

Weryfikowanie informacji w sieci

Przewodnik po podstawach



Weryfikowanie informacji w sieci
Wrzesień 20, 2022
by [Shaydanay Urbani](#)

Table of contents

- Wstęp.
- Absolutne podstawy.
- Pochodzenie.
- Źródła.
- Daty.
- Lokalizacje.
- Motywacje.
- Przewodnik po podstawach: Informacyjny bałagan i zbieranie informacji

Weryfikacja treści online może wyglądać przerażająco, ale nie jest trudna.

Dobra weryfikacja sprowadza się głównie do wykonywania repetytywnych czynności, i umiejętnego korzystania z cyfrowych narzędzi śledczych. Dobrze też, jeśli wykonuje się ją z dozą kreatywności.

Obecnie dostępnych jest wiele narzędzi weryfikacyjnych, co sprawia że zapamiętanie wszystkich zasobów jakie są dostępne nie jest łatwe.

Między innymi dlatego postanowiliśmy stworzyć ten krótki przewodnik, aby stał się Twoim oparciem w niekiedy złożonej sztuce weryfikacji.

Zawiera podstawowe założenia, listy kontrolne oraz nasze ulubione wskazówki i techniki. Co najważniejsze, przedstawiamy w nim pięć filarów weryfikacji, które mamy nadzieję, posłużą Ci jako punkt odniesienia.

Informacje rozchodzą się szybko, a dezinformacja jest tak łatwa do generowania i rozpowszechniania, że każdy dziennikarz — nie tylko reporter zajmujący się nowymi technologiami, czy redaktor mediów społecznościowych — powinien znać i umieć dokonywać weryfikacji.

Ten problem jest szczególnie widoczny w newsroomach, gdzie dziennikarze często pracują pod dużą presją, aby zarówno szybko donieść o aktualnych wydarzeniach, jak i rzetelnie ustalić fakty.

Dlatego współczesne newsroomy muszą wiedzieć jak chronić się przed oszustwami i nieumyślnym wprowadzaniem w błąd szerszej publiczności. Wielu agentów od dezinformacji postrzega relacje z uznanych serwisów informacyjnych jako swój cel i będzie wykorzystywać przestrzenie internetowe do rozsiewania plotek i zmanipulowanych treści, mając nadzieję na dotarcie do większej liczby odbiorców.

Więcej informacji na ten temat można znaleźć w naszym pierwszym szkicu [Niezbędnika do Rzetelnej Weryfikacji w Czasach Manipulacji i Chaosu Informacyjnego](#).



Nie daj się nabrać. Naucz się weryfikować.

Jak korzystać z tego przewodnika?

Zanim rozpoczniesz jakąkolwiek przygodę z weryfikacją, zacznij od przeczytania naszego pierwszego rozdziału, „Absolutnych podstaw”. Znajdziesz tam koncepcje, które warto znać i które mogą zaoszczędzić Twój czas — a niekiedy nawet ocalić dziennikarski honor.

Reszta broszury podzielona jest na pięć podstawowych czynności sprawdzających, które należy wykonać w odniesieniu do treści, którą chcesz zweryfikować, niezależnie od tego, czy jest to materiał naocznych świadków, zmanipulowane nagranie czy śmieszny mem.

Spośród tych rozdziałów najważniejszy rozdział to „Pochodzenie”, więc zwróć szczególną uwagę właśnie na niego.

Resztę materiału możesz przejrzeć w wolnym czasie i bezpośrednio przejść do listy wskazówek, która jest dla Ciebie najistotniejsza. Weryfikacja to płynny proces znajdowania nowych wskazówek i dowodów, a postępy jakie poczynisz w jednej dziedzinie przyjdą z pomocą w innej.

Absolutna podstawa

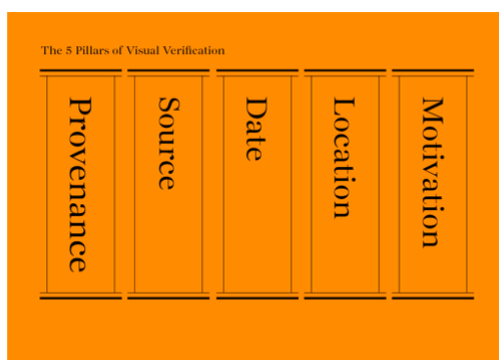
Zanim zweryfikujesz jakąkolwiek treść online, zadaj sobie najbardziej podstawowe pytanie: Czy treści, które oglądam, są powiązane z wydarzeniem, które faktycznie miało miejsce?

W niektórych okolicznościach, takich jak wydarzenia z ostatniej chwili, to pytanie może być właśnie tym, co próbujesz ustalić za pomocą weryfikacji. Ale w niektórych przypadkach tak nie jest.

Wyobraź sobie, że znajdujesz film, który twierdzi, że przedstawia długie kolejki i niezadowolonych pasażerów na międzynarodowym lotnisku Chicago O’Hare. Zanim wpadniesz w przysłowiową dziurę bez dna, aby zweryfikować osobę, która nagrała wideo, datę i godzinę lub lokalizację, twoje pierwsze pytanie powinno brzmieć: Czy rzeczywiście są jakiegokolwiek doniesienia o problemach na lotnisku?

Innym przykładem jest szeroko krytykowany nagłówek, który pojawił się przed wyborami w USA w 2016 r.: „Papież popiera Donalda Trumpa”. Możesz przeprowadzić dowolną weryfikację strony internetowej, kto ją utworzył, kiedy artykuł został opublikowany i jak daleko się rozprzestrzenił itp., ale podstawowe twierdzenie artykułu powinno być pierwszą rzeczą, którą sprawdzasz.

5 filarów weryfikacji



5 filarów wizualnej weryfikacji:

1. Pochodzenie
2. Źródło
3. Data
4. Lokalizacja
5. Motywacja

Zaletą weryfikacji jest to, że łatwo ją rozłożyć na części pierwsze. Dzieje się tak, ponieważ bez względu na to, czy oglądasz wideo naocznego świadka, przerobione zdjęcie, konto słupa czy mem, podstawowe czynności kontrolne, które musisz wykonać zawsze będą takie same:

- Pochodzenie: Czy patrzysz na oryginalne konto, artykuł lub fragment treści?
- Źródło: kto utworzył konto lub artykuł albo uchwycił oryginalną treść?
- Data: kiedy powstał dany materiał?
- Lokalizacja: gdzie założono konto, utworzono witrynę internetową lub umieszczono fragment treści?
- Motywacja: Dlaczego założono konto, stworzono stronę internetową lub umieszczono fragment treści?

