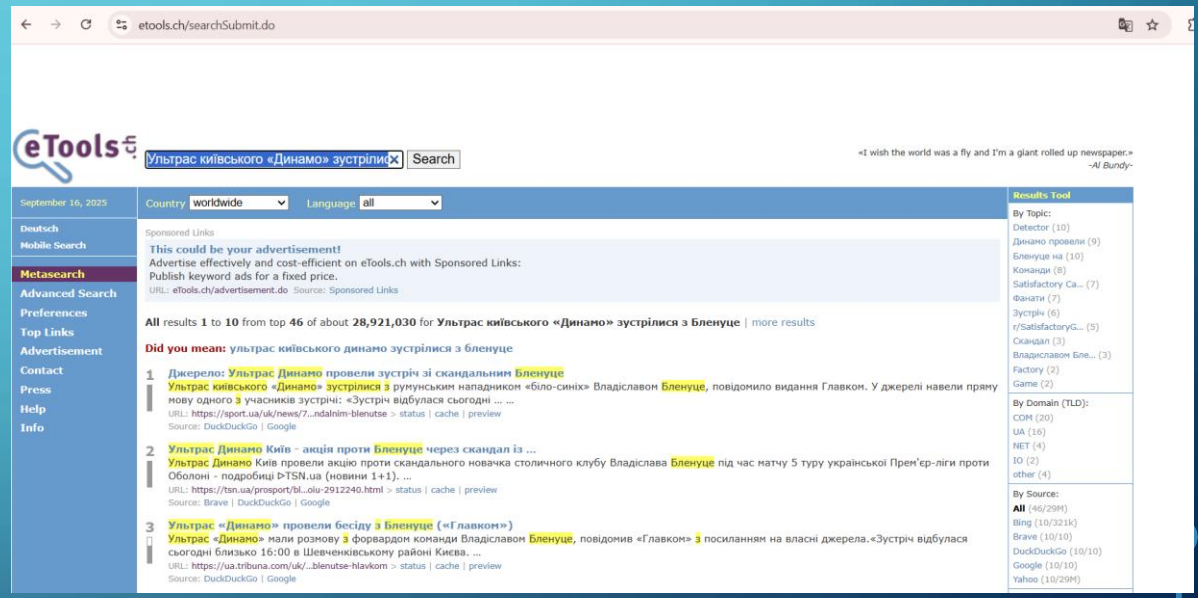
ETOOLS

Особливості: Швейцарська метапошукова система, що одночасно запитує основні міжнародні пошуковики (Google, Bing тощо).

- Забезпечує конфіденційність: не збирає чи не ділиться персональними даними користувачів.
- Швидка обробка з підсумком джерел результатів.

Потенціал для OSINT:

- Ідеальна для анонімного пошуку, зменшуючи ризик відстеження.
- Корисна для одночасного сканування кількох двигунів, що розширює охоплення даних.
- Обмеження: Обмежена глобальна індексація, краща для європейського контенту.



