

ДО БЕЗПЕЧНІШОЇ ЕКОСИСТЕМИ УКРАЇНСЬКИХ ЗМІ ТА ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА: ЯК МОЖЕ ДОПОМОГТИ РОЗВІДКА ВІДКРИТИХ ДЖЕРЕЛ (OSINT)

ІНСТРУМЕНТИ ТА ЗАХОДИ БЕЗПЕКИ, ЯКІ МОЖНА ВИКОРИСТОВУВАТИ
ДЛЯ СПРОСТУВАННЯ ПРОПАГАНДИ ТА ПЕРЕВІРКИ ІНФОРМАЦІЇ В
ІНТЕРНЕТІ ПІД ЧАС КОНФЛІКТУ З РОСІЄЮ, ЩО ТРИВАЄ

НАТАЛІЯ АНТОНОВА

РОМАН ОСАДЧУК

ЛУКАС АНДРІУКАЙТІС

У ПАРТНЕРСТВІ З ІНСТИТУТОМ БЕЗПЕКИ ТА ТЕХНОЛОГІЙ ТА ЦИФРОВОЇ
КРИМІНАЛІСТИЧНОЇ ЛАБОРАТОРІЇ АТЛАНТИЧНОЇ РАДИ

СЕРПЕНЬ 2022 РОКУ

ЗМІСТ

ОГЛЯД СИТУАЦІЇ	1
ЯК ПЕРЕВІРИТИ ВІДЕО У ЧАС КОНФЛІКТУ	2
РОЗШИРЕНИЙ ПОШУК ТА YOUTUBE	3
КОРИСНІ ІНСТРУМЕНТИ ТА ПЛАГІНИ	4
ДОСЛІДЖЕННЯ ЕКСТРЕМІЗМУ	7
ПОШУК ЗА ГЕОТАГАМИ	8
ЗОБРАЖЕННЯ, СТВОРЕНІ ШІ	9
ЯК ЗВОРОТНИЙ ПОШУК ЗОБРАЖЕНЬ, ПЕРЕВІРКА ТА ДОСЛІДЖЕННЯ МЕТА-ДАНИХ МОЖЕ ДОПОМОГТИ БОРОТИСЯ З ДЕЗІНФОРМАЦІЄЮ З ВИКОРИСТАННЯМ ЗОБРАЖЕНЬ....	9
ЗВОРОТНИЙ ПОШУК ЗОБРАЖЕНЬ ТА АНАЛІЗ ФОТОГРАФІЙ МОЖУТЬ ПРОТИДІЯТИ ПРОПАГАНДІ.....	10
ВІД GOOGLELENS ДО ГЕОЛОКАЦІЇ.....	13
ЗНАЙОМСТВО ІЗ ВИКОРИСТАННЯМ ТІНЕЙ ПРИ АНАЛІЗІ ФОТОГРАФІЙ.....	14
ЯК ПРАЦЮЄ ТЕЛЕГРАМ + ТА ЯКІ В НЬОГО ВРАЗЛИВОСТІ	15
ТЕМНІ МЕРЕЖІ ТЕЛЕГРАМ	16
ДВА НАЙКРАЩИХ ІНСТРУМЕНТИ ТЕЛЕГРАМ	16
ДОДАТКОВІ РЕСУРСИ.....	19
ВИСНОВОК	19

Інститут безпеки та технологій та автори цього звіту запрошують вільно використовувати наведену в ньому інформацію для навчальних для цілей, за умови чіткого цитування повного джерела у відтвореному матеріалі.

У партнерстві з [Лабораторією цифрових криміналістичних досліджень Атлантичної ради](#).

Висловлені в цьому тексті погляди належать виключно авторам.

Copyright 2022, Інститут безпеки та технологій



ОГЛЯД СИТУАЦІЇ

Перевірка інформації та боротьба з діпфейками—необхідна навичка будь-якого журналіста, і вона стає ще важливішою під час війни. В умовах нинішньої атаки Росії на Україну як українська екосистема ЗМІ, так і екосистема ЗМІ всього світу зазнають навали російської воєнної пропаганди та дезінформації, що розроблені для заплутування та деморалізації українців та їхніх союзників.

Цей посібник призначений для українських журналістів та для тих, хто висвітлює події війни Росії проти України, щоб познайомити їх із деякими з найкращих інструментів та практик виявлення дезінформації, яка розповсюджується через відео, зображення, а також канали Telegram, та шляхів боротьби із нею.

Згідно інформації від Сполучених Штатів та інших урядів Заходу, Росія склала список ключових осіб для захоплення на українських територіях і, можливо, їхнього подальшого вбивства. Це означає, що безпека ключової інформації є справою надзвичайної важливості у спротиві російській загрозі.

Цей посібник пропонує практичні поради із захисту вашої цифрової діяльності та покращення вашої цифрової гігієни. Для цілей цього посібника ми визначаємо цифрову гігієну як набір регулярних практик, які спрямовані на безпеку цифрових активів та цифрового сліду.

Зауважте: *Оскільки технологія постійно розвивається та еволюціонує, те саме відбувається із загрозою дезінформації. Через це важливо не відставати від найновіших розробок у сфері дезінформації в Інтернеті. Використовуйте цей посібник, але не забувайте відслідковувати надійні джерела з питань російської дезінформації та пропаганди, щоб не пропустити нововведення або зміни у тактиці.*

ЯК ПЕРЕВІРИТИ ВІДЕО У ЧАС КОНФЛІКТУ

Відео—це важливий інструмент в арсеналі дезінформації Росії, особливо через те, що більшість широкого загалу мають труднощі з аналізом візуального та аудіо-компонентів. Редагування відео з метою введення в оману може також просувати дезінформацію російської сторони. Тому, коли ми зважаємо на важливість відеоматеріалів, не забуваймо, наскільки популярні такі ресурси, як YouTube, в Росії:

Користувачі YouTube

Year	Users
2012	800,000,000
2013	1,000,000,000
2014	1,100,000,000
2015	1,200,000,000
2016	1,400,000,000
2017	1,500,000,000
2018	1,800,000,000
2019	2,000,000,000
2020	2,300,000,000

Джерело: YouTube

Найпопулярніші країни за версією користувачів Youtube

	Country	Users
1.	 Індія	225,000,000
2.	 США	197,000,000
3.	 Бразилія	83,000,000
4.	 Японія	60,000,000
5.	 Росія	58,000,000

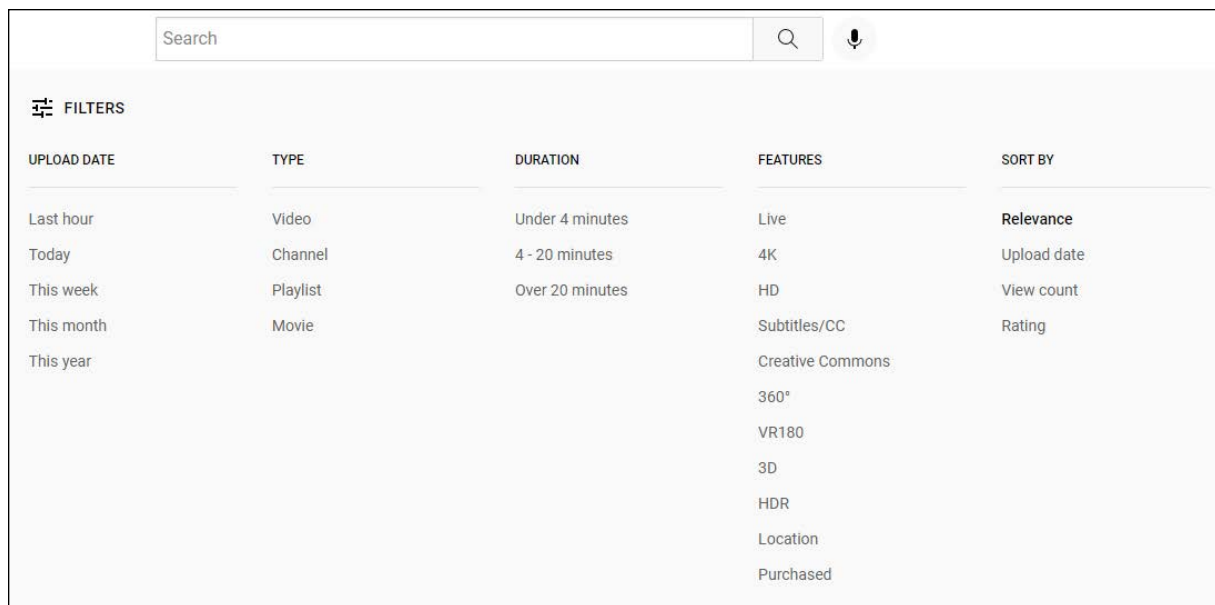
Джерело: Global Media Insights

Як показали [численні звіти](#) та [дослідження](#), алгоритми YouTube допомагають у розповсюдженні оманливої інформації на цій платформі, створюючи безкінечні порочні кола, які включають дезінформацію та теорії змов. Російська дезінформація не є тут винятком і тому може легко розповсюджуватися на платформі — це може шкодити діям української сторони у війні як всередині країни, так і за кордоном та сіяти розгубленість і недовіру між українцями та їхніми союзниками по всьому світу.

