* **Пошук публічних документів за допомогою Google Dorks.** Використовуючи оператор intitle, знайдіть відкриті директорії з документами на сайтах освітніх установ (домен .edu). Запит: intitle:"Index of" site:\*.edu. Проаналізуйте знайдені файли на наявність корисної інформації (наприклад, презентацій чи звітів). Очікуваний результат: Список з 5-10 посилань з описом вмісту. Інструменти: Google Search.
* **Виявлення панелей адміністрування сайтів.** Застосуйте оператор inurl для пошуку сторінок входу до адмін-панелей. Запит: inurl:admin login. Виберіть 3 сайти та перевірте, чи вони захищені (без спроб входу). Очікуваний результат: Звіт про знайдені URL з аналізом потенційних вразливостей. Інструменти: Google Search.
* **Комбінування операторів Google Dorks для пошуку резервних копій баз даних.** Знайдіть SQL-файли резервних копій. Запит: inurl:backup filetype:sql. Проаналізуйте, чи файли містять чутливу інформацію. Очікуваний результат: Приклади знайдених файлів з поясненням ризиків. Інструменти: Google Search.
* **Аналіз соціальних мереж для OSINT.** Оберіть публічний профіль на Twitter (наприклад, відомої особи) та проаналізуйте активність: дати публікацій, геолокації, кола спілкування. Побудуйте схему зв’язків. Очікуваний результат: Діаграма зв’язків та висновки про активність. Інструменти: Twitter (X), Maltego або ручний аналіз.
* **Пошук інформації в китайськомовному інтернеті за допомогою Baidu.** Знайдіть бізнес-реєстри компаній у Китаї (наприклад, через QCC.com). Проаналізуйте дані про обрану компанію (адреса, контакти). Очікуваний результат: Звіт з витягнутими даними. Інструменти: Baidu Search.
* **Агрегація результатів з метапошукових систем.** Використовуючи Etools, порівняйте результати пошуку за запитом "OSINT tools" з кількох пошуковиків. Виділіть унікальні джерела. Очікуваний результат: Таблиця порівняння результатів. Інструменти: Etools.
* **Виявлення пристроїв за допомогою Shodan.** Знайдіть відкриті веб-камери в певному регіоні (наприклад, geocode: для міста). Проаналізуйте порти та сервіси. Очікуваний результат: Список пристроїв з описом вразливостей. Інструменти: Shodan.
* **Перевірка скомпрометованих email-адрес.** Введіть 5 публічних email-адрес (з новин) у Have I Been Pwned? та проаналізуйте витоки даних. Очікуваний результат: Звіт про виявлені витоки з рекомендаціями. Інструменти: Have I Been Pwned?
* **Архівування сайтів за допомогою Wayback Machine.** Знайдіть архівовані версії сайту (наприклад, bbc.com) за 2020 рік та порівняйте з поточною версією на зміни в контенті. Очікуваний результат: Скріншоти та аналіз змін. Інструменти: Wayback Machine.
* **Веб-збирання даних з новинних джерел.** Використовуючи простий скрипт на Python (з бібліотекою BeautifulSoup), витягніть заголовки новин з сайту (наприклад, cnn.com) за темою "terrorism". Очікуваний результат: Список заголовків у файлі. Інструменти: Python, BeautifulSoup.
* **Аналіз публічних даних урядових звітів.** Знайдіть урядові звіти про бюджети (наприклад, на сайті США) за допомогою Bing. Проаналізуйте демографічні дані. Очікуваний результат: Витяг звіту з ключовими фактами. Інструменти: Bing Search.
* **Пошук "сірої літератури" за допомогою Wolfram Alpha.** Запитайте статистичні дані про демографію (наприклад, "population Syria refugees") та проаналізуйте для GEOINT-контексту. Очікуваний результат: Графік або таблиця даних. Інструменти: Wolfram Alpha.
* **Моніторинг тенденцій у соціальних мережах.** За допомогою Twitter Advanced Search (x\_keyword\_search) знайдіть пости з хештегом #OSINT за останній місяць. Проаналізуйте настрої. Очікуваний результат: Топ-10 постів з аналізом. Інструменти: Twitter (X).
* **Використання Brave Search для анонімного OSINT.** Знайдіть інформацію про компанію без трекінгу (наприклад, "company vulnerabilities"). Порівняйте з Google. Очікуваний результат: Порівняльний звіт. Інструменти: Brave Search.
* **Аналіз даних з інструментами агрегації.** Зберіть дані з кількох джерел (новини, соцмережі) про подію (наприклад, "Syria refugees") та агрегуйте в Excel. Очікуваний результат: Таблиця з патернами. Інструменти: Excel.
* **Пошук мультимедійного контенту за допомогою Lycos.** Знайдіть архівні відео про військові операції. Проаналізуйте на релевантність OSINT. Очікуваний результат: Список відео з описом. Інструменти: Lycos.
* **Виявлення зв’язків за допомогою FaganFinder.** Пошукайте інформацію про особу (публічну фігуру) через спеціалізовані пошуки (люди, документи). Побудуйте профіль. Очікуваний результат: Профіль з джерелами. Інструменти: FaganFinder.
* **Перевірка фактів з кількох джерел.** Оберіть суперечливу тему (наприклад, "OSINT usage in USA") та перевірте в Google, Bing та Yahoo. Узагальніть. Очікуваний результат: Звіт з підтвердженнями/спростуваннями. Інструменти: Google, Bing, Yahoo.
* **Комплексний OSINT-аналіз для військових цілей.** Імітуючи підхід Ізраїлю (Hatsaf), зберіть дані про військову спроможність країни з відкритих джерел (новини, звіти). Застосуйте коефіцієнти ваги для об’єктивності. Очікуваний результат: Структурований звіт з джерелами. Інструменти: Пошукові системи, Wayback Machine.