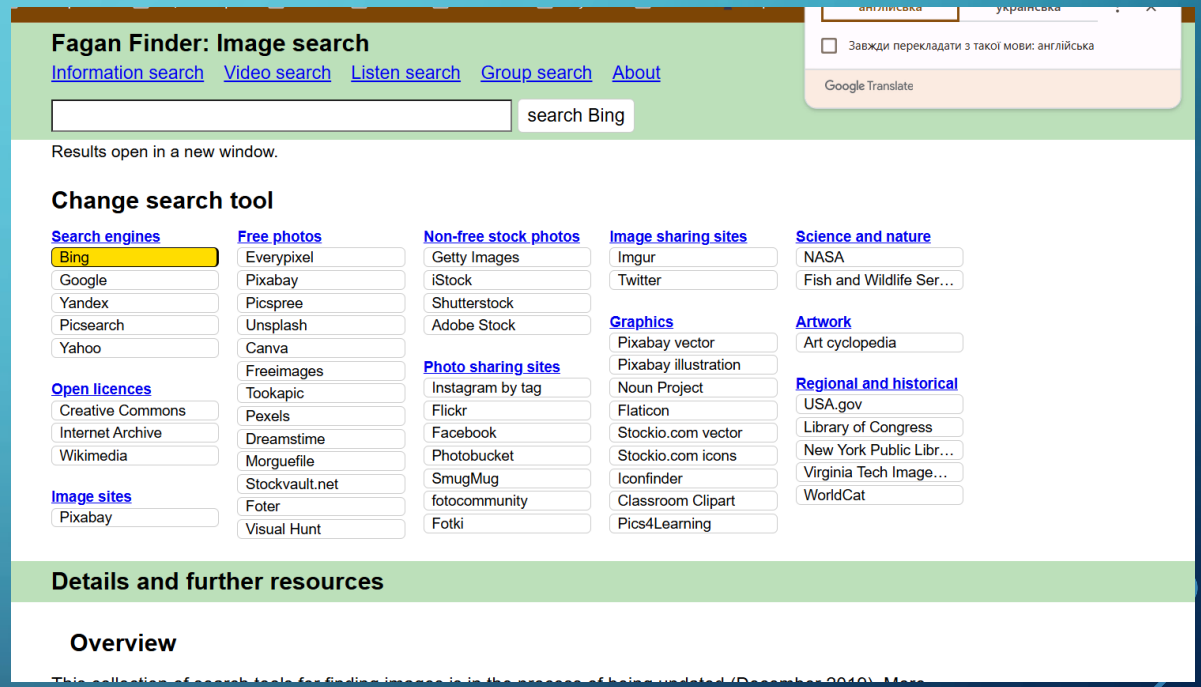
FAGANFİNDER

Особливості:

- Метапошукова система з колекцією інтернет-інструментів для пошуку будь-якого контенту (люди, зображення, новини, академічні ресурси).
- Агрегує результати з кількох баз даних та пошуковиків в одному інтерфейсі.
- Підтримує спеціалізовані пошуки, включаючи метадані та приховану інформацію.

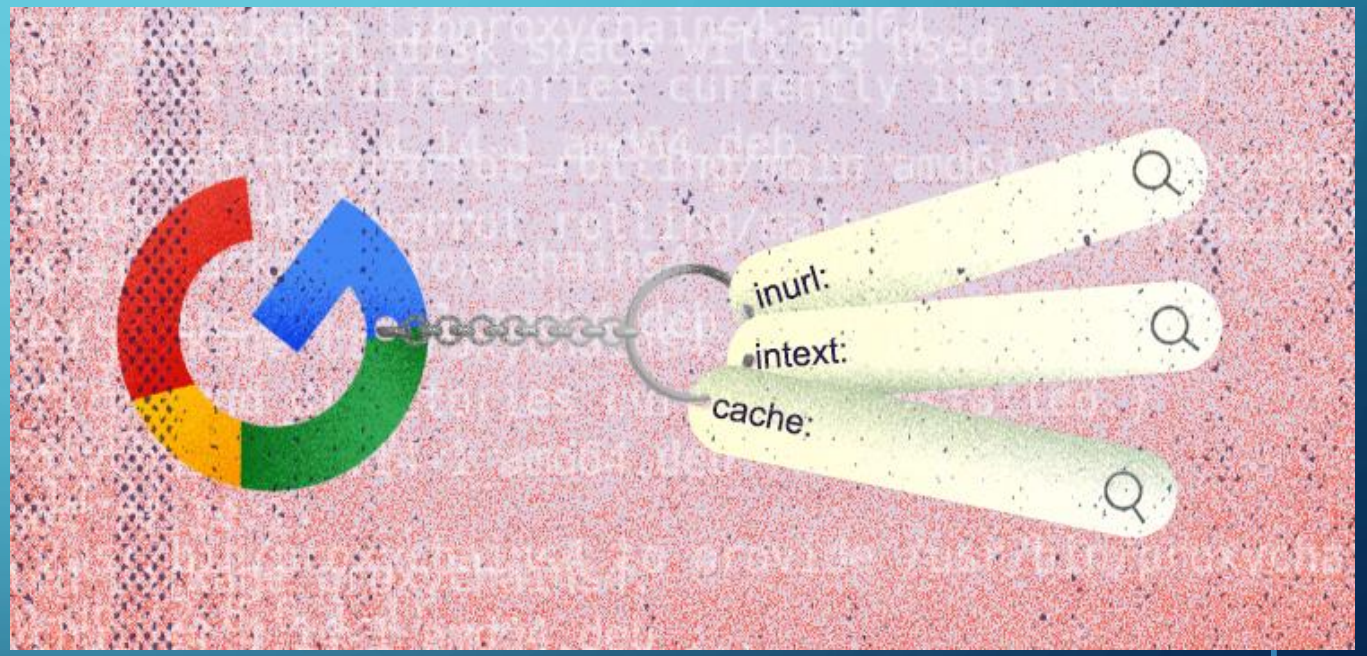
Потенціал для OSINT:

- Потужна для глибоких розслідувань: пошук людей, зображень та документів.
- Дозволяє виявляти метадані та приховані зв'язки в документах.
- Обмеження: Інтерфейс може бути застарілим, потребує ручного фільтрування.