РОЗШИРЕНИЙ ПОШУК ТА YOUTUBE

Щоб ретельно дослідити відео на YouTube та зрозуміти їх потенційний вплив, а також для того, щоб розвінчати брехню або невірно подану інформацію у цих відео, важливо спочатку ознайомитися з фільтрами YouTube та з розширеним пошуком на цій платформі. Це буде особливо корисно, якщо ви захочете дізнатися про історію певного відео (наприклад: коли воно вперше з'явилося). Також це корисно для пошуку відео за певною темою, щоб з'ясувати, як ця конкретна тематика висвітлюється на платформі — процес, що корисний для розвінчування, підготовки репортажів, а також документування потенційно шкідливого змісту:

Фільтри YouTube і розширений пошук



Для поглибленого вивчення питання просто скористатися стандартним пошуком YouTube, скоріше за все, буде недостатньо, оскільки алгоритм YouTube може спотворити результати і згаяти ваш час (а під час війни час—дорогоцінна річ). Використовуючи розширений пошук, можна відфільтрувати відео за датою завантаження, довжиною та за особливостями, при цьому можна використовувати різні способи сортування. *ПРИМІТКА: коли ви шукаєте якусь конкретну фразу чи словосполучення, пошуковий запит треба вводити, використовуючи лапки.*

Визначення джерела відео та визначення конкретних осіб та місць на відео може бути легшим, якщо ви використаєте зворотний пошук зображень за скріншотами кадрів вказаного відео. Зворотний пошук зображень—це процес, за допомогою якого ви можете встановити, де ще публікувався цей скріншот та зображення. *ПРИМІТКА: якщо предмет дослідження не простий, вам варто використовувати декілька різних інструментів зворотного пошуку зображень.*

Ось декілька інструментів, які ви можете використовувати, вивантажуючи конкретний

скріншот:

Інструменти зворотного пошуку зображень

Name	URL
Yandex	yandex.com/images
Bing	bing.com/visualsearch
TinEye	tineye.com
Google Images	images.google.com

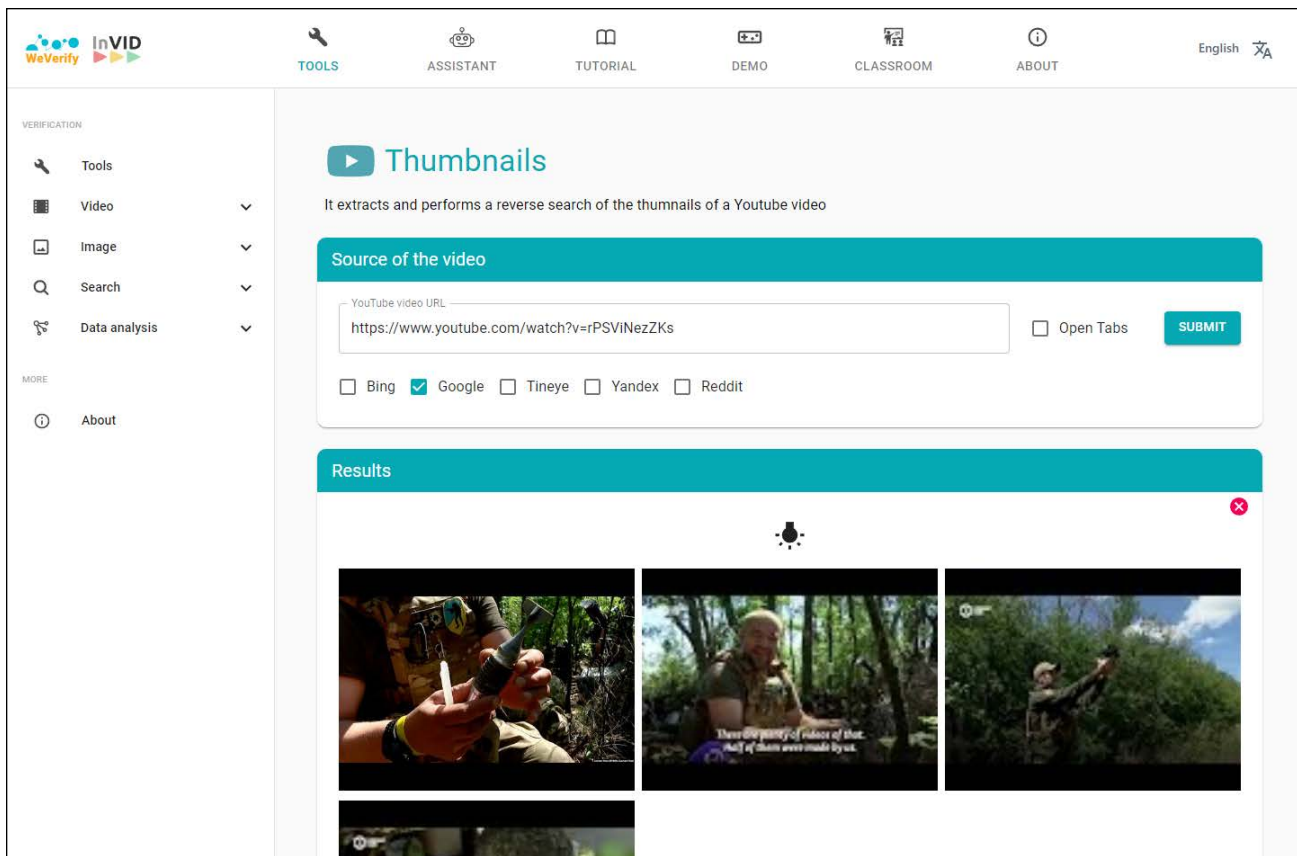
Google, TinEye, Bing і Yandex є популярними інструментами зворотного пошуку зображень. Однак зауважте, що Яндекс є російською компанією. Будьте обережні, використовуючи платформи, пов'язані з Росією, у контексті конфлікту в Україні.