Im więcej wiesz o każdym filarze, tym lepsza będzie twoja weryfikacja.

Nieuchwytna pewność

Weryfikacja jednak nie jest niezawodna. To bardziej jak szukanie wskazówek i zbieranie przekonujących dowodów. Wyobraź sobie tradycyjne biuro detektywistyczne. Do tablicy przypięte są fragmenty informacji: lokalizacja, nazwa, wymowny cytat. Linie między wskazówkami przedstawiają sieć połączeń. Na tym polega weryfikacja informacji pobranych z sieci: te same metody, których reporterzy i śledczy zawsze używali, aby dotrzeć do prawdy, tym razem zastosowano w Internecie.

Weryfikując materiały pamiętaj, żeby zebrać jak najwięcej dowodów, ale miej na uwadze również to, że nawet najlepsze poszukiwania mogą nadal spełznąć na niczym.

Fakt, że nie możemy być czegoś pewni wskazuje jednak na coś równie istotnego w zawodzie dziennikarza, że czasami bycie szczerym z tym, co wiemy i co udało się nam ustalić, a czego nie wiemy, zwłaszcza jeśli te informacje mają być poddane szerszej publice, jest ważniejsze niż bycie pierwszym w podaniu przełomowej informacji.

Poniższe strony to dwie tabele, które zbudowaliśmy w celu ułatwienia weryfikacji mediów obrazkowych — jedna dla zdjęć, a druga dla nagrań wideo, które pomogą Ci ocenić, jak rzetelna jest Twoja weryfikacja i gdzie mogą znajdować się ewentualne luki w Twojej pracy.

Przewodnik po weryfikacji wizualnej: zdjęcia

FAKE

TRUE

Czy patrzysz na oryginalną wersję zdjęcia?	Wtórne wyszukiwanie obrazów pokazuje identyczne zdjęcia, które pojawiły się w wyszukiwarce zanim wydarzenie, które sprawdzasz miało miejsce.	Wtórne wyszukiwanie obrazów pokazuje podobne wyniki z pewnymi identycznymi cechami, co może sugerować, że jest to część kolażu lub przeróbki.	Wyszukiwanie danych w każdej sieci społecznościowej ujawnia, że jest to pierwsza z wielu wersji zdjęcia udostępniona online, ale nie otrzymaliśmy jeszcze potwierdzenia od autora	Nie możemy znaleźć żadnych podobnych zdjęć online, a podstawowe testy cieni i odbić sugerują, że nie zostało ono zmanipulowane	Zdjęcie zostało przesłane bezpośrednio do nas i potwierdziliśmy jego wiarygodność ze źródłem
Czy wiesz, kto wykonał zdjęcie?	Zdjęcie zostało przesłane z anonimowego numeru lub konta w aplikacji	Zdjęcie zostało dodane przez osobę z anonimowego konta, której nie możemy namierzyć na innych kontaktach społecznościowych	Byliśmy w stanie zweryfikować autora zdjęcia, przy użyciu wyszukiwarki podając pełne imię i nazwisko tej osoby lub używając wtórnego wyszukiwania obrazów zdjęcia profilowego, albo sprawdzając rejestr domeny	Wykorzystaliśmy media społecznościowe do skontaktowania się z twórcą zdjęcia	Autor odpowiedział na nasze pytania, jego wypowiedź skonfrontowaliśmy z danymi EXIF, pogodą i indywidualnymi informacjami dot. autora.
Czy wiesz, gdzie zostało zrobione zdjęcie?	Lokalizacja zdjęcia jest niemożliwa do ustalenia. Zdjęcie nie posiada żadnych charakterystycznych elementów wizualnych, które można wykorzystać	Zweryfikowaliśmy lokalizację używając innych zdjęć z danego miejsca, ale nie mogliśmy ich porównać ze zdjęciami z satelity i widoku ulicy	Wykorzystaliśmy inne wskazówki wizualne, takie jak oznakowanie, architekturę i ubiór, aby potwierdzić region geograficzny	Porównaliśmy krajobraz i punkty orientacyjne za pomocą narzędzi do mapowania i potwierdziliśmy współrzędne szerokości/długości i geograficznej	Źródło było w stanie potwierdzić inne punkty orientacyjne w polu widzenia, które pasowały do tych pokazanych na mapach internetowych
Czy wiesz, kiedy zrobiono zdjęcie?	Zdjęcie zostało wysłane do nas anonimowo i jest pozbawione danych EXIF	Sprawdziliśmy datę na platformie społecznościowej, aby zobaczyć, kiedy zdjęcie zostało po raz pierwszy udostępnione online, ale nie mamy danych EXIF potwierdzających, kiedy zostało ono zrobione	Zdjęcie było dodane na social media, krótko po jego wykonaniu w momencie zdarzenia. Zawiera dowody, które pasują do relacji innych naocznych świadków	Jesteśmy w stanie potwierdzić, że warunki pogodowe oraz cienie, które są na zdjęciu pasują do lokalizacji i czasu, w którym rzekomo zostało zrobione zdjęcie	Zdjęcie zawiera dane EXIF, które potwierdzają nasze poprzednie wnioski i przypuszczenia, co do momentu, w którym zostało zrobione



Czy wiesz, dlaczego zrobiono zdjęcie?	Nie wiemy kto wykonał to zdjęcie więc trudno nam się jest wypowiedzieć na temat motywacji tej osoby	Konto społecznościowe zostało utworzone bardzo niedawno, a jego aktywność na portalach sugeruje, że przesyłający rzadko publikuje online, więc niewiele jest dowodów potwierdzających motywacje tego użytkownika	Szersze wyszukiwanie w Internecie prawdziwego nazwiska przesyłającego ujawniają, że jest on powiązany z pewnymi aktywistami lub organizacjami, ale nie ma dodatkowych informacji o jego motywach	Aktywności w mediach społecznościowych przesyłającego potwierdzają powody, dla których mógł zrobić zdjęcie np. jest to wczasowicz, dziennikarz, pracuje lokalnie	Fotograf był w stanie potwierdzić okoliczności zrobienia zdjęcia
--	---	--	--	--	--