GOOGLE DORKS

- Google Dorking надає можливість розгортати більш широкий пошуковий процес. Пошукові системи зазвичай індексують хедери й наповнення веб-сторінок, а для оптимізації пошукових запитів зв'язують їх. Google Dorking (або ж Google Hacking) дозволяє дещо модифікувавши звичний пошуковий термін у стрічці пошуку, додавши спеціальні оператори пошуку, відшукати такі фрагменти тексту загальнодоступних веб-сторінок, які будуть свідчити, до прикладу, про наявність версій уразливих веб-додатків. Також якщо пошук націлений на конкретну компанію, можна за допомогою цієї техніки відшукати звіти, податкові декларації, які можуть не прослідковуватися при стандартному пошуку й не бути на веб-сайтах цих компаній.



ОПЕРАТОР INTITLE

- у Google дозволяє шукати сторінки, у заголовках яких (HTML-тег <title>) містяться вказані слова чи фрази. Це допомагає знаходити специфічні веб-ресурси, що відповідають точним критеріям пошуку.Синтаксис: intitle:"ключова фраза" (лапки для точної фрази) або intitle:слово (для окремого слова).
- Особливості: Дозволяє звузити пошук до сторінок із певними заголовками, що часто вказують на їхній вміст (наприклад, адмін-панелі, логіни, документи).Комбінується з іншими операторами (inurl:, site:, filetype:) для підвищення точності.

- Приклад використання
- Запит: intitle:"Login" inurl:admin
- Результат: Знаходить сторінки з "Login" у заголовку та "admin" в URL, наприклад, панелі адміністрування сайтів.
- Пояснення: Пошук виявляє сторінки входу до адмін-панелей, які можуть бути погано захищені або залишені відкритими.
- Запит: intitle:"Index of" site:*.edu
- Результат: Знаходить відкриті директорії на сайтах освітніх установ (домен .edu).Пояснення: Виявляє незахищені каталоги з файлами, які можуть містити документи, презентації чи бази даних.

GOOGLE DORKS: ОПЕРАТОР INURL ДЛЯ OSINT

- Опис: Оператор inurl: у Google шукає слова чи фрази безпосередньо в URL-адресі сторінки. Це дозволяє знаходити ресурси з певними шляхами, параметрами чи ключовими словами в адресі, що часто вказує на тип контенту (наприклад, адмін-розділи чи файли).
- Синтаксис: inurl:"ключова фраза" (для точної фрази) або inurl:слово (для окремого слова).
- Особливості:
- Зосереджується на структурі URL, що допомагає виявляти динамічні сторінки, API чи приховані директорії.
- Комбінується з іншими операторами для точності, наприклад, з intitle: чи site:.
- 2. Приклад використання
- Запит: inurl:admin login
- Результат: Знаходить сторінки з "admin" та "login" в URL, наприклад, http://example.com/admin/login.php.
- Пояснення: Виявляє потенційні панелі адміністраторів, які можуть бути доступні без автентифікації.
- Запит: inurl:backup filetype:sql
- Результат: Локалізує SQL-файли резервних копій у URL з словом "backup".
- Пояснення: Шукає бази даних, що залишилися відкритими на сервері.