КОРИСНІ ІНСТРУМЕНТИ ТА ПЛАГІНИ

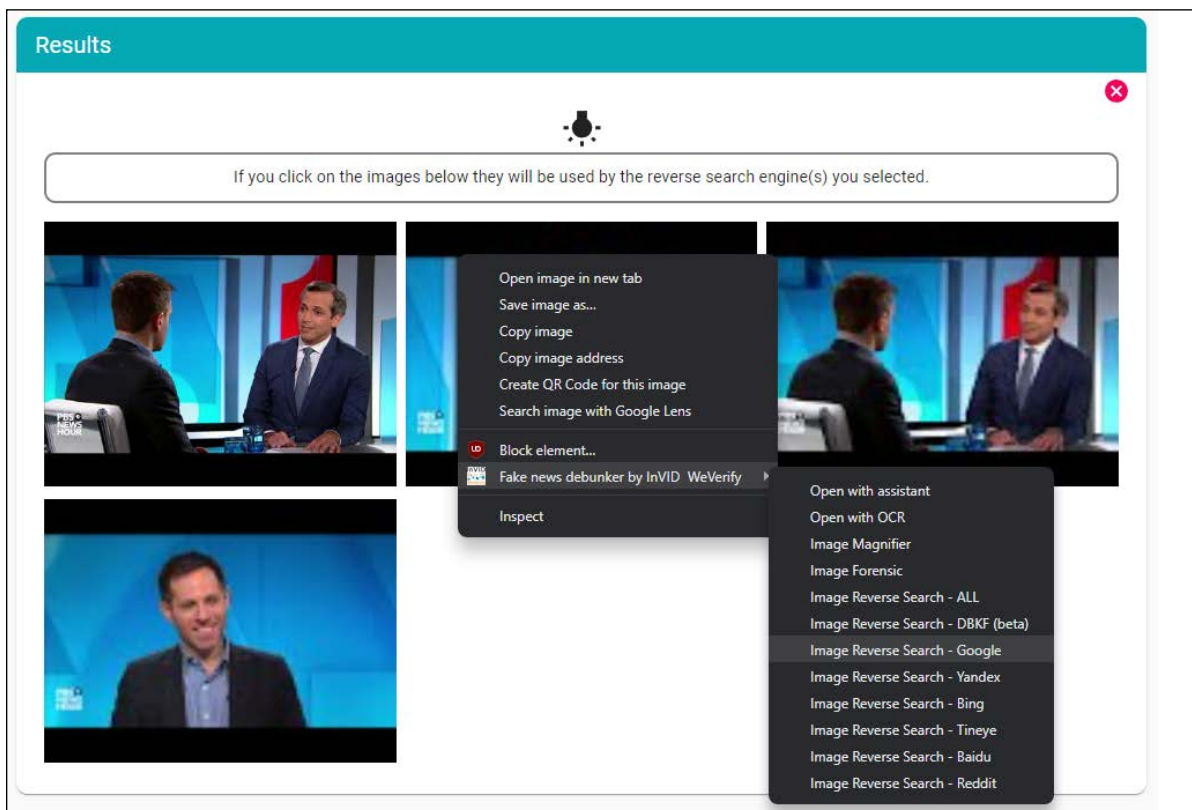
Для складніших або ширших тем, коли потрібно більше даних для перевірки або спростування відеоматеріалу, існують широкодоступні інструменти для аналізу відео. Один з них—[YouTube DataViewer](#) від Amnesty International, а також плагін [InVID plugin](#).

Плагін InVID може зекономити дослідникові час, коли потрібно провести зворотний пошук зображень, аналізуючи мініатюри YouTube (зображення передперегляду відео на сторінці YouTube). Наприклад, на початку пандемії COVID-19, відео яке описувалося як реальне, відзняте жертвами COVID-19, що спричинило швидке розповсюдження цього відео, після аналізу за допомогою InVID виявилось фрагментом кінострічки. Такі історії показали, як пошук скріншотів з використанням плагіна може допомогти зупинити дезінформацію.

Пошук InVID через скріншоти негайно приводить нас до фільму, який нічого спільного не має з COVID, як можна бачити на зображенні вище. Виявляти подібного роду оманливу інформацію особливо важливо, бо Росія дуже часто відмиває діпфейки, намагаючись зробити їх вірусними в інших країнах — зауважте, як [індійські користувачі Twitter](#) розповсюджують підробки від Росії, які спрямовані проти України.

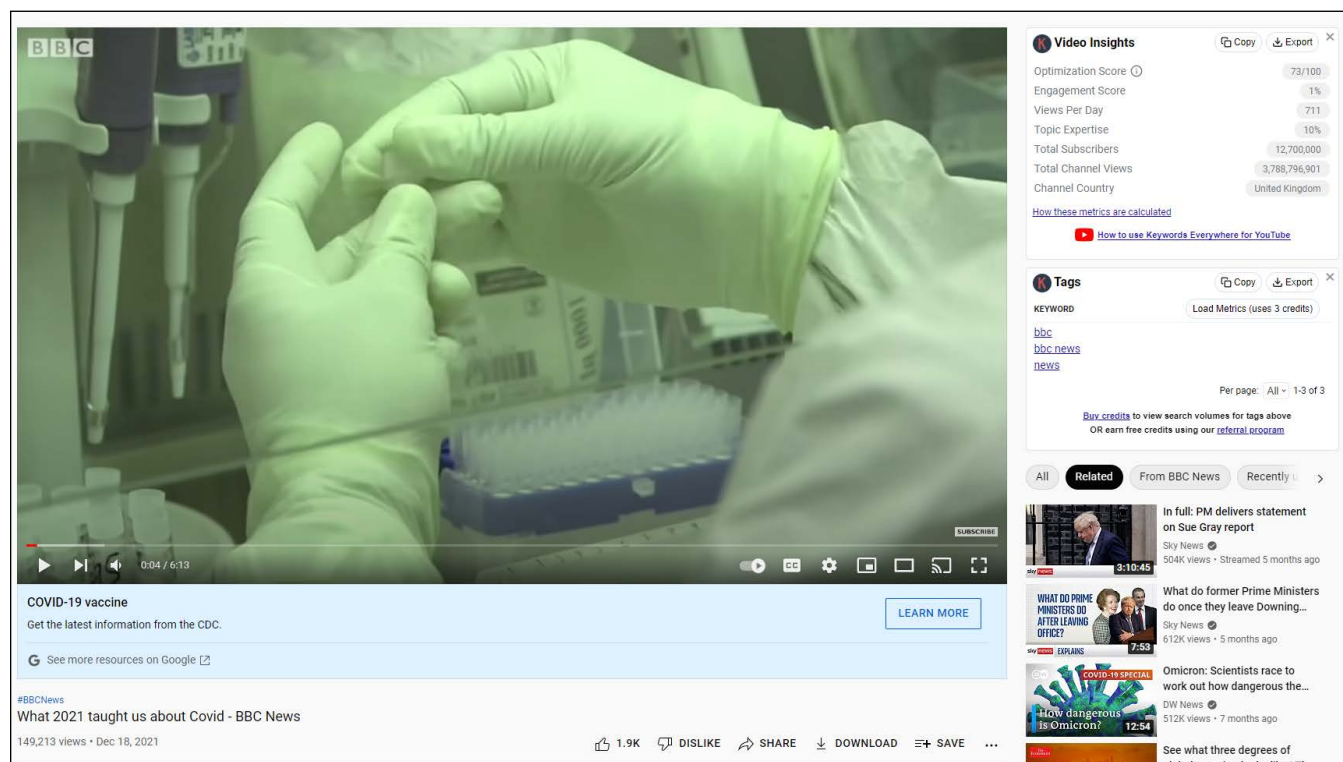


Використовуючи InVID, ви можете легко вибрати, які саме пошуковики використати у зворотному пошуку зображення — всі пошуковики стандартні, вам не потрібно їх завантажувати, щоб використовувати:



Коли ви спростовуєте дезінформацію, важливо розуміти, наскільки конкретне відео розповсюдилось та які в нього були показники — знаючи це, можна приблизно уявити його вплив і відслідкувати, як воно розповсюджується.

Інструмент [Keywords Everywhere](#) особливо корисний для цієї мети. Зауважте інформацію, яку він надає для цього відео BBC, котре ми взяли в якості прикладу. Ви можете використовувати цей інструмент для аналізу відео з джерел, що мають репутацію чи відомість набагато гіршу, ніж BBC, і отримати набагато більше прозорості:



The screenshot displays a YouTube video player for a BBC News video titled "What 2021 taught us about Covid - BBC News". The video content shows a person in a white lab coat and gloves working with laboratory equipment, including a pipette and a multi-well plate. The video player interface includes a progress bar, play/pause button, and a "SUBSCRIBE" button. Below the video player, there is a description area with the text "COVID-19 vaccine" and "Get the latest information from the CDC." and a "LEARN MORE" button. To the right of the video player, there is a "Video Insights" panel from Keywords Everywhere. This panel provides various metrics for the video, including Optimization Score (73/100), Engagement Score (1%), Views Per Day (711), Topic Expertise (10%), Total Subscribers (12,700,000), Total Channel Views (3,788,796,901), and Channel Country (United Kingdom). Below these metrics, there is a "Tags" section showing the keyword "bbc" and its search volume (1.9K). The panel also includes a "How to use Keywords Everywhere for YouTube" link and a "Buy credits" button.