Przewodnik po weryfikacji wizualnej: filmy i nagrania video

Czy patrzysz na oryginalną wersję nagrania?	Szukając nagrania przy użyciu elementów jego opisu, widzimy, że w mediach społecznościowych ten materiał pojawił się już wcześniej	Wsteczne wyszukiwanie elementów nagrania w wyszukiwarkach obrazów, pokazuje że istnieją podobne jego wersje, ale nie wiemy, która wersja jest oryginalna	Wyszukiwanie w Internecie skróconego kodu URL video sugeruje, że jest to pierwsza wersja udostępniona online, ale nie mogliśmy porozmawiać z autorem	Nie udało się nam znaleźć innej wersji tego nagrania w sieci	Nagranie było przesłane do nas osobiście i byliśmy w stanie porozmawiać ze źródłem.
Czy wiesz, kto wykonał nagranie?	Nagranie zostało przesłane z anonimowego numeru lub konta w aplikacji	Chociaż nagranie pojawiło się w social media, to jego autor chce pozostać anonimowy i nie możemy dotrzeć do jego innych kont społecznościowych	Byliśmy w stanie zweryfikować autora nagrania, przy użyciu wyszukiwarki podając pełne imię i nazwisko tej osoby lub używając wtórnego wyszukiwania obrazów zdjęcia profilowego, albo sprawdzając rejestr domeny	Wykorzystaliśmy media społecznościowe do skontaktowania się z twórcą zdjęcia	Autor odpowiedział na nasze pytania, jego wypowiedź skonfrontowałem z raportem, pogodowym, z jego aktywnością w sieci i informacjami dotyczącymi urzędu
Czy wiesz, gdzie zostało zrobione nagranie?	Nie jesteśmy w stanie określić, gdzie zostało zrobione nagranie. Brakuje poszczególnych elementów, które mogą opisać to miejsce	Przetłumaczone fragmenty tekstu stanowią odpowiedź, gdzie zostało wykonane zdjęcie, ale nie jesteśmy w stanie zweryfikować tej lokacji	Wykorzystaliśmy inne wskazówki wizualne, takie jak oznakowanie, architekturę i ubiór, aby potwierdzić region geograficzny	Porównaliśmy krajobraz i punkty orientacyjne za pomocą narzędzi do mapowania i potwierdziliśmy współrzędne szerokości/długości geograficznej	Autor odpowiedział na nasze pytania, a jego opis miejsca pasował do danych jakie zebraliśmy na podstawie analizy wizualnej



					miejsca
Czy wiesz, kiedy zrobiono nagranie?	Nagranie zostało przesłane do nas anonimowo i nie ma żadnych metadanych	Wiemy kiedy nagranie pojawiło się online na platformach, ale nie wiemy kiedy zostało wykonane	Nagranie było dodane na social media, krótko po jego wykonaniu w momencie zdarzenia. Zawiera dowody, które pasują do relacji innych naocznych świadków.	Porozmawialiśmy z autorem i byliśmy w stanie potwierdzić, że znajdował się w miejscu, w którym miało miejsce wydarzenie	Potwierdziliśmy, że warunki pogodowe i wszelkie cienie widoczne na obrazie są skorelowane z godziną, datą i lokalizacją podaną przez źródło
Czy wiesz, dlaczego zrobiono nagranie?	Nie wiemy kto jest autorem nagrania, więc jego motywacje są nam nieznane	Autor dołączył do mediów społecznościowych dopiero niedawno i nie jest zbyt aktywny online, więc mało wiemy o jego celach	Szersze wyszukiwanie w Internecie prawdziwego nazwiska przesyłającego ujawniają, że jest on powiązany z pewnymi aktywistami lub organizacjami, ale nie ma dodatkowych informacji o jego motywach	Aktywności w mediach społecznościowych przesyłającego potwierdzają powody, dla których mógł nagrać materiał np. jest to wczasowicz, dziennikarz, pracuje lokalnie	Porozmawialiśmy z osobą, która wyjaśniła nam okoliczności nagrania materiału

Czy warto to zweryfikować?

Uważaj na dziury bez dna!

Często weryfikacja zajmuje kilka minut. Innym razem może zaprowadzić Cię na długą i bezowocną ścieżkę zakrawającą o obsesję.

Pamiętaj, żeby wiedzieć, kiedy się poddać i zrezygnować z wykorzystania pewnych materiałów, czy podania niektórych informacji swoim odbiorcą.

Należy również pamiętać, że pielęgnowanie jednej hipotezy o tym, skąd pochodzi treść lub czy jest ona prawdziwa, może nie tylko narazić na szwank integralność Twojej weryfikacji, albo zwyczajnie zmarnować Twój cenny czas.

Jesteśmy ludźmi i to naturalne, że reagujemy instynktownie na to, czy prezentowana treść jest prawdziwa czy fałszywa. Ale przez cały czas musimy pamiętać o tym, że warto być sceptycznym, zwłaszcza jeśli chodzi o materiały w sieci.

W takich sytuacjach sprawdza się powiedzenie starego redaktora: nawet jeśli twoja mama mówi, że cię kocha, sprawdź to.

Internet to rozległe i zagmatwane miejsce. Jeśli zbyt intensywnie szukasz konkretnego dowodu, możesz po drodze przeoczyć sprzeczne dowody.

Jak zrozumieć rozprzestrzeniania się fałszywych informacji?

Zgłaszanie dezinformacji to trudna sztuka. Badania pokazują, że nawet sprostowanie fałszywych informacji może w pewien sposób utrwalić fałszywe plotki. Oznacza to, że nagłaśnianie dezinformacji, nawet w dobrych intencjach, może zwiększyć ekspozycję na treści, które w przeciwnym razie mogłyby przepaść w sieci.

Jeśli weryfikujesz część wprowadzającą w błąd treści, ponieważ chcesz ją zgłosić lub napisać krytykę, zastanów się najpierw, jaki zasięg ma ta treść w Internecie?

Ile osób mogło już zobaczyć tą fałszywą tezę? Trudno jest oszacować to dokładnie posługując się tylko dostępnymi wskaźnikami, które zwykle są udostępnieniami, polubieniami, retweetami, wyświetleniami lub komentarzami. Ale ważne jest, aby mimo wszystko spróbować to zrobić. Nawet małe lub niszowe społeczności mogą wydawać się większe w Internecie.

Jeśli trafisz na nieprawdziwą treść, która spotkała się z bardzo niskim zaangażowaniem, zastanów się, czy warto jest ją w ogóle weryfikować albo o niej pisać.

Aby uzyskać więcej informacji na ten temat, przeczytaj pierwsze wydanie [Niezbędnika do Rzetelnej Weryfikacji w Czasach Manipulacji i Chaosu Informacyjnego](#).

Jak oszczędzić czas i się nie frustrować?

Prowadź dokumentację

Zrób zdjęcie ekranu (ang. screenshot) wszystkiemu, co Cię zadziwi! Treść może zostać szybko usunięta lub zablokowana przez platformę na której się pojawiła. Czasami to naprawdę niesamowite, jak szybko się to dzieje, i jak szybko można stracić kluczowe ślady. Ten krok jest również istotny z punktu widzenia przejrzystości Twojej weryfikacji.