- 3. Застосування для OSINT
- Для чого використовується:
- Виявлення структур сайтів: Пошук шляхів до чутливих розділів, як /config/, /db/ чи /api/, для аналізу архітектури ресурсів.
- Збір даних про сервери: inurl:wp-admin – виявлення WordPress-сайтів для моніторингу вразливостей чи контенту.
- Моніторинг подій: Пошук URL з ключовими словами, пов'язаними з організаціями (наприклад, inurl:press site:company.com для прес-релізів).
- Як використовує OSINT-аналітик:
- Для картинування веб-присутності компаній чи осіб, виявлення незахищених ендпоінтів.
- Для крос-перевірки інформації з відкритих джерел, наприклад, пошук логів чи конфігів для розслідувань.
- Для геолокації ресурсів через URL-параметри.
- 4. Рекомендації та обмеження
- Етика: Застосовуйте тільки для легальних розслідувань; не експлуатуйте вразливості.
- Технічні аспекти: Обмежте запити, щоб уникнути блокування; використовуйте проксі.
- Обмеження: Не всі URL індексуються; динамічні параметри можуть змінюватися.

Ми окреслили 14 операторів розширеного пошуку, які можуть бути корисними дослідникам для уточнення результатів пошуку, зокрема:

- **«** пошуковий термін **»** = точна фраза, тобто **«** Skopenow спрощує вашу належну перевірку та процес подання претензій **»**

Лапки дозволяють користувачам примусово встановити точну відповідність для необхідних слів або фраз. Оператор точної відповідності можна використовувати для уточнення результатів, щоб переконатися, що певна фраза включена в результати, або виключити синоніми під час пошуку окремих слів. Пошук точної фрази під час розслідування може знайти матеріал, написаний конкретною особою чи компанією.

- **АБО** або **|** = пошуковий термін ***або*** пошуковий термін, ***тобто*** Ед **АБО** Едвард або Ед **|** Едуард **|** Едвін

Оператор АБО дає змогу шукати кілька слів як альтернативи одне одному, знаходячи X або Y або обидва. Оператор вертикальної лінії (|) функціонує так само, як і «АБО». Дослідники можуть використовувати оператор АБО, коли для суб'єкта відомий лише псевдонім, що дає змогу одночасно шукати різні варіації одного імені.

- **+** або **|** = пошуковий термін ***і*** пошуковий термін, тобто Стів Адамс **|** Скопенов

Оператор I дає змогу шукати результати, які мають містити дві різні фрази слова, шукаючи як X, так і Y. Результати включатимуть лише ті результати, які містять обидві пошукові фрази. Оператор плюс (+) також можна використовувати замість «|». AND може бути корисним для слідчих під час пошуку інформації про особу, гарантуючи, що результати пов'язані з нею, включаючи ім'я її роботодавця.

- **–** = Не пошуковий термін, тобто Skopenow **–** www.skopenow.com

Оператор «мінус» дозволяє користувачам виключати слово чи фразу з результатів пошуку. Коли результати великі, видалення нерелевантних слів, які займають важливе місце в багатьох результатах, особливо корисно, якщо потрібно зменшити результати.

- **site:** = Тільки на цьому сайті, тобто на сайті "Skopenow" **:** twitter.com

Оператор сайту дозволяє користувачам обмежувати результати лише тими, що містяться на певному веб-сайті. Досліджуючи бізнес, оператор сайту може переконатися, що результати надходять саме з його офіційного веб-сайту.

- **filetype:** = Тільки цей тип файлу, тобто тип файлу OSINT **:** pdf АБО **тип файлу:** docx

Оператор типу файлу дозволяє обмежити результати пошуку файлами певного типу, видаляючи інші типи файлів і стандартні веб-сторінки. тип файлу: може бути корисним під час розслідування під час пошуку контрактів і офіційних документів у документах PDF або Word.

- **intitle:** = Показувати результати лише з текстом у заголовку сайту, тобто **intitle:** final.attendee.list "Шахрайство"

Оператор intitle дозволяє користувачам знаходити веб-сторінки з певним словом або фразою в заголовку. Дослідники можуть використовувати оператор intitle для пошуку відповідних веб-сторінок і статей, які містять відповідне ключове слово.

- **inurl:** = Показувати результати лише з текстом у веб-адресі веб-сайту, тобто **inurl:** резюме "john smith"

Оператор inurl дозволяє користувачам знаходити веб-сторінки з певним словом або фразою у веб-адресі. Слідчі можуть використовувати оператор inurl для пошуку відповідних веб-сторінок, які містять ключове слово у веб-адресі.

- **intext:** = Показувати лише ті результати, у яких текст знаходиться в основному тексті веб-сайту, тобто Skopenow **intext:** OSINT

Оператор intext дозволяє користувачам знаходити веб-сторінки з певним словом або фразою в основному тексті веб-сторінки. Дослідники можуть використовувати оператор intext для пошуку результатів, коли ключове слово в тілі веб-сторінки обмежує результати, наприклад рік або назва місця.