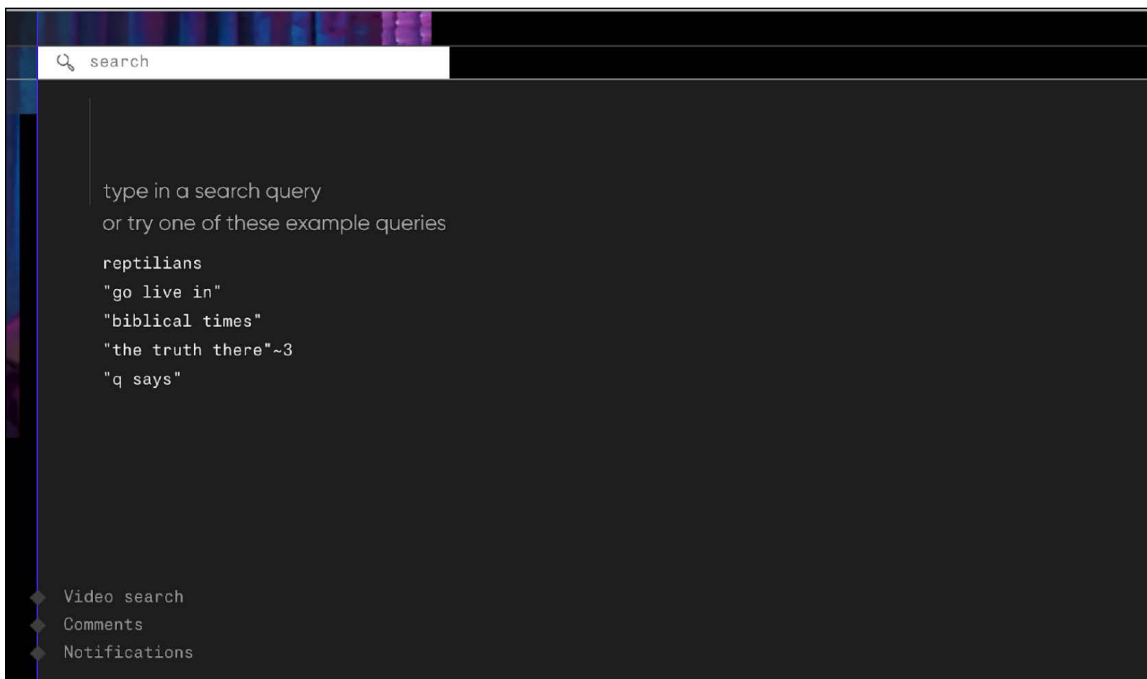
Metric	Value
Optimization Score	73/100
Engagement Score	1%
Views Per Day	711
Topic Expertise	10%
Total Subscribers	12,700,000
Total Channel Views	3,788,796,901
Channel Country	United Kingdom

Keyword	Search Volume
bbc	1.9K

ДОСЛІДЖЕННЯ ЕКСТРЕМІЗМУ

Якщо ви працюєте у сфері дослідження радикального екстремізму, вам варто використувати Raditube в якості посібника для розуміння відеоматеріалів екстремістів. Зважайте на те, що екстремісти крайнього правого спектру в США вже давно допомагають розповсюджувати російську пропаганду, оскільки вона легко просочується з однієї відповідної екосистеми до іншої.

Raditube може допомогти виявити зв'язки та спільні теми на різних каналах, а також історію каналів:



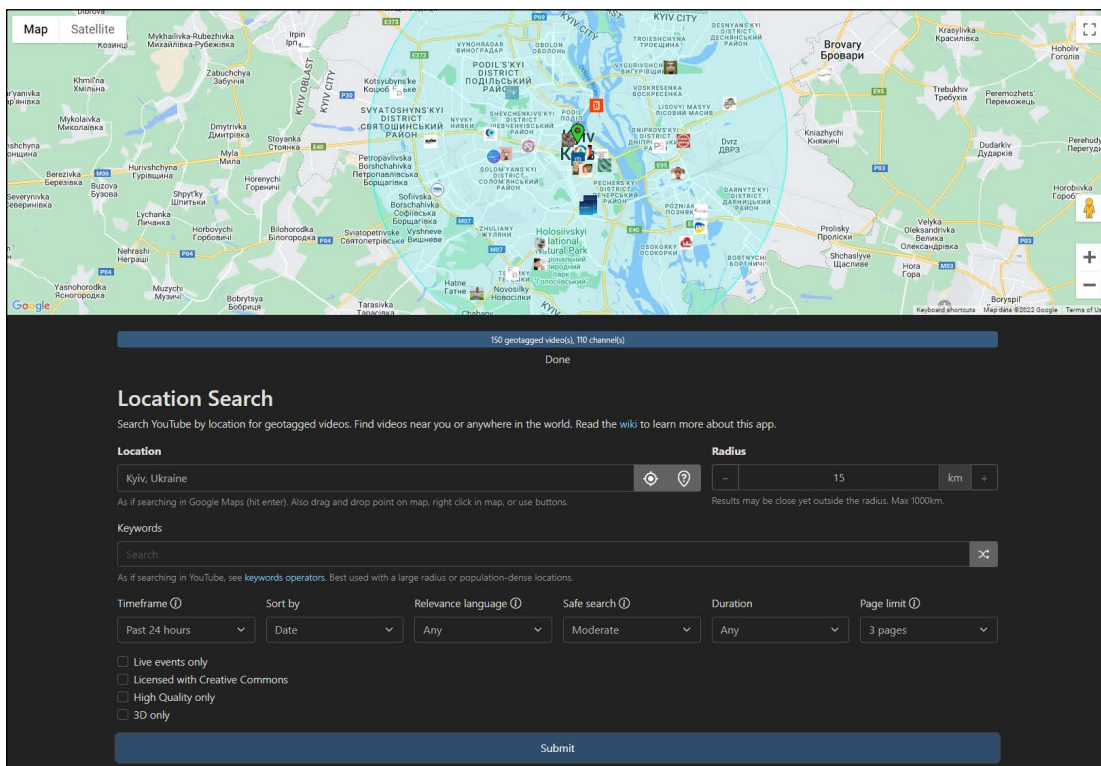
Raditube корисний тим, що він показує статус окремих каналів, а також їх статистику— таким чином, ви знаєте, які з них продовжують залишатися активними:

channel name	status	views	subscribers	videos	since
#PedoGate	removed	9.882 views	0 subs	19 videos	2017-0
#SeekingTheTruth JoshWho News	removed	21.813.536 views	98.500 subs	833 videos	2016-0
AMTV	active	527.951 views	693.000 subs	11 videos	2007-0
And We Know	removed	21.773.688 views	346.000 subs	110 videos	2011-0
Annette Cividanes	removed	10.932.824 views	88.300 subs	424 videos	2014-0
Anon 7	removed	76.855 views	1.500 subs	141 videos	2014-1
April LaJune, copyright Holder	active	1.363.434 views	78.000 subs	513 videos	2010-1

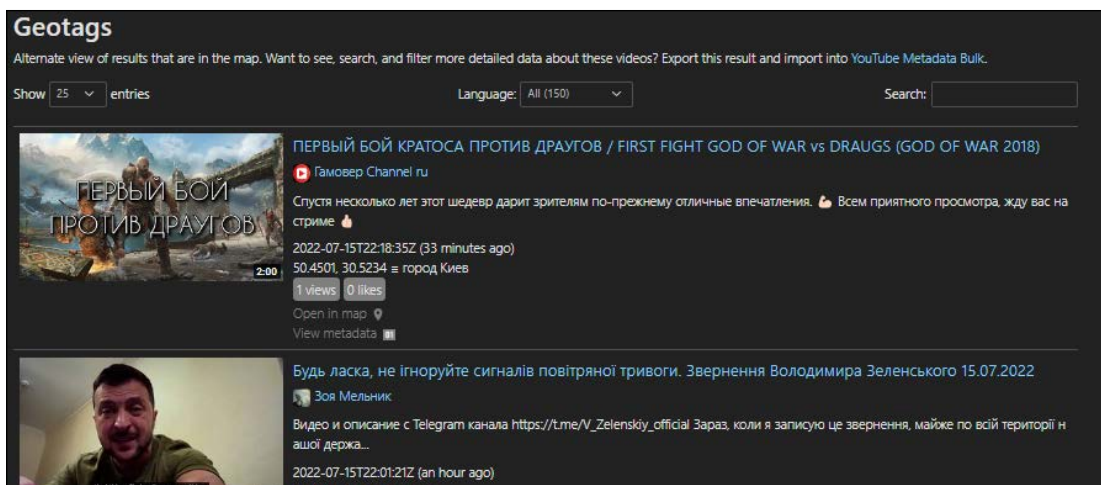
ПОШУК ЗА ГЕОТАГАМИ

І нарешті, [YouTube GeoFind](#) це інструмент, котрий може допомогти вам зберегти час, шукаючи відмічені геотагами відео за місцезнаходженням. Це надзвичайно корисно під час конфлікту, оскільки приблизно з однієї локації завантажують багато відео як під час бойових операцій, так і під час інших подій.

