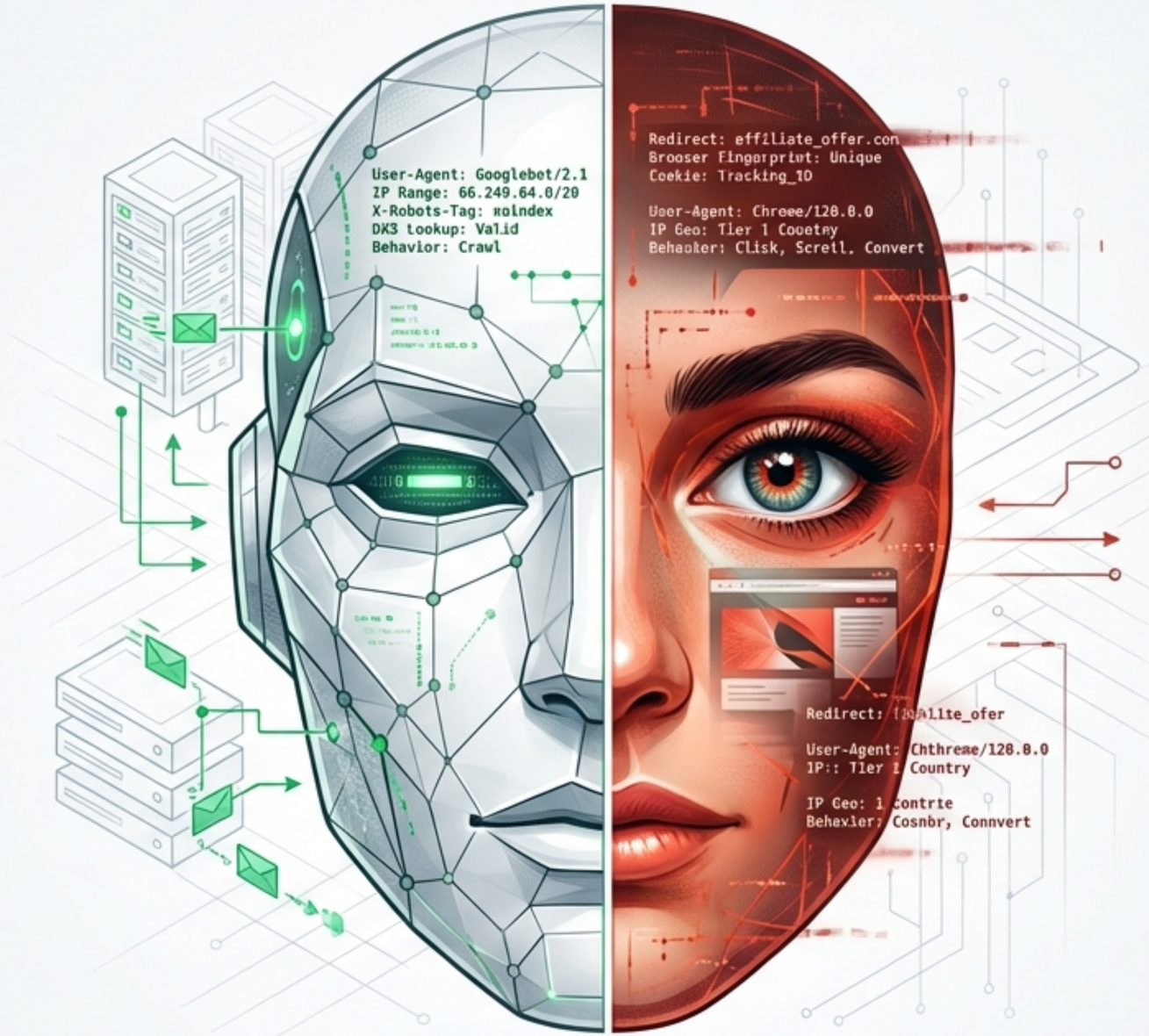
Анатомія клоакінгу

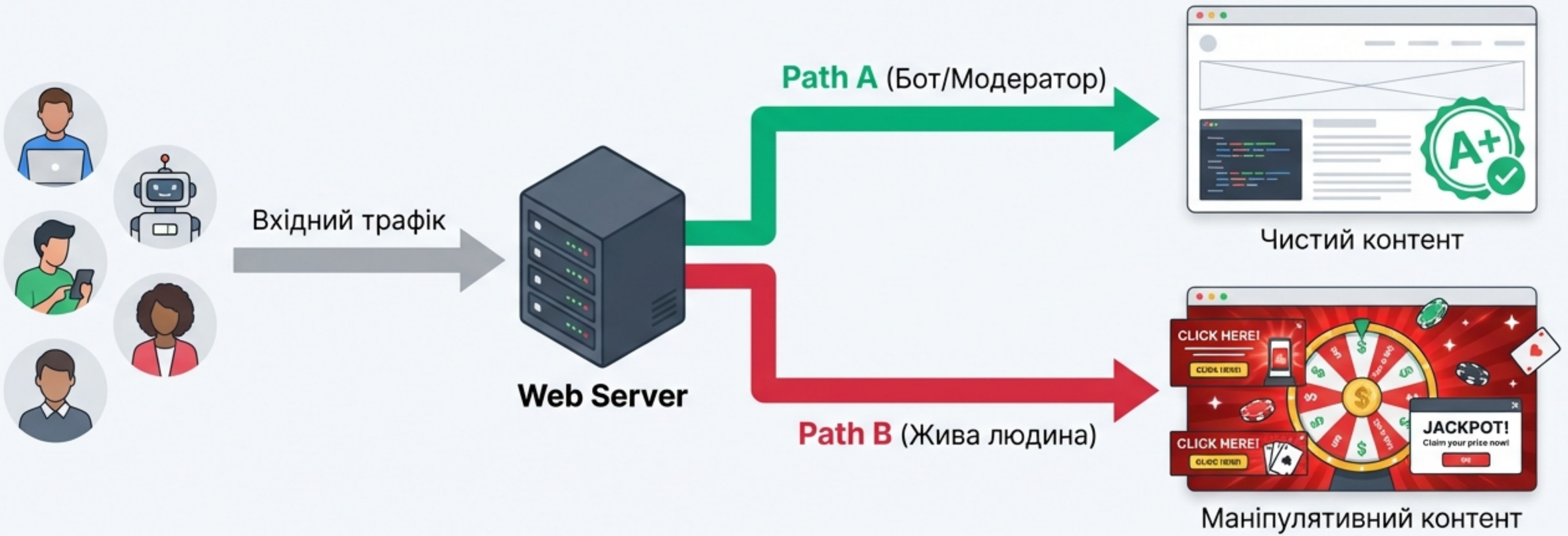
- Як сервери розрізняють людей та ботів.
- Технічний гайд з виявлення та розуміння прихованої маршрутизації трафіку в SEO та арбітражі.



Два паралельні світи на одній URL-адресі

Що це таке? Клоакінг — це метод підміни контенту, при якому пошукові роботи та звичайні користувачі бачать абсолютно різну інформацію за однією адресою.

Мета: Маніпуляція алгоритмами для отримання високих позицій або проходження модерації, приховуючи реальний вміст сторінки.



Чому вебмайстри та хакери йдуть на ризик

SEO-маніпуляції (Переоптимізація)

Швидке підвищення рейтингу за рахунок показу ботам текстів, перенасичених ключовими словами (keyword stuffing), які б відлякали реальних читачів.

Арбітраж трафіку (Обхід модерації)

Просування заборонених або "сірих" офферів (гемблінг, крипта, адалт) в Google Ads чи Facebook шляхом показу модераторам цілком легальної сторінки.

Кіберзлочинність (Приховування зломів)

Хакери маскують шкідливий код або спам-редиректи так, щоб власник сайту та антивіруси бачили нормальний ресурс, а пошуковий трафік перенаправлявся на фішинг.

Технічні тригери: як сервер впізнає «своїх»

IP-Based (За IP-адресою)

Звіряння IP-адреси відвідувача з відомими базами адрес пошукових систем (наприклад, підмережі Googlebot).

User-Agent

Аналіз ідентифікатора браузера. Якщо сервер бачить рядок на кшталт Googlebot/2.1, він активує підміну.