- Możesz wykonać zrzut ekranu w systemie Mac OS, naciskając polecenie + shift + 5, a następnie przeciągając kursor nad obszar, który chcesz przechwycić, lub używając narzędzia do wycinania w systemie Windows.
- Pomocne może być użycie narzędzia do przechwytywania ekranu, takiego jak Evernote, które pozwala szybko zbierać dowody.
- [Wayback Machine](#) to rozszerzenie przeglądarki, które umożliwia zapisywanie zarchiwizowanych wersji stron internetowych.
- [Hunch.ly](#) to bardzo przydatne narzędzie, które pozwala udokumentować całe śledztwo poprzez automatyczne pobieranie zrzutów ekranu z przeglądarki internetowej i ich katalogowanie. Jest to płatne narzędzie, więc nie jest dostępne dla wszystkich, ale jeśli potrzebujesz niezawodnego systemu do dokumentowania dochodzeń, Hunchly.ly może być tego wart.

Nie zapomnij sprawdzić Google

Istnieje wiele imponujących narzędzi do weryfikacji. Wiele z nich przedstawiamy w tym przewodniku. Pamiętaj jednak, że czasami wystarczy proste wyszukiwanie w Google.

Nie zapomnij o używaniu telefonu

W wielu sytuacjach najlepszym rozwiązaniem jest po prostu znalezienie numeru telefonu lub adresu e-mail źródła, dzięki czemu można się z nim bezpośrednio skontaktować i zapytać o udostępnienie treści. Nawet wysłanie prostej wiadomości może rozpocząć prywatną rozmowę, w której możesz dowiedzieć się o wiele więcej niż rezygnując z kontaktu.

Skonfiguruj zestaw narzędzi

Jeśli zamierzasz przeprowadzać wiele weryfikacji lub innych rodzajów badań z wykorzystaniem sieci, warto stworzyć system zakładek, który będzie zawierał wszystkie Twoje ulubione witryny. Jak wspomniano wcześniej, jednym z największych wyzwań może być samo zapamiętanie narzędzi, którymi dysponujesz.

Foldery zakładek w przeglądarce internetowej są dobre, ale naszym ulubionym sposobem do zapisywania narzędzi jest strona [Start.me](#).

Przejrzyście wyświetli wszystkie zakładki i umożliwia szybkie skonfigurowanie i ciągle dodawanie nowych zasobów. Możesz użyć jej również jako swojej strony głównej.

Monitoruj jednocześnie powiązane treści

Podczas weryfikowania treści pomocne może być stworzenie pulpitu nawigacyjnego do monitorowania i systemu zbieżnych alertów, aby można było szybko wychwycić podobną treść, jeśli się pojawi. Możesz użyć słów kluczowych i języka z badanej treści, aby na przykład skonfigurować kolumnę wyszukiwania w [TweetDeck](#) lub skonfigurować listę kont, które często wchodzi w interakcję z Twoim źródłem. Aby uzyskać więcej informacji o tym, jak skutecznie monitorować media społecznościowe, zobacz nasz [Niezbędnik do Rzetelnej Weryfikacji w Czasach Manipulacji i Chaosu Informacyjnego](#).

Bycie na bieżąco

Weryfikacja ciągle się zmienia. Platformy technologiczne modyfikują ustawienia prywatności, usuwane są narzędzia badawcze i budowane są nowe. Jeśli chcesz być na bieżąco, regularnie aktualizuj swój zestaw narzędzi lub zapoznaj się z najnowszymi technikami społeczności zajmującej się weryfikacją i Open Source Intelligence (OSINT).

Istnieje wiele publicznych list OSINT/weryfikacyjnych na Twitterze, które możesz śledzić, aby to zrobić. Więcej informacji na temat znajdowania i tworzenia list można znaleźć w pierwszym przewodniku Essential Guide on Newsgathering and Monitoring.

Zatroszcz się o swoje bezpieczeństwo

Istnieje wiele środków ostrożności, które należy podjąć, w trakcie przeprowadzania śledztw online. Zwłaszcza jeśli Twoja praca będzie wymagała infiltracji bardzo zamkniętych i anonimowych przestrzeni, takich jak Discord.

Oto kilka podstaw do rozważenia:

Upewnij się, że masz wysoki poziom osobistego bezpieczeństwa cyfrowego. Jeśli to możliwe, używaj menedżera haseł. Sprawdź swój własny "cyfrowy szlak" i ustawienia prywatności na wszystkich swoich kontaktach społecznościowych. Ile ktoś mógłby dowiedzieć się o Tobie, Twojej rodzinie i przyjaciółach za pośrednictwem Twoich kont? Rozważ użycie VPN i anonimowej przeglądarki internetowej, takiej jak [Tor](#). Jeśli uczestniczysz lub wchodzisz w interakcję z ludźmi w zamkniętych i anonimowych grupach, uważaj na ilość ujawnianych danych osobowych.

Etyka i standardy nadal obowiązują

Pisanie i omawianie mediów przy pomocy treści wydobytych z sieci, wcale nie oznacza, że podstawowe zasady etyki dziennikarskiej i standardy można zarzucić. Wręcz odwrotnie, pojawia się nowe kwestie etyczne. Oto kilka punktów i pytań, nad którymi warto się zastanowić:

1. Tak jak e-mail nie jest tak efektywny jak rozmowa kwalifikacyjna, którą przeprowadziłeś osobiście, tak samo będzie z cytatem wyciągniętym z internetu. Rozmawiaj bezpośrednio z ludźmi, jeśli masz do nich dostęp.
2. Niektóre narzędzia weryfikacyjne wykorzystują luki w tym jaki platformy społecznościowe ukrywają ustawienia prywatności i prowadzą ludzi do udostępniania rzeczy, o których nie zdawali sobie sprawy, że są publiczne. Unikaj niepotrzebnej ingerencji w czyjeś życie prywatne.
3. Jeśli robisz zrzuty ekranu i dokumentujesz dane z mediów społecznościowych, pamiętaj że za tymi danymi stoją prawdziwi ludzie. Jeśli twoje systemy nie są bezpieczne, a dane wpadają w inne ręce, możesz nieumyślnie narazić ludzi na ryzyko.
4. Jeśli podczas weryfikacji zamierzasz opublikować cokolwiek w zamkniętych lub anonimowych grupach, czy użyjesz swojego prawdziwego imienia i nazwiska? Czy przedstawiś grupie swoje prawdziwe cele uczestniczenia w nich?