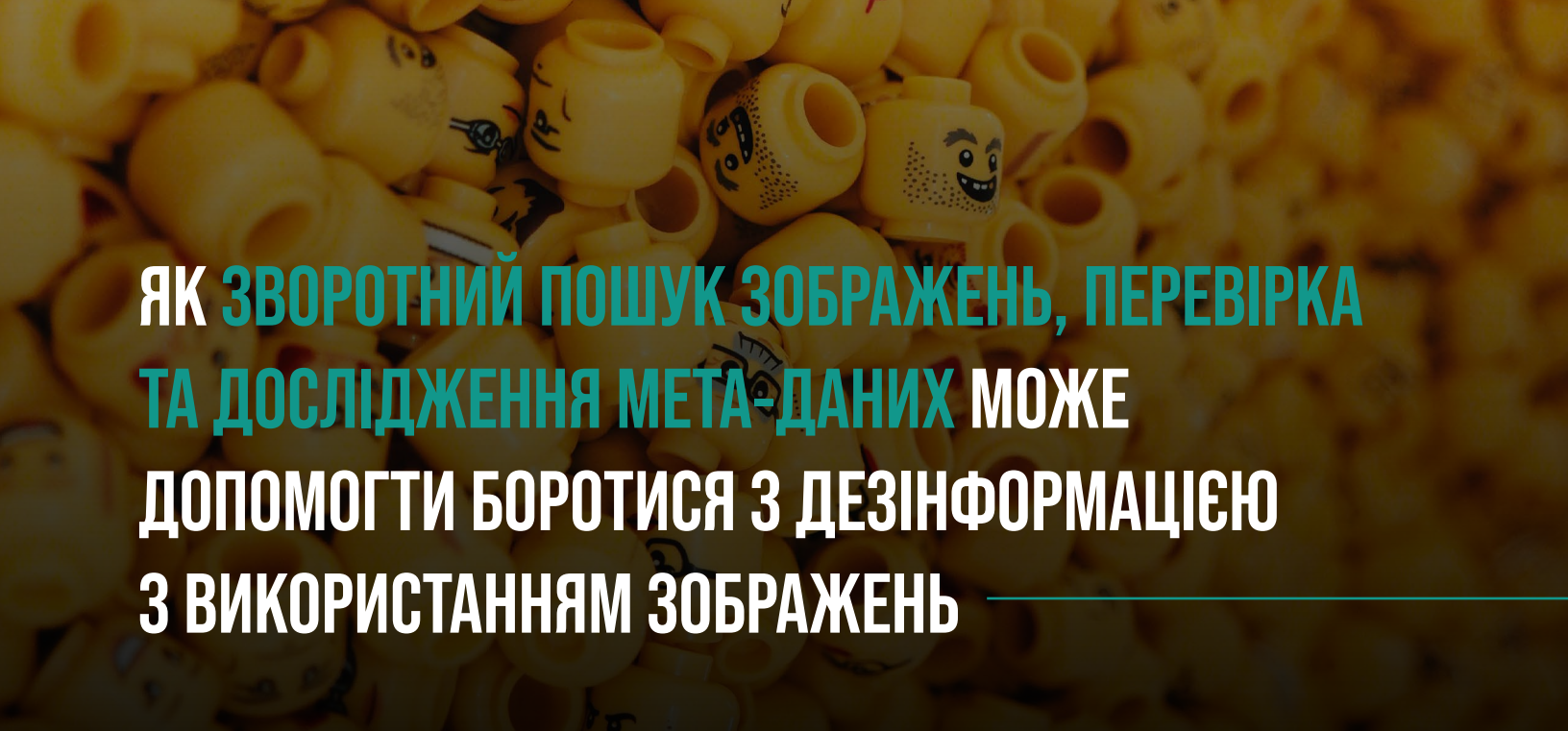
Ось типовий пошук для всіх відео з геотагом «Київ, Україна». Зауважте, будь ласка, що вам треба натиснути “submit” («подати»), коли ви заповните всю релевантну інформацію з фільтрування у підказках на сторінці:



Результати з'являться під кнопкою «Submit»:



До безпечнішої екосистеми українських ЗМІ та громадянського суспільства:
як може допомогти розвідка відкритих джерел (OSINT)



ЯК ЗВОРОТНИЙ ПОШУК ЗОБРАЖЕНЬ, ПЕРЕВІРКА ТА ДОСЛІДЖЕННЯ МЕТА-ДАНИХ МОЖЕ ДОПОМОГТИ БОРОТИСЯ З ДЕЗІНФОРМАЦІЄЮ З ВИКОРИСТАННЯМ ЗОБРАЖЕНЬ

Аналіз зображень під час війни є критично важливим для виявлення дезінформації та підтвердження фактів на місцях. Хоча багато принципів роботи залишаються такими самими, як і для вивчення відео, інструменти для цього використовуються інші.

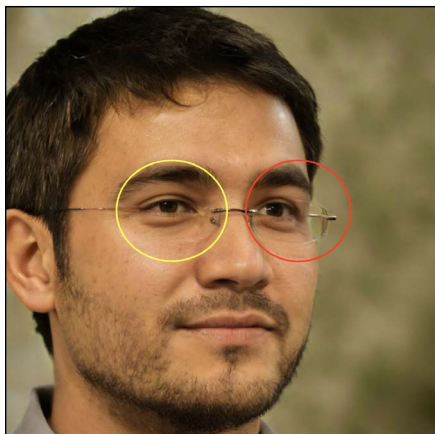
Робота з одним зображенням також означає, що у вас менша контактна поверхня для пошуку — отже, слід відточити увагу, щоб помічати дрібні деталі, які звичайний глядач часто пропускає.

ЗОБРАЖЕННЯ, СТВОРЕНІ ШІ

Часто починати доводиться з аналізу джерела зображення. Зараз створені штучним інтелектом (ШІ) зображення можуть допомагати троям та пропагандистам і навіть використовуватись у створення цілих фальшивих персоналій в мережі—з метою розповсюдження дезінформації.

Цієї особи не існує—це вебсайт, який допоможе вам ознайомитися із тим, наскільки добре може працювати цей ШІ. Натисніть на “refresh” («оновити»), щоб з легкістю згенерувати обличчя неіснуючої особи, яке можна використати для фальшивої мережевої персоналії.

Будь ласка, зауважте: асиметричність може вказати зображення, створені штучним інтелектом. Це часто проявляється, коли людина на зображенні носить окуляри. Зверніть увагу—окуляри не відображаються належним чином:



Тим не менше, мірою покращення ШІ профілі з подібними підробними фото можуть вводити в оману все більше людей. Тому важливо не втрачати пильності і ретельно розбирати будь-яке підозріле джерело — не забувайте, надійні джерела зазвичай мають солідний цифровий слід, котрий має багато дрібних деталей, тобто, вони видаватимуться більш “людськими”, на відміну від ідентичностей, які спеціально створені, щоб відповідати вашим інтересам і змусити вас ігнорувати червоні прапорці стосовно ідентичності цього облікового запису. Дрібні деталі, про які

йшлося вище, можуть включати будь-що—від невдалих фотографій до близьких сімейних зв’язків, які можна побачити в індивідуальному цифровому відбитку профіля.