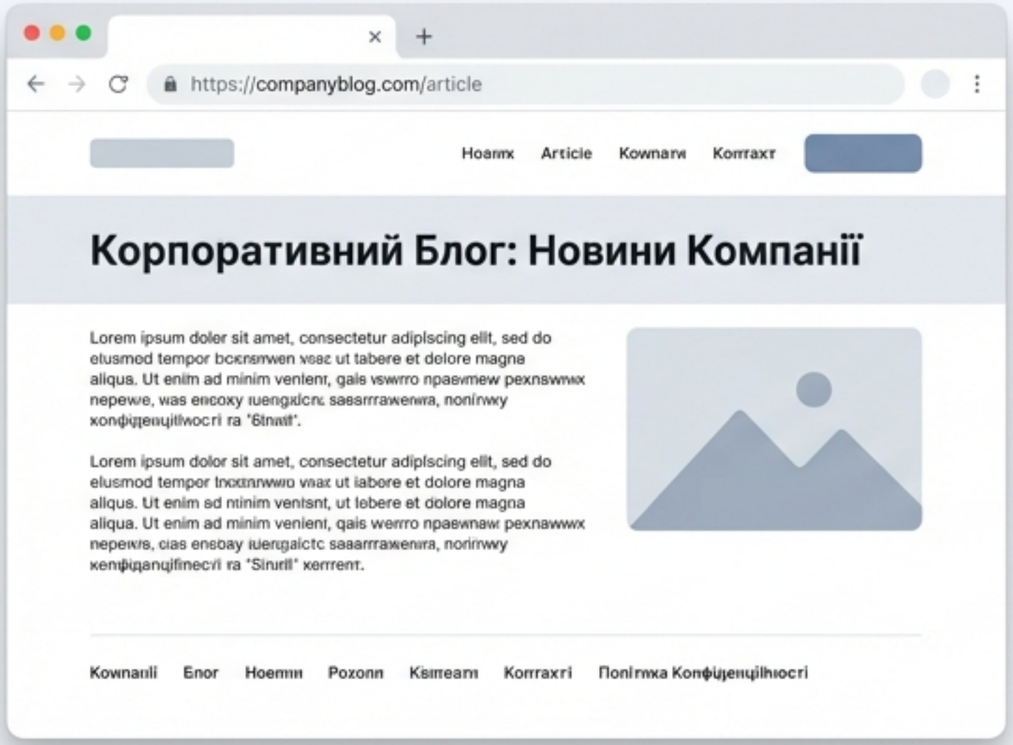
HTTP Referer

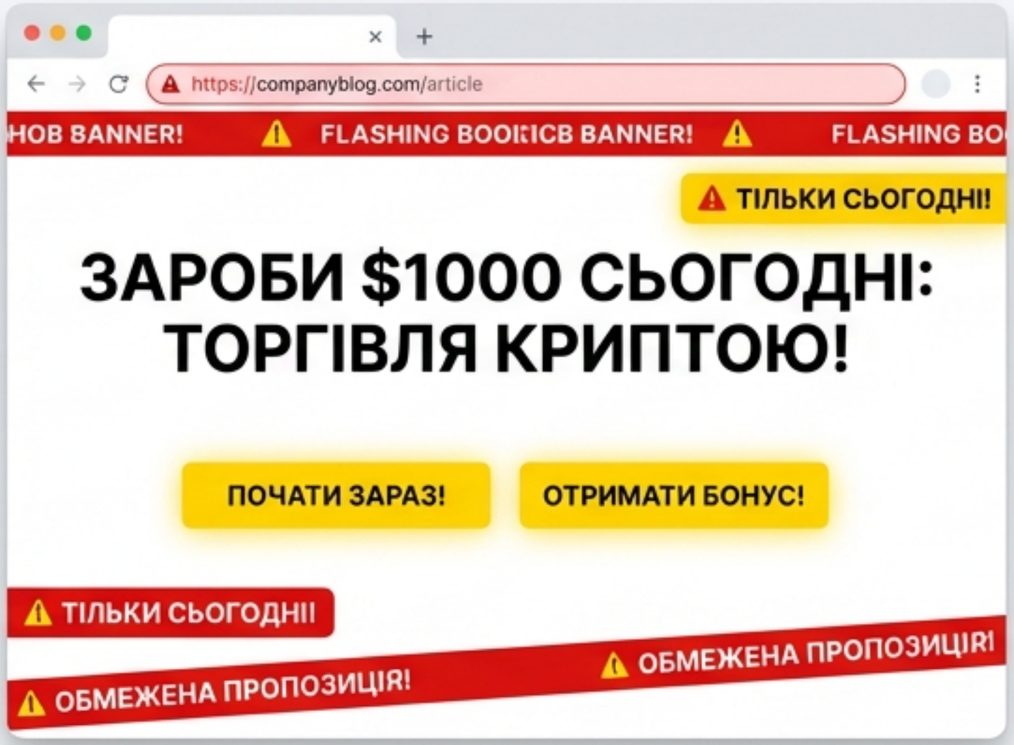
Перевірка джерела переходу. Якщо користувач прийшов з результатів пошуку — йому показують рекламу. Якщо зайшов за прямим посиланням — бачить звичайний сайт.