Więcej informacji na temat etyki i odpowiedzialnego raportowania można znaleźć w przewodniku [First Draft dotyczącym odpowiedzialnego raportowania w czasie manipulacji informacjami](#) oraz w rozdziale dotyczącym kwestii etycznych w przewodniku First Draft po zamkniętych grupach, aplikacjach do przesyłania wiadomości i aplikacjach online.

Pochodzenie

Czym jest oryginalna treść?

Sprawdzenie pochodzenia informacji, to jeden z najważniejszych punktów weryfikacji, który powinien zostać przeprowadzony jako pierwszy. Rzetelne określenie skąd pochodzą treści pozwoli Ci lepiej poznać kontekst i motywację jej twórców.

Jeśli masz wątpliwości, co do formy, czy kontekstu w jakim pierwotnie pojawiła się sprawdzana przez Ciebie treść w Internecie, to warto to prześledzić.

Nierzadko, do rozprzestrzeniania nieprawdziwych treści wykorzystuje się materiały, które pojawiły się w Internecie wiele lat wcześniej.

Mogły one być częścią żartu na 4chanie lub pojawiły się w wyniku skoordynowanej kampanii na grupie na Facebooku. Jeśli nie zadasz sobie pytań o pochodzenie treści, takich jak — kto był ich oryginalnym autorem, kiedy, gdzie i dlaczego zostały one opublikowane — to niewykluczone, że podasz do wiadomości informacje, które są nieprawdziwe.

Uwaga!

Bardzo łatwo jest pobrać zawartość ze strony internetowej lub Twittera, a następnie przesłać tę samą treść na inną platformę społecznościową. Są to tak zwane “scrapy”, które z pewnością utrudniają ustalenie, czy masz do czynienia z oryginalną treścią.

Wyszukiwania obrazów przy użyciu wstecznego wyszukiwania

Weryfikacja treści wizualnych przy użyciu wstecznego wyszukiwania obrazów (ang. reverse image search) to sposób, w którym wykorzystuje się zaawansowane oprogramowanie do znajdowania pasujących lub podobnych obrazów w dużej bazie danych, takiej jak zasoby Google Images. Z wyszukiwania wstecznego obrazów korzysta się w weryfikacji z dwóch głównych powodów:

1. Media wizualne są bardzo przekonujące, co oznacza, że wiele skutecznych form dezinformacji ma właśnie postać zdjęć i filmów.
2. Odwrotne wyszukiwanie obrazów pomaga ustalić pochodzenie treści, lub przynajmniej znaleźć inne jej wersje. Jeśli wiesz, że istnieją starsze wersje obrazu prezentowanego online jako nowe, jest to oczywisty znak, że najprawdopodobniej jest to treść wyrwana z kontekstu, zmieniona lub po prostu błędna.

Przewodnik po narzędziach

Każda z głównych wyszukiwarek internetowych jest nieco inna. Oto krótki opis różnic.



Google Images

Najbardziej użyteczną częścią wyników wyszukiwania odwrotnego obrazu Google znajduje się na dole strony, w sekcji „Strony zawierające pasujące obrazy”, co pozwala nam zobaczyć artykuły, które wcześniej używały tego zdjęcia. Google nie pozwala nam jednak porządkować wyników wyszukiwania według daty, ale pozwala nam wybrać niestandardowy zakres dat w celu zawężenia wyników. Wejdź na images.google.com, naciśnij ikonę aparatu w polu wyszukiwania i prześlij tam zdjęcie, lub obraz który sprawdzasz.

Yandex

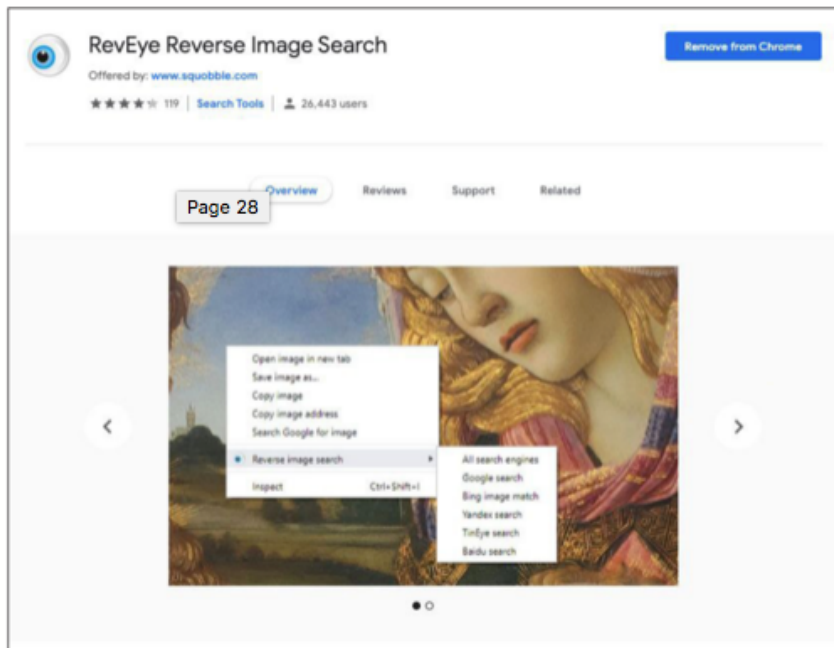
Rosyjska wyszukiwarka Yandex ma dużą bazę danych i kilka dodatkowych funkcji, których Google nie obsługuje, takich jak znajdowanie odwróconych twarzy lub obrazów. Jeśli nie znajdziesz czegoś w Google, wypróbuj Yandex.

TinEye

Zaletą TinEye jest to, że umożliwia łatwe porządkowanie wyników według daty. Oznacza to, że możesz szybko zobaczyć kiedy po raz pierwszy fotografia, która sprawdzasz została opublikowana, co przydaje się w określeniu jej pochodzenia. Minusem jest to, że zasoby TinEye są znacznie mniejsze niż innych wyszukiwarek, więc jeśli szukasz czegoś naprawdę rzadkiego, bardzo możliwe, że nie znajdziesz tego w TinEye.

Polecane przez nas narzędzie nr 1: rozszerzenie RevEye Reverse Image Search ([Chrome](#) lub [Firefox](#)).

Dzięki rozszerzeniu przeglądarki RevEye możesz kliknąć prawym przyciskiem myszy na zdjęcie i natychmiast przeprowadzić wyszukiwanie zdjęcia w dowolnej z wyżej wymienionych wyszukiwarek i paru innych. Z RevEye wyszukiwanie zdjęć możesz również przeprowadzić jednocześnie na wszystkich z nich.



RevEye Reverse Image Search, as available on the Chrome web store.
Retrieved September 7, 2019. Screenshot by author.