ЗВОРОТНИЙ ПОШУК ЗОБРАЖЕНЬ ТА АНАЛІЗ ФОТОГРАФІЙ МОЖУТЬ ПРОТИДІЯТИ ПРОПАГАНДІ

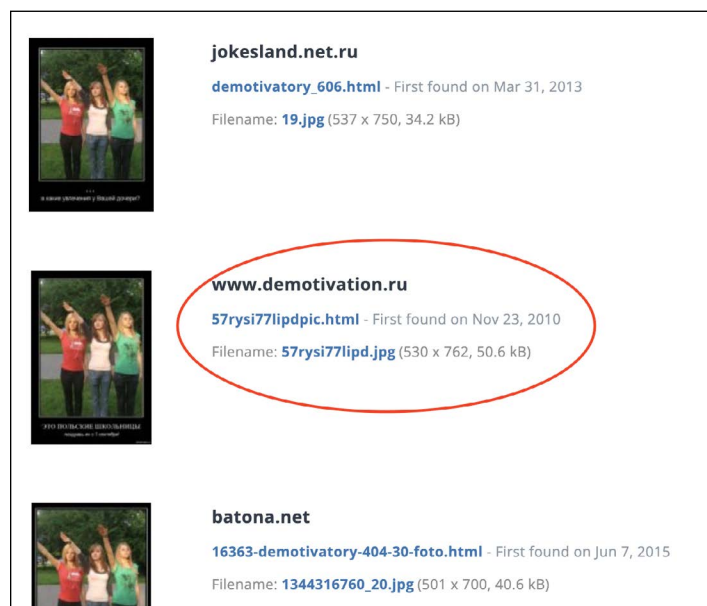
Велике занепокоєння стосовно зображень викликає те, як вони просочуються з російської екосистеми до західної—часто без необхідного контексту.

Наприклад, це зображення було заявлено російською пропагандою як фото Катерини Прокопенко, дружини українського захисника Азовсталі. Метою публікації зображення була дискредитація Прокопенко, коли вона відвідувала Папу, прохаючи його втрутитися у ситуацію із захисниками Азовсталі в Україні, які потрапили у пастку. Це зображення потім розповсюдилося в англомовному Твіттері, а звідти його, не перевіряючи, поширили користувачі з Америки, таким чином підтримуючи зусилля російської пропаганди:



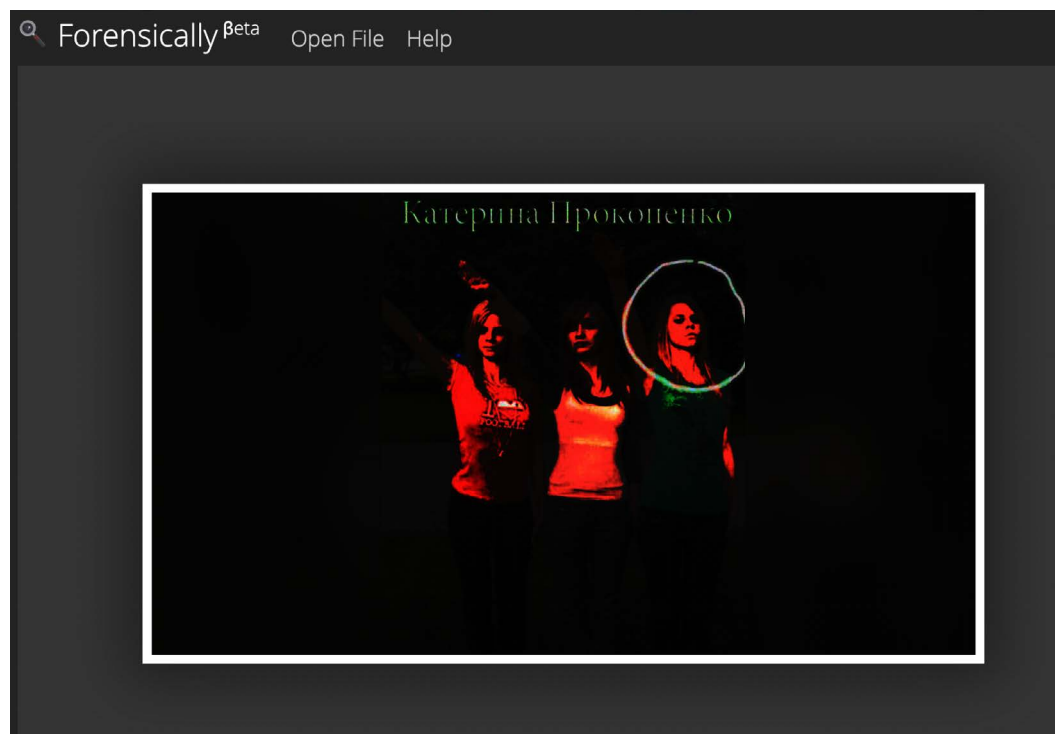
В той час як жінка праворуч має віддалену схожість із Прокопенко, швидкий візуальний аналіз дозволить вам помітити польський прапор на футболці жінки зліва. Це перша підказка, яка вказує, що ми маємо справу з дезінформацією.

Швидкий зворотний пошук зображення за допомогою такого корисного інструменту, як [TinEye](#) може підтвердити, що одним з перших джерел публікації сайту був російський сайт мемів дванадцять років тому. Підвантаживши це зображення до TinEye, ми можемо побачити довгу історію використання цього зображення на різних вебсайтах, включаючи російські сайти мемів десятирічної давнини, і визначити, що жінка праворуч просто схожа на Прокопенко, а отже, це не вона на фотографії:



З такими зображеннями часто можливо дослідити більше їх елементів.

Використовуючи такий інструмент, як [Forensically](#), можна переглянути різні рівні цього зображення, зробивши розгортку за рівнями. Ясно, що це зображення взяли з сайтів, які ми знайшли в процесі зворотного пошуку зображення, після чого додали новий рівень—обвели колом фото і написали ім'я Прокопенко, щоб дискредитувати її (різниця в кольорі дає вам підказку):



Ще хороший приклад схожого інструменту—[FotoForensics](#), де ви можете підвантажити фотографії так само, як ви це робили на Forensically. Саме так FotoForensics подає змінену фотографію Кім Джон Уна. Знов-таки, відмінність у кольорі показує вам, що зображенням маніпулювали, і де саме на ньому вносили зміни:



І, нарешті, хоча платформи соціальних мереж вичищають з фотографій мета-дані — тобто, місце, час, інформацію про прилад та іншу інформацію, котра може видати походження зображення — якщо ви зможете знайти оригінал фото десь в мережі—наприклад, в бібліотеці зображень, ви зможете використати цілий набір інструментів для аналізу мета-даних конкретного зображення.

Ось хороший приклад результату, що видає FotoForensics для зображення, в якого не було вичищено мета-дані — зауважте наявний рівень деталізації:

EXIF

Make	Apple
Camera Model Name	iPhone X
Orientation	Horizontal (normal)
X Resolution	72
Y Resolution	72
Resolution Unit	inches
Software	12.3
Modify Date	2019:12:29 20:14:14
Y Cb Cr Positioning	Centered
Exposure Time	1/50
F Number	1.8
Exposure Program	Program AE
ISO	250
Exif Version	0231
Date/Time Original	2019:12:29 20:14:14
Create Date	2019:12:29 20:14:14

Approximate GPS Location

This information is interpreted from the GPS metadata. **Locations are approximate.** Although the coordinates appear precise, mobile devices typically have low accuracy.

Approximate Coordinates	28.542828, 77.302392
Approximate Location	2.41 miles (3.88 km) SW of Sector, IN
Approximate Range	+/- 165 meters (541.3 feet)

28°32'34.2"N 77°18'08.6"E

GD Bina Mang, Block G, Jasola Vihar, New Delhi, Delhi 110025

View larger map

За відсутності надійних мета-даних навички та інструменти геолокації та хронолокації можуть вам допомогти визначити місце фотографування.

ВІД GOOGLELENS ДО ГЕОЛОКАЦІЇ

Зараз GoogleLens швидко покращує свої інструменти для визначення орієнтирів. Якщо на вашій фотографії є якийсь визначний орієнтир, виріжте ту частину фотографії, на якій цей орієнтир чітко видно і немає інших елементів, які можуть заплутати програму, підвантажте вирізане фото на GoogleLens і подивіться, що буде в результатах.

Для важких випадків, де на фото немає орієнтирів або якихось легко впізнаваних деталей, ви можете скористатися даними з супутників.