- **allintext:** = знайти всі слова на веб-сторінці, тобто **allintext:** skopenow страхове шахрайство

Оператор allintext дозволяє користувачам знаходити веб-сторінки, які містять список ключових слів в основному тексті веб-сторінки, але не обов'язково поруч. Слідчі можуть використовувати оператор allintext, якщо для пошуку результатів потрібно більше ніж одне ключове слово як прив'язку в тілі веб-сторінки, наприклад кілька ключових слів або імен, пов'язаних зі злочином.

- **cache:** = Показувати лише кешовані посилання, тобто **кеш:** skopenow.com

Оператор кешу дозволяє користувачам повертати останню кешовану версію веб-сторінки, коли веб-сторінку було проіндексовано. Слідчі можуть використовувати оператор кешу, щоб знайти попередні версії відредагованих або видалених веб-сторінок, щоб знайти вилучені розвідувальні дані.

- * = символ підстановки, тобто "robdouglas * com"

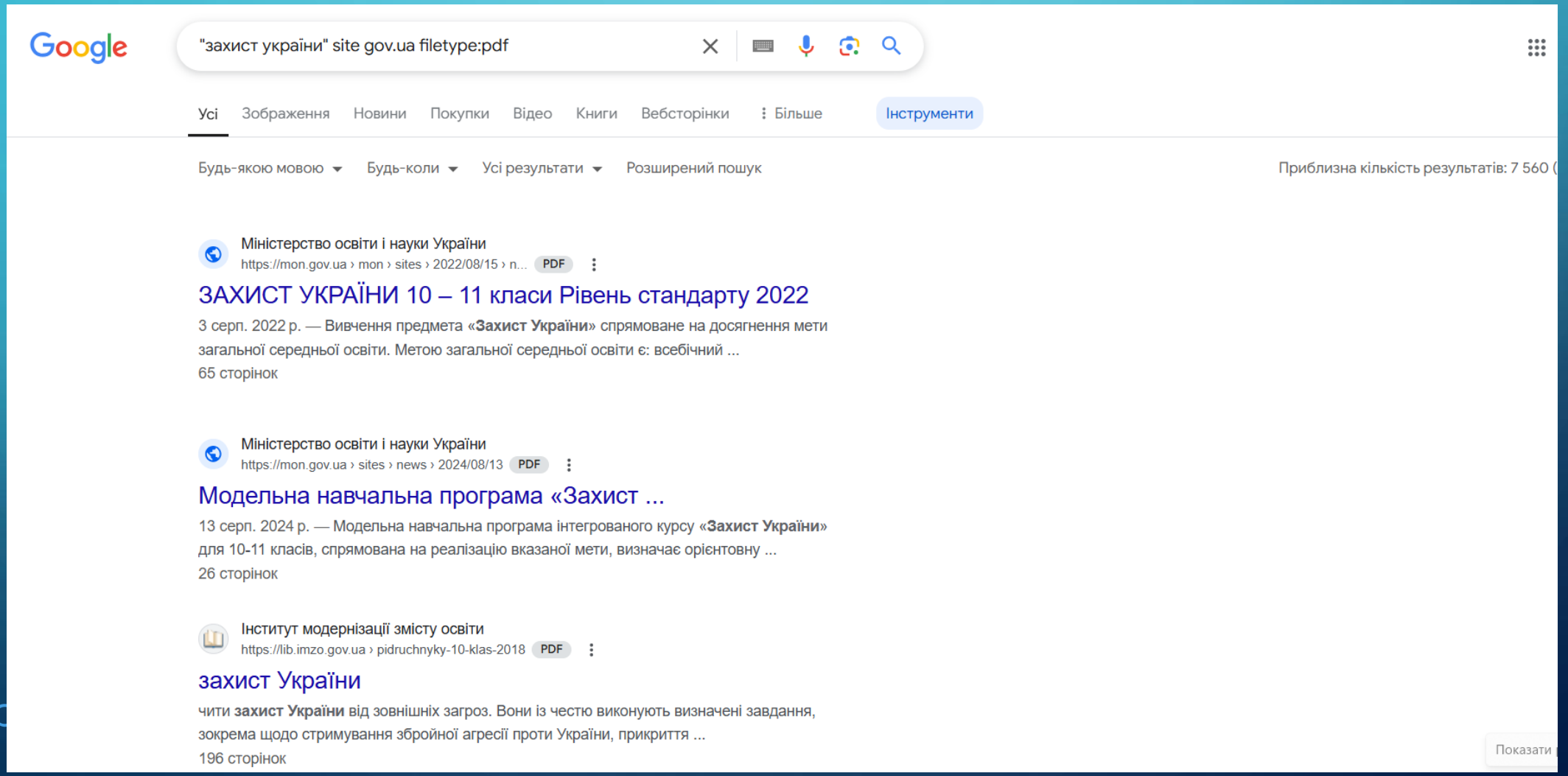
- * = символ підстановки, тобто "robdouglas * com"