Weryfikacja wideo i korzystanie z InVid

Wyszukiwanie pochodzenia filmów jest podobne do weryfikacji zdjęć. Często pierwsza klatka wideo jest używana jako „miniaturka” wideo, czyli inaczej widok podglądu, który pokazuje się przed odtwarzaniem wideo i może być użyty do weryfikacji. Zrób zrzut ekranu klatki z filmu i przeprowadź na nim odwrotne wyszukiwanie obrazu w dokładnie taki sam sposób, jak w przypadku każdego innego materiału zdjęciowego.

Jednym z najskuteczniejszych narzędzi do weryfikacji filmów jest wtyczka [InVID Verification](#), której możesz użyć za pośrednictwem rozszerzenia przeglądarki Chrome lub Firefox. Oto niektóre z jej możliwości:

- Możesz z nią sprawdzić skąd pochodzi materiał, dzieląc dowolny film z mediów społecznościowych na miniatury, a następnie automatycznie zlecić wykonanie wstecznego wyszukiwania obrazu na wybranych przez Ciebie fragmentach nagrania za pomocą jednego kliknięcia.
- Pokazuje podstawowe dane związane z filmem: informacje o dacie i godzinie przesłania, informacje o koncie użytkownika, udostępnieniach i polubieniach oraz powiązany z nagraniem tekst.

- Wykorzystuje przetwarzanie języka naturalnego, aby wybrać komentarze dotyczące filmu wideo związane z weryfikacją — innymi słowy, wszelkie komentarze, które mogą dostarczyć wskazówek, czy film jest oryginalny, mylący lub wyrwany z kontekstu.
- Posiada lupę, dzięki której szybko sprawdzisz mały tekst na zdjęciu lub filmie — na przykład numer identyfikacyjny z boku samolotu.

Sprawdź anonimowe przestrzenie dla wcześniejszych wersji

Deinformacje, memy i inne rodzaje treści generowanych przez użytkowników w sieci społecznościowej często pochodzą z hermetycznych i anonimowych grup. Jeśli próbujesz znaleźć pierwszą wersję mema lub podejrzanego twierdzenia, czasami warto zacząć poszukiwania w określonych miejscach w sieci, gdzie komunikują się członkowie tych grup:

- Sprawdź Reddit: Możesz użyć do tego paska wyszukiwania.
- 4chansearch.com umożliwia przeszukiwanie witryn archiwów 4chan i aktualnych zbiorów 4chan
- [Gab.ai](https://gab.ai) jest jak Alt-Twitter, na której wylądowało wielu użytkowników zablokowanych przez Twitter
- Kanały do rozpowszechniania mowy nienawiści, grupy na Facebooku i grupy WhatsApp są trudniejsze do znalezienia i dokładnego rozczesania, ale mogą być warte wysiłku przy dłuższych łowach

Źródło

Chcesz wiedzieć jak sprawdzić, kto umieścił oryginalny fragment treści w Internecie? Kiedy mówimy o weryfikacji źródła, rozróżniamy, kto opublikował treść, a kto ją podał dalej. Głównym źródłem jest ten, kto uchwycił dany moment.

Przypuśćmy, że ktoś w Kairze nagrał na swoim telefonie wideo naocznego świadka, wysłał je swojemu przyjacielowi w Paryżu, a przyjaciel opublikował wideo na Twitterze. Ale głównym źródłem jest naoczny świadek w Kairze, a nie przyjaciel z Paryża. Idealnie chcemy zidentyfikować obie osoby. Identyfikacja oryginalnych źródeł nie jest łatwa, ale warta wytrwałej weryfikacji. W tym rozdziale znajdziesz kilka wskazówek i pytań, jak to zrobić.

Podstawowe pytania dotyczące źródeł

- Kim jest przesyłający?
- Sprawdź inne przesłane przez niego treści: Czego możesz się dowiedzieć o tym koncercie?
- Czy to możliwe, że autor tylko przesłał treść i nie jest jej oryginalnym twórcą?
- Czy to możliwe, że osoba, do której należy profil znajdowała się w pobliżu miejsca, w którym miało miejsce wydarzenie?
- Czy możesz znaleźć jakieś dane kontaktowe do tej osoby? Poszukaj numeru telefonu lub adresu e-mail, aby móc bezpośrednio z nimi porozmawiać. Ważne jest aby podjąć próbę

porozmawiania ze źródłem przed złożeniem jakichkolwiek oświadczeń o jego tożsamości i publikowanych treściach.

Wskazówki dotyczące badania źródeł

Wiele osób pozostawia po sobie w Internecie sporo ślady i niesamowite jest, jak wiele czasami możesz się dowiedzieć, łącząc punkty między różnymi kontami społecznościowymi należącymi do tych osób:

Oto kilka wskazówek:

- Spójrz na nazwę użytkownika konta i sprawdź, czy możesz znaleźć inne nazwy kont, które są takie same
- Wykonaj wyszukiwanie wtórne obrazów na zdjęciach z konta, które weryfikujesz
- Wyszukaj fragmenty wypowiedzi, aby sprawdzić, czy istnieją inne konta, które publikują dokładnie te same treści
- Jeśli znajdziesz jakiegokolwiek informacje kontaktowe powiązane z kontem, umieść je w pasku wyszukiwania i sprawdź, czy łączy Cię z innymi kontami na mediach społecznościowych.
- Możesz umieścić wiadomość e-mail w Skypie, która pokaże Ci wszystkich użytkowników powiązanych z tym adresem e-mail.
- Poszukaj źródła na LinkedIn, aby sprawdzić, czy możesz znaleźć przydatne informacje identyfikujące.
- Wiele postów w sieciach społecznościowych ma unikalny identyfikator, zwykle znajdujący się na końcu adresu URL.
- Możesz skopiować ten identyfikator i wkleić go do Google, aby zobaczyć, gdzie jeszcze treść została osadzona.
- Poszukaj strony internetowej powiązanej z kontem w mediach społecznościowych i wyszukaj tam wszelkie informacje identyfikujące.

Czy to konto jest zautomatyzowane?

Obecnie toczy się wiele dyskusji na temat botów i istnieje wiele narzędzi, które mogą pomóc określić, czy konta społecznościowe są zautomatyzowane (na przykład [Hoaxy](#) lub [BotSentinel](#)). Ale uważaj: kryminalistyka, zwłaszcza dotycząca botów to nieprecyzyjna nauka.