Хоча на перший погляд це завдання може здаватися непосильно складним, не забувайте про два основних принципи геолокації:

1. Це не гра у здогадки, це гра виключення можливостей.
2. Надійне знаходження елементів із зображення на супутникових знімках може допомогти підтвердити місце зйомки, якщо зворотний пошук зображення не видав бажаних та/або корисних результатів.

Як SentinelHub, так і Google Maps можуть надати вам безкоштовні, легкі у використанні інструменти для проведення геолокації конкретного віддаленого місця, із можливістю розібратися, коли було зроблено знімок, за змінами у місцевому середовищі/інфраструктурі. Ось приклад того, як географічні елементи на фото солдата можуть бути співвіднесені з супутниковими знімками, таким чином допомагаючи провести хронолокацію фото одночасно з геолокацією:

When was The Image Taken?



Вище: немає виступу / виступ / відсутня споруда

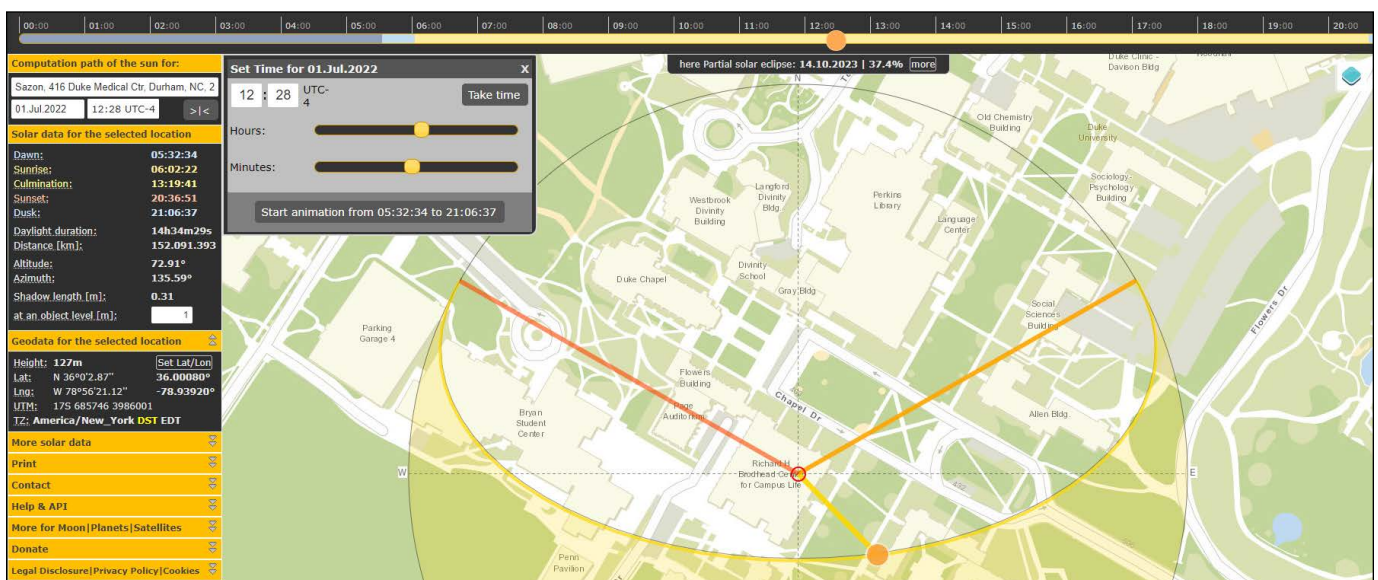
ЗНАЙОМСТВО ІЗ ВИКОРИСТАННЯМ ТІНЕЙ ПРИ АНАЛІЗІ ФОТОГРАФІЙ

Якщо ви не можете ідентифікувати, де який напрямок на фотографії, вам може допомогти такий інструмент як [SunCalc.org](https://www.suncalc.org). SunCalc розраховує довжину тіні на основі конкретного місця та пори року, і показує корисні анімації, що допомагають дослідникам відслідкувати рух тіней протягом дня.

Цей інструмент може бути винятково цінним, якщо ви провели геолокацію зображення, але не впевнені, коли його зробили. Також він може допомогти проаналізувати тіні на фото, де відоме приблизне місцезнаходження в момент зйомки, і ви намагаєтеся з'ясувати, в який бік обернені певні елементи фотографії, що може допомогти виявити точне місцезнаходження, де фото було зроблене.

Почніть з використання адреси добре вам відомої пам'ятки. На прикладі нижче ми використовуємо каплицю Університету Дюка у Даремі, Північна Кароліна.

Зауважте, що ви маєте натиснути на кнопку, обведену фіолетовим, щоб програти анімацію того, як тінь каплиці рухатиметься протягом дня. Ви можете вводити різні дати на SunCalc, щоб побачити, як змінюється рух тіні у різні пори року. Коли ви згодом перейдете до аналізу менш знайомих місць за допомогою SunCalc, ви навчитеся розуміти рух тіней і використовувати це для того, щоб покращити свої навички хронолокації та розуміння простору:





ЯК ПРАЦЮЄ **ТЕЛЕГРАМ** + ТА ЯКІ В НЬОГО ВРАЗЛИВОСТІ

Як продемонстрував поточний конфлікт в Україні, відсутність регулювання у Телеграм створила чудове середовище для розповсюдження дівфейків та дезінформації. Можливість аналізувати Телеграм-канали—важлива частина сьогодишнього набору для розслідувань.

До останнього часу Телеграм не прокручував рекламу в себе на платформі. Це створило так звану модель тіньової економіки, де канали приймали публікації за фінансову винагороду та/або в обмін на подібну послугу публікації контенту.

У Росії журналісти [задокументували](#) зв'язки між декількома популярними Телеграм-каналами та Кремлем і виявили, що існує можливість публікувати фактично будь-яке повідомлення на певних каналах Телеграм—за гроші. В Україні Служба Безпеки України виявила мережу каналів, [спеціалізованих](#) на підривній діяльності і пов'язаних з Головним Розвідувальним Управлінням Росії. Українські [ЗМІ](#) та [НУО](#) провели розслідування ще розлогіших мереж, які розповсюджували підривну пропаганду та дезінформацію як перед ескалацією, так і під час неї. [Служба Безпеки України](#) та [Рада Національної Безпеки та Оборони](#) викрили підривні пропагандистські канали і опублікували їх список.

Саме така риса, як відсутність модерації, дозволяє Телеграм бути таким величезним центром розповсюдження для дівфейків та дезінформації.

ТЕМНІ МЕРЕЖІ ТЕЛЕГРАМ

Багато російських каналів Телеграм, про які вам слід знати, вдають, ніби мають “інсайдерську інформацію” про те, що відбувається у Кремлі /у Москві/на окупованих територіях України, і так далі. Важливо розуміти, що тролі та платні пропагандисти часто вдають, ніби вони інсайдери—з метою посіяти безлад та плутанину.

Ось деякі популярні російські канали Телеграм, пов’язані з Кремлем:



- Дозволяють анонімне адміністрування
- Канали дають «унікальну інсайдерську» інформацію.
- Зазвичай підсилюють те, що транслюють схожі за змістом канали або проплачені повідомлення на інших каналах

Дуже сильно викривають такі мережі випадки, коли ви бачите, як ті самі повідомлення розповсюджуються на різних каналах. Завжди остерігайтеся подібних скоординованих зусиль.

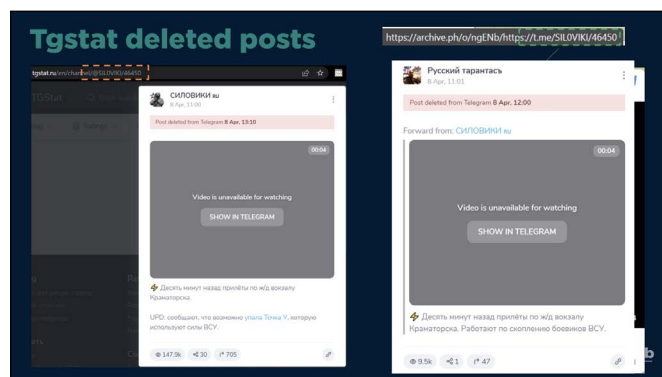
ДВА НАЙКРАЩИХ ІНСТРУМЕНТИ ТЕЛЕГРАМ

Коли ви досліджуєте канали, зауважте, що пошук вручну видасть вам лише ті канали, на які ви вже підписані у Телеграм. Для розширеного пошуку на зараз можна використовувати такі інструменти, як [TGStat](#) та [Intelligence X](#).