Оператор зірочки представляє символ підстановки в рядках пошуку, займаючи місце слів або фраз між двома ключовими словами. Слідчі можуть використовувати оператор зірочки, щоб знайти адреси електронної пошти, замінивши ім'я домену символом підстановки.

- **карта:** = карта конкретного місця, тобто **карта:** Манхеттен

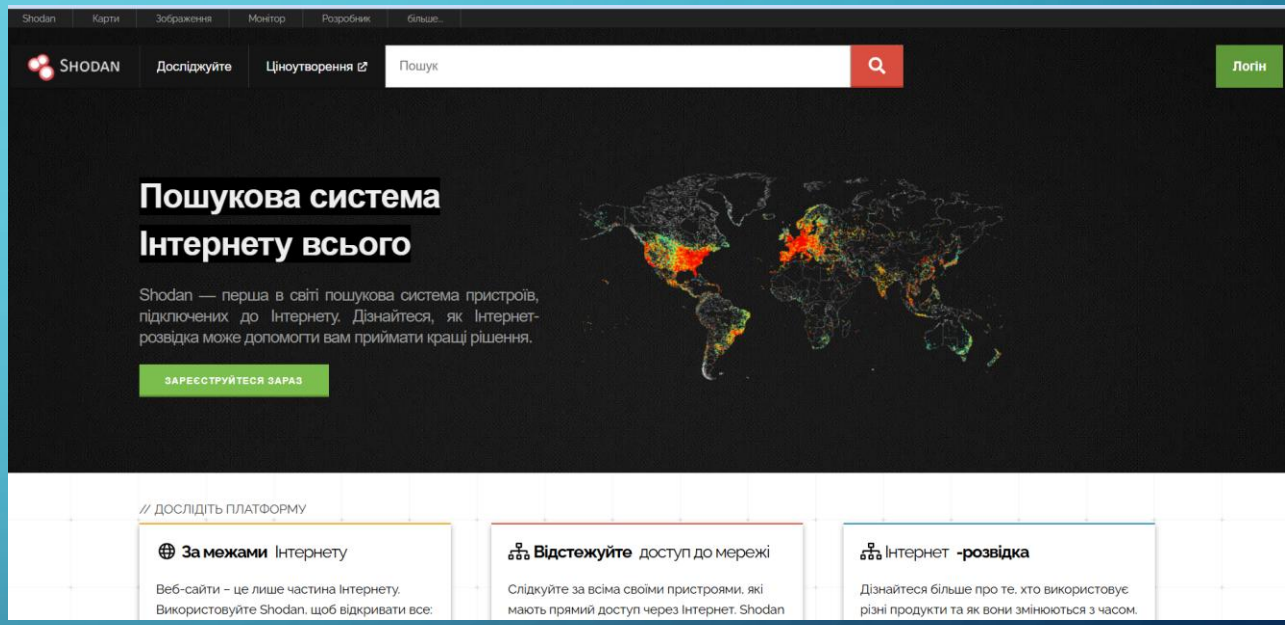
Оператор карти дозволяє користувачам змусити Google показувати результати карти для пошуку за місцем розташування. У результатах відображаються лише дані про місцезнаходження та не включаються останні новини. Дослідники можуть використовувати оператор карти, щоб зосередитися на геопросторових даних.