Oto, co musisz wiedzieć:

- Wiele narzędzi wykorzystuje 50 tweetów dziennie jako miarę do przewidywania, czy konto jest zautomatyzowane. Jednak wiele kont, które w ogóle nie są zautomatyzowane, z łatwością przekracza tę liczbę.
- Sama automatyzacja konta nie jest problemem — istotne jest to czy konsekwentnie rozpowszechnia dezinformacje online — czy to tworzoną przez ludzi, czy maszyny
- Na przykład mianem „cyborgów” określa się ludzi, którzy wykazują zachowanie podobne do botów, takie jak częste i konsekwentne publikowanie postów przez cały dzień. Niektórzy są

opłacani - to ich praca. Inni przedstawiciele tej grupy to po prostu zagorzali zwolennicy konkretnego stanowiska politycznego lub kandydata politycznego, którzy postrzegają swoją aktywność online jako rolę we wspieraniu sprawy, na której im zależy.

- Jeśli nadal chcesz dowiedzieć się, czy konto jest faktycznie zautomatyzowane, lepszym wykładnikiem może być aktywność na Twitterze w ciągu dnia. Większość ludzi musi spać, więc ich aktywność powinna obejmować okres ciszy, aby to odzwierciedlić. To wciąż nie jest jednak doskonałe rozwiązanie, bo tweety można też łatwo zaplanować tak, by pojawiały się o różnych porach dnia i nocy.

Korzystanie z Twitonomy do zrozumienia kont na Twitterze

[Twitonomy](#) to kolejne świetne narzędzie, którego używamy do badania kont na Twitterze. Oto kilka interesujących pytań dotyczących kont, na które Twitonomy może pomóc Ci odpowiedzieć:

- Kiedy powstały i jak prezentuje się historia ich tweetów na przestrzeni czasu?
- Jaka jest ich średnia liczba tweetów dziennie?
- Jaki procent ich tweetów jest retweetowanych?
- Których użytkowników retweetują najczęściej?
- Którym użytkownikom odpowiadają najczęściej?
- Jakie są ich najczęściej używane hashtagi?

Sprawdzanie domen

Czasami będziesz chciał zbadać własność określonej witryny. Istnieje wiele witryn, które ci w tym pomagają, ale [viewDNS.info](#) jest ulubionym. Umożliwia wykonywanie podstawowych wyszukiwań domen i adresów IP, ale obejmuje także inne wyszukiwania, w tym historyczne adresy IP dla domeny i lokalizatory adresów IP.

Oto kilka krótkich wskazówek dotyczących domen:

Jeśli kwestionujesz autentyczność witryny, poszukaj podejrzanych zakończeń adresów URL.

Jeśli rejestrujący zapłacił za ukrycie informacji rejestracyjnych domeny, poszukaj starych wersji tej witryny.

Czasami witryna zostanie przeniesiona na nowszą, a rejestrujący zapłaci jedynie za ochronę nowej witryny, zapominając również o ukryciu poprzedniej wersji.

Możesz poszukać odmian adresu URL, takich jak .net lub .info, lub możesz wyszukać domenę w Google i sprawdzić, czy pojawi się coś z nią związanego. Pamiętaj, że te informacje są automatycznie chronione przez przepisy RODO w Europie.

Możesz sprawdzić adresy IP, aby zobaczyć inne witryny hostowane na tym samym serwerze. Te witryny niekoniecznie są powiązane, ale wyniki mogą być czasami naprawdę owocne.

Narzędzia w jakie warto zainwestować

Wiele narzędzi, których wcześniej używaliśmy do badania mediów społecznościowych, zostało zamkniętych z powodu uzasadnionych obaw o prywatność. Jednak nadal istnieją bardzo dobre płatne narzędzia, w które warto zainwestować, takie jak [Spokeo](#) i [Pipl](#). Bazy danych jakie zawierają są szczególnie pomocne w znajdowaniu informacji kontaktowych.

Data

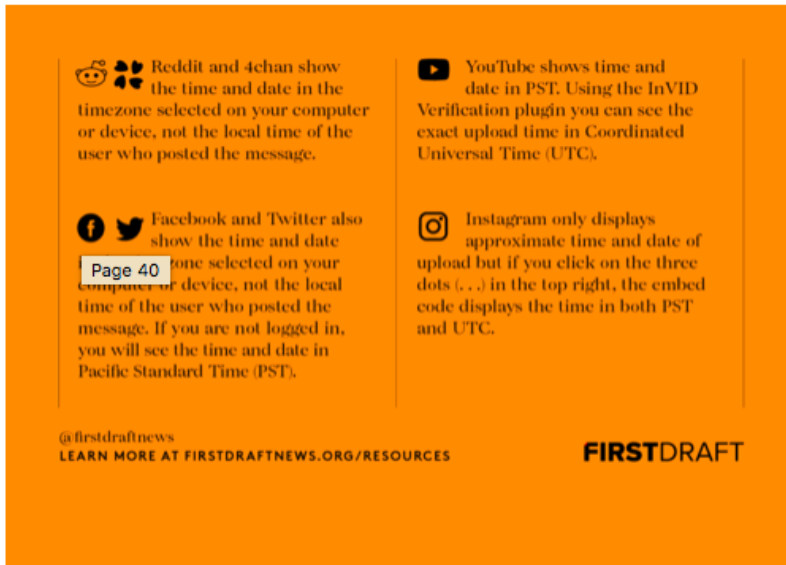
Kiedy treść została zarejestrowana? Każdy post w mediach społecznościowych ma sygnaturę czasową, ale sygnatury czasowe informują tylko, kiedy treść została przesłana, a nie kiedy została faktycznie stworzona, czy zarejestrowana. Prawdziwie dobrze wykonana weryfikacja powinna więc móc określić, kiedy powstał materiał.

Teraz, gdy smartfony są tak wszechobecne, często zdarza się, że ludzie dodają treści zaraz po uchwyceniu, ale nie można zakładać, że tak jest.

Użytkownicy mogą również pobierać treści innych osób i ponownie je publikować dni lub lata po ich pierwszym pojawieniu się w sieci. W tym rozdziale dowiesz się, jak zbliżyć się do określenia faktycznego

Przewodnik po znacznikach czasu w mediach społecznościowych

Wszystkie platformy mają różne sposoby wyświetlania dat i godzin. Poniżej znajdują się przydatne odniesienia:



Dane Exif

Kolejną przydatną metodą znajdowania godziny lub daty kiedy fragment treści został uchwycony, są metadane w zapisane w pliku.

Każde zdjęcie, które robimy aparatem cyfrowym, zawiera dodatkowe informacje w pliku obrazu, takie jak godzina, data, ustawienia aparatu, informacje o urządzeniu, a nawet współrzędne, jeśli urządzenie ma włączony GPS. Nazywa się to jego danymi Exif (format pliku obrazu wymiennego).