Зауважте, що хоча TGStat є найпотужнішим інструментом для аналізу Telegram на момент написання цього посібника, він створений у Росії, і, як і у випадку із самим Telegram, ми рекомендуємо: якщо ви вирішите досліджувати Telegram, вам варто не використовувати ваш власний телефон і обліковий запис Telegram, а використати так званий «одноразовий телефон» та маріонетковий (фейковий) обліковий запис.

Коли ви знайомитиметесь із TGStat, зауважте, що в нього є можливість шукати витерті повідомлення на Телеграм (докладніше про це далі). Це стає особливо цінним, коли пропагандисти заявляють про нанесення удару по військових, а пізніше виявляється, що вони вбили цивільних і вирішили замести сліди, витерши всі докази.

Повідомлення нижче посилається на удар у Краматорську, в якому було вбито численних цивільних, що й пояснює те, що це повідомлення було витерто з проросійського каналу:



Маємо зауважити: хоча TGStat зараз є найпотужнішим інструментом для аналізу Телеграм, є велике «але» — його робили росіяни. Тим не менше, ми можемо використовувати російські інструменти проти російської пропаганди. Цей інструмент безкоштовний на певний обмежений період часу, з обмеженими можливостями роботи.

Хоча він і корисний, ми б дуже порадили використовувати анонімний телефон та віртуальний аккаунт у ТГ для користування ним.

Ми також можемо використовувати Телеграм та TGStat, не створюючи аккаунт на Телеграм. В більшості випадків TGStat корисний, тому що він архівує публікації—а це дозволяє вам переглянути їх навіть після того, як оригінал було відредаговано або знищено. Це корисно для того, щоб виявити [маніпуляцію інформацією](#), перевірити [мета-дані](#) відеоматеріалу, який був замінений, і подивитися на оригінал публікації.

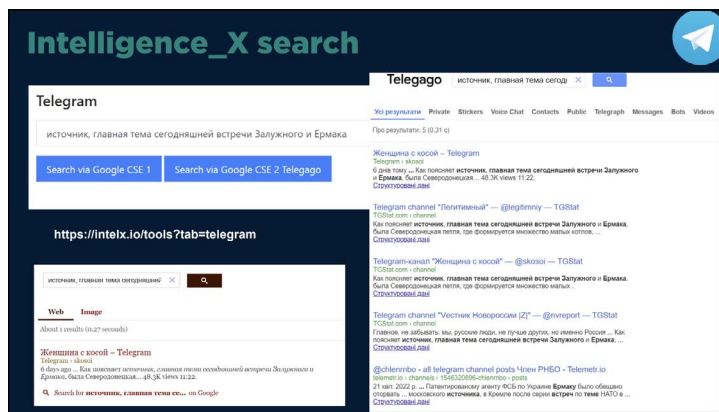
Щоб подивитися на публікацію через TGStat, нам треба скопіювати посилання з публікації у Телеграм, яка нас цікавить, через мережеву або комп'ютерну версію Телеграм. Скажімо, ми зацікавлені у публікації від RIA за посиланням https://t.me/rian_ru/168574. Щоб побачити її у TGStat, нам потрібно вставити частину URL до TGStat, ось таким чином https://tgstat.ru/en/channel/@rian_ru/168574. Зауважте, що фрагмент “rian_ru/168574” було скопійовано з початкового посилання і додано до шаблону “<https://tgstat.ru/en/channel/@>”.

Публікації на Телеграм використовують послідовну нумерацію, а це означає, що число у кінці URL з каналу означає номер публікації. Якщо ви бачите, що декілька сторінок мають дві послідовних публікації, але їх нумерація не послідовна, наприклад, одне число між ними пропущене— є чималий шанс, що публікація між цими повідомленнями була стерта, так що ви можете перевірити її на TGStat, і якщо вона була заархівована до того, як її витерли — ви побачите опубліковану інформацію.

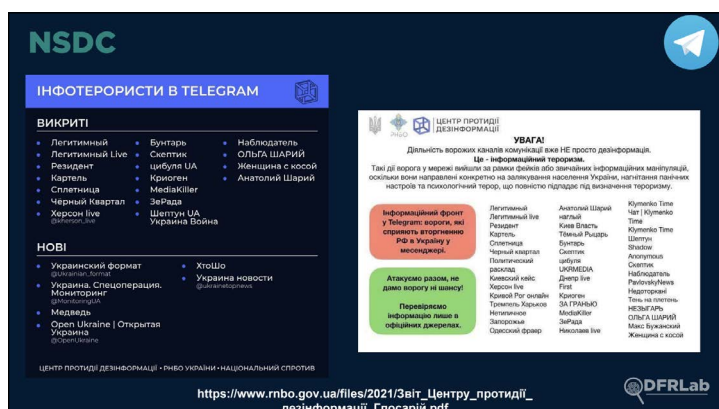
Якщо ви побачите повідомлення “This channel cannot be displayed” («Цей канал не може бути відображений»), просто скопіюйте посилання з екосистеми Телеграм (з мережевого або комп’ютерного застосунку) і вставте його в будь-який браузер. Це дозволить вам переглядати публікацію незалежно від вашого місцезнаходження.

Якщо ви хочете побачити більше, ніж одну конкретну публікацію, а не одну, наприклад, сторінку «про канал», і подивитися кілька публікацій цього каналу у форматі єдиної стрічки, вам потрібно буде відредагувати посилання URL. Ось URL, яке ми використовували вище: https://t.me/rian_ru/168574—до нього слід додати «s/» перед назвою каналу, щоб відкрити можливість прокручувати його публікації. Отже, посилання після редагування виглядатиме так: https://t.me/s/rian_ru/168574.

В той самий час, Intelligence_X—зручний інструмент для аналізу, які канали використовують такі самі фрази. У пошуку нижче наведено приклад, котрий показує, які проросійські канали цитують одне й те саме джерело:



Знов-так, українські джерела боротьби з дезінформацією, так як РНБО (Рада Національної Безпеки та Оборони України), публікують списки каналів Телеграм, які пов’язують з російською кампанією пропаганди, що постійно оновлюються – наприклад, наведені тут:



Ці списки можуть бути хорошим відправним пунктом для будь-кого, хто не має досвіду роботи з Телеграм і хоче дослідити створені там широкі мережі дезінформації.

ВИСНОВОК

Інформаційний простір під час війни змінюється дуже швидко, і орієнтуватися в ньому здебільшого нелегко. Ми сподіваємося, що, використовуючи інструменти, описані вище, ви зможете заощадити свій час та зусилля при спростуванні дезінформації.

При цьому важливо завжди пам'ятати про цілі будь-якої кампанії з дезінформації: вона створюється для того, щоб заплутати, деморалізувати та виснажити свою аудиторію.

Тому для будь-якого журналіста та дослідника важливо робити перерви, відходити від подібного контенту і дозволяти собі відпочити. Дбайте про власну безпеку, здоров'я, залишайтеся активними — і ви зможете ефективніше протидіяти дезінформації та пропаганді Росії.

ДОДАТКОВІ РЕСУРСИ

Нижче ми подаємо посилання на інші ресурси, що можуть бути цікавими:

Поради КЗЖ для журналістів, що висвітлюють війну та заворушення, пов'язані з нею

Ведення воєнних репортажів: [Англійська](#) | [Українська](#) | [Російська](#)

Арешт та затримання: [Англійська](#) | [Українська](#) | [Російська](#)

Громадські заворушення: [Англійська](#) | [Українська](#) | [Російська](#)

Закриття Інтернету: [Англійська](#) | [Українська](#) | [Російська](#)

Шаблон оцінки ризиків: [Англійська](#) | [Українська](#) | [Російська](#)



ІНСТИТУТ БЕЗПЕКИ ТА ТЕХНОЛОГІЙ
www.securityandtechnology.org

counterdisinfo@securityandtechnology.org

Copyright 2022, The Institute for Security and Technology