HTTP Accept-Language

Фільтрація за мовними налаштуваннями браузера для відокремлення ботів від локальних користувачів.

White Page проти Black Page





White Page (Для ботів): Ідеально чиста сторінка. Відповідає всім правилам рекламних мереж, має високу швидкість завантаження, політику конфіденційності та "білий" контент.

Black Page (Для цільової аудиторії): Агресивний лендінг або оффер. Саме тут відбувається продаж, збір лідів або перенаправлення на партнерські програми. Ця сторінка повністю ізольована від очей модераторів.

Шкала порушень: від «Сірого» до «Чорного»

Сірий клоакинг (Gray Hat):

Приховування частини тексту за допомогою CSS/JS-скриптів. Наприклад, розміщення невидимого тексту (білим по білому), приховування посилань розміром в один піксель або редиректи партнерських лінків (affiliate link cloaking).

Чорний клоакинг (Black Hat):

Повна підміна контенту. Фішинг, поширення шкідливого ПЗ (Malware), підміна тематики сторінки (наприклад, бот бачить "Мультфільми Disney", а користувач — порнографію або онлайн-казино).

Де проходить межа: що НЕ є клоакінгом

- **Геотаргетинг:** Зміна мови або валюти на основі IP-адреси користувача (наприклад, редирект на .fr для користувача з Франції).
- **Адаптивний дизайн:** Показ компактної версії сайту для мобільних пристроїв.
- **Paywalls (Платний доступ):** Закриття контенту для незареєстрованих користувачів, за умови використання методу Flexible Sampling (дозволяє ботам індексувати закритий текст).
- **Динамічний контент:** Використання JS для вкладок, акордеонів або тултипів.

Matt Cutts

"Золоте правило від Google: **Ставтеся до Googlebot як до звичайного користувача у стандартному браузері.**"

Ризики та незворотні наслідки

Ручні санкції та деіндексація:

Google повністю видаляє сайт з результатів пошуку за порушення Spam Policies. Відновлення вимагає повного очищення та тривалого очікування після подачі запиту на перевірку.

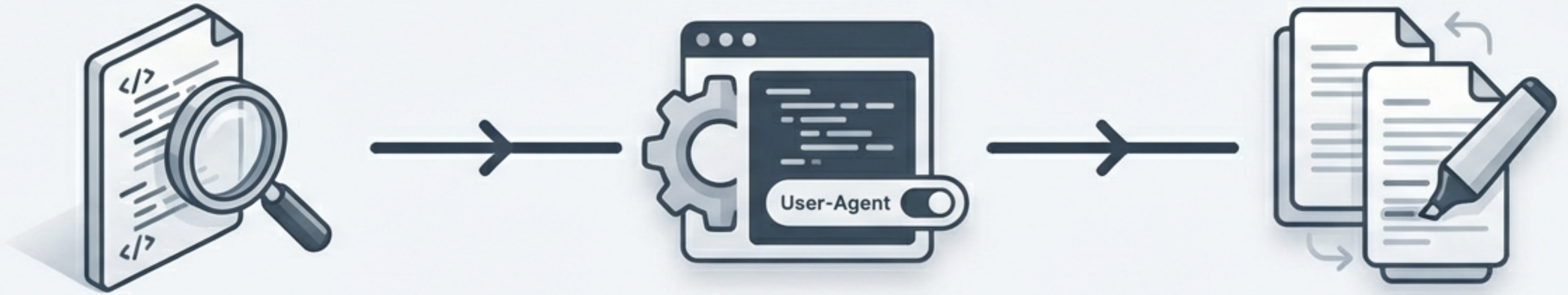
Блокування рекламних акаунтів:

Facebook та Google Ads назавжди банять акаунти рекламодавців (і пов'язані платіжні дані) при виявленні клоакінгу.