КОМБІНУВАННЯ ОПЕРАТОРІВ



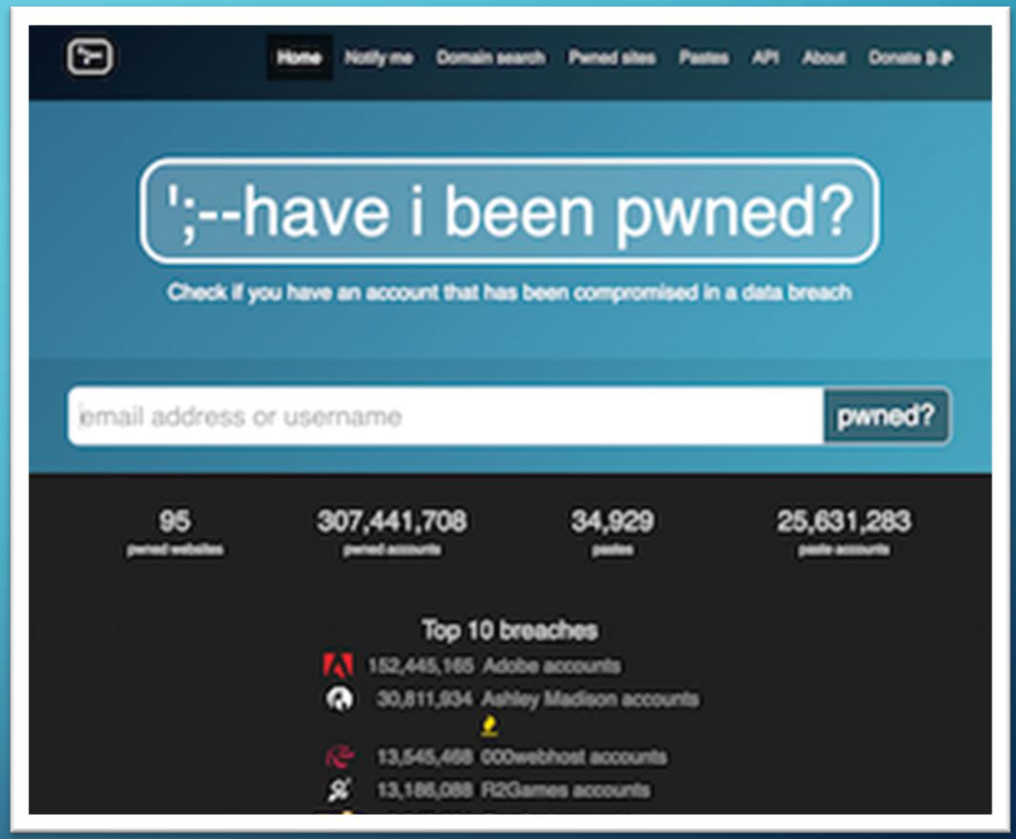
SHODAN

- Shodan не шукає веб-сайти, як, наприклад, Google, а підключені по IPv4-пдресах до Інтернету пристрої (камери відеоспостереження, роутери, датчики безпеки). Він виступає як пошукова система, яка сканує усі загальнодоступні системи з допомогою фільтрів, аби відшукати конкретні пристрої із зазначеними відкритими портами, операційними системами. Shodan індексує банери, на яких є відкриті певні порти. Прикладом відкритих для Інтернету систем є веб-камери, сервери, маршрутизатори. За допомогою Shodan можна сканувати порти знайдених систем, ідентифікувати сервіси, які на відкритих портах працюють і визначити версії таких сервісів. Shodan має функцію генерації коротких звітів щодо, наприклад, деталей CVE-коду вразливостей. Робота ресурсу ґрунтується на запитах з'єднання з безліччю можливих IP-адрес, та індексуванні отриманої шляхом цих запитів з'єднань



«HAVE I BEEN PWNED?»

- Ще одним ефективним інструментом для пасивного OSINT є «Have I been Pwned?». Цей сервіс дозволяє перевірити наявність скомпрометованих облікових даних поштових скриньок. Він архівує й використовує численні відомі витоки баз даних і перевіряє, чи введена електронна адреса була виявлена серед цих витоків. Такі витоки зазвичай відбуваються з різних джерел, і багато з них містять численні набори даних різних типів: адреси електронної пошти, паролі, імена, імена користувачів, хеші паролів, інформація платіжних карток, номери телефонів, адреси та інше.



ІНТЕРНЕТ-АРХІВ

- **The Wayback Machine** - цифровий інтернет-архів, що дозволяє побачити як сайт виглядав у минулому