Втрата репутації:

Користувачі, які переходять за сніпетом і бачать нерелевантний контент, миттєво залишають сайт (високий Bounce Rate), що вбиває поведінкові фактори.

Чек-лист діагностики: як знайти приховану загрозу



Крок 1: Імітація бота.

Використовуйте інструмент "Переглянути як Googlebot" (Fetch as Googlebot) у Google Search Console, щоб отримати вихідний код, який бачить пошуковик.

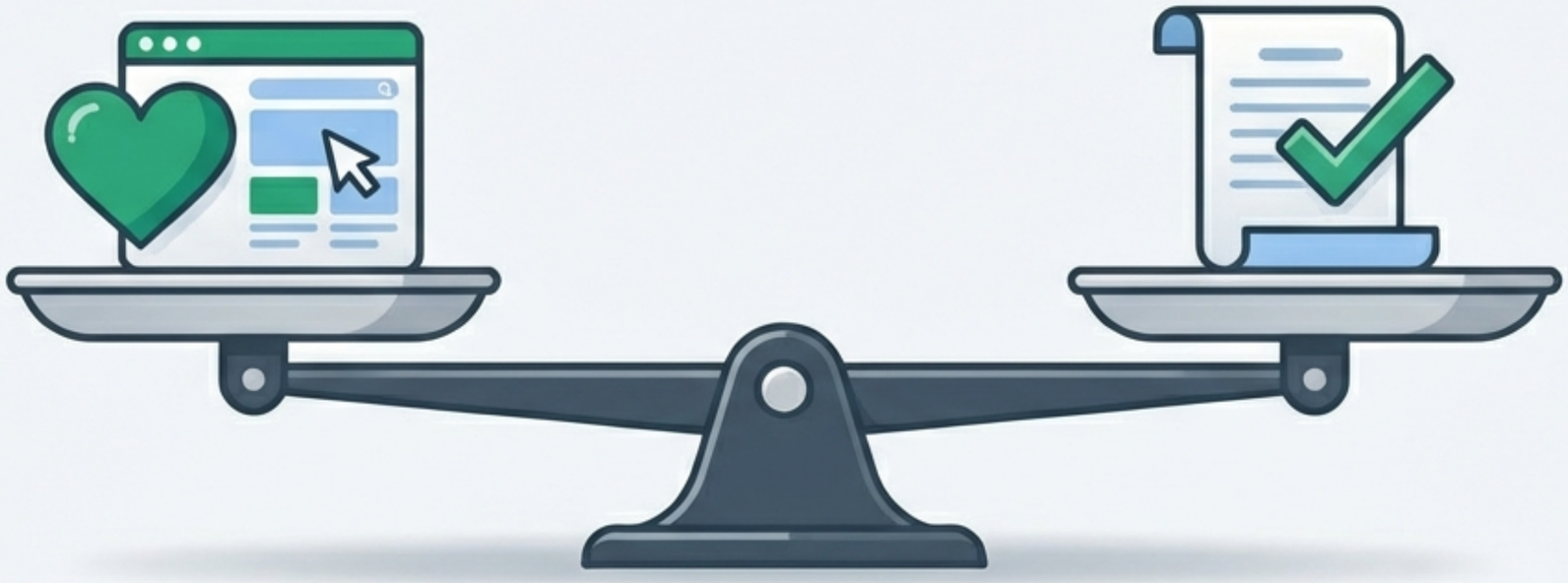
Крок 2: Підміна User-Agent.

У Chrome DevTools відкрийте Network conditions, вимкніть Use browser default та оберіть Googlebot. Перезавантажте сторінку.

Крок 3: Порівняння коду.

Скопіюйте HTML-код, який бачить користувач, та код, який бачить бот. Завантажте їх у Diffchecker.com, щоб підсвітити будь-які приховані скрипти або підмінені текстові блоки.

Прозорість — єдина стратегія успіху



- Пошукові системи безперервно **вдосконалюють алгоритми машинного навчання** для виявлення клоакінгу. Довгостроково приховати підміну неможливо.
- Замість спроб обманути ботів, **інвестуйте** ресурси у **Core Web Vitals**, якісний **семантичний контент** та справжню цінність для користувача.
- **Важливо: Регулярно перевіряйте свій сайт** на наявність хакерського клоакінгу (зловмисних редиректів), щоб захистити свій бізнес та трафік.