Świetnym darmowym narzędziem do przeglądania danych Exif pliku jest przeglądarka Exif 20 Jeffrey'a. Po prostu prześlij plik obrazu, a wyświetli on dodatkowe zapisane informacje. Ale uwaga: prawie wszystkie platformy mediów społecznościowych usuwają dane Exif, gdy użytkownik przesyła obraz, więc będziesz potrzebować oryginalnego pliku, aby to zadziałało. Podczas weryfikacji treści naocznych świadków poproś przesyłającego o przesłanie oryginalnego pliku obrazu pocztą e-mail w celu dokończenia weryfikacji.

Jest to warte zachodu, jeśli wątpisz w wiarygodność opublikowanego przez kogoś obrazu lub pliku. Co więcej metoda ta działa również na innych typach plików. Oczywiście, zawsze możliwe jest sfalszowanie lub zmiana metadanych pliku, ale tylko najbardziej wyrafinowani oszuści będą tego próbować.

Profesjonalne porady i narzędzia do weryfikacji dat

- Wtyczka InVID Verification pozwala zobaczyć czas przesyłania filmów społecznościowych w UTC.
- [SunCalc](#) pozwala zobaczyć kąt słońca w konkretnym dniu w określonym miejscu, co może pomóc określić, o której porze dnia coś się wydarzyło na zdjęciu lub filmie.

- [Wolfram Alpha](#) to skomputeryzowana wyszukiwarka wiedzy, która między innymi pozwala sprawdzić pogodę od określonej daty. Wpisz frazę, np. „Jaka była pogoda w Omaha 5 listopada 2017 r.”, aby uzyskać wynik.
- Zawsze pamiętaj, aby najpierw określić prawdziwe pochodzenie materiału. Wykonaj wtórne wyszukiwanie obrazu, jeśli patrzysz na media wizualne, aby sprawdzić, czy istnieją starsze wersje treści.

Lokalizacja

Gdzie została uchwycona treść? Posty w mediach społecznościowych są często oznaczone geotagiem lokalizacji, ale niekoniecznie jest to lokalizacja, w której uchwycone zostało np. zdjęcie, czy nagranie. Geotagi mogą być błędne, treść można nagrać w jednym miejscu na świecie, a następnie przesłać gdzie indziej. Użytkownicy mediów społecznościowych oddalonych od siebie tysiące kilometrów mają możliwość swobodnego zawłaszczania treści innych osób i publikowania je tak, jakby były ich własnymi.

Ten rozdział pomoże Ci zweryfikować, gdzie została przechwycona oryginalna treść.

Podstawowe pytania dotyczące lokalizacji

- W jakim miejscu znajduje się konto powiązane z treścią?
- Czy dodają tagi do lokalizacji w swoich treściach?
- Jeśli zidentyfikowano lokalizację, czy ma sens, że właściciel konta tam był?
- Czy autor treści wcześniej odnotowywał swoją lokalizację w innych postach?

Wyszukiwanie lokalizacji na platformach

Kiedyś wyszukiwanie według lokalizacji na platformach było bardzo łatwe, ale ze względu na zmieniające się obawy dotyczące prywatności wiele z tych funkcji zostało usuniętych. Istnieje kilka narzędzi innych firm, które nadal umożliwiają przeprowadzanie tych wyszukiwań. Na przykład narzędzie wyszukiwania [whopostedwhat](#) na Instagramie umożliwia wyszukiwanie postów oznaczonych konkretną datą w określonej lokalizacji. Wiele z tych narzędzi innych firm pojawia się i znika, więc najlepiej jest zbudować własny zestaw narzędzi i być na bieżąco ze zmianami i aktualizacjami.

Nie daj się zwieść! Geotagi mogą Cię oszukać

Czasami możesz zobaczyć lokalizację geograficzną powiązaną z konkretnym tweetem lub postem na Facebooku, ale tymi informacjami można też łatwo manipulować, tak jak metadanymi.

Zawsze niezależnie weryfikuj lokalizację

Jeśli oglądasz zdjęcie lub film, znajdź lokalizację na mapie lub obrazie satelitarnym, aby móc je znaleźć.

Nawet zdjęcia satelitarne mogą być wadliwe

Geolokalizacja jest zawsze trudniejsza, gdy zdjęcia satelitarne są nieaktualne. Niektóre warte opublikowania wydarzenia, takie jak ekstremalna pogoda lub wojna, mogą radykalnie zmienić krajobraz w ciągu kilku minut. To sprawia, że geolokalizacja filmów jest wyzwaniem w krajach takich jak Syria czy krajach dotkniętych katastrofą naturalną np. huraganem.

Wyteż swoje zmysły obserwacyjne

Najważniejszą umiejętnością, jaką należy rozwinąć w celu weryfikacji lokalizacji, jest umiejętność obserwacji. To niesamowite, co możesz geolokalizować, jeśli zwrócisz uwagę na szczegóły na zdjęciach i filmach.

Oto kilka pytań, które pomogą Ci zacząć:

- Czy dostrzegasz jakieś unikalne cechy geograficzne? Główne drogi? Duże trawiaste pola? Góry?
- Czy istnieją unikalne budynki, które łatwo byłoby dostrzec na zdjęciach satelitarnych?
- Szukaj numerów telefonów, tablic rejestracyjnych, tytułów firmowych i napisów na banerach i znakach.
- Zbadaj kontekst: Czy w treści są jakieś wydarzenia i okoliczności, które mogą pojawić się w artykułach z wiadomościami?
- Zwróć uwagę na pogodę, liście i ubrania — czy to ma sens dla lokalizacji?

Sprawdzanie lokalizacji przy użyciu widoku satelitarnego i widoku ulicy

Oto kilka narzędzi, o których warto wiedzieć, gdy samodzielnie weryfikujesz lokalizację:

- Możesz wyszukiwać nazwy sklepów i przeglądać lokalizacje w widoku satelitarnym w [Mapach Google](#).
- [Google Earth](#) da Ci większe pole do popisu - możesz z nim przeglądać historyczne dane satelitarne.
- Jeśli naprawdę interesujesz się zdjęciami satelitarnymi, warto przyjrzeć się różnym wyszukiwarkom, które podadzą dane z różnych czasów. [Bing](#) i [Yandex](#) to dwie inne opcje. Yandex dostarcza więcej danych o Europie Wschodniej niż Google.
- Wikimapia to ciekawe narzędzie, które pozwala społeczności opisywać obiekty na mapie.
- Geolokalizacja często wiąże się z identyfikacją wielu różnych elementów na zdjęciu lub filmie, które pomagają nam w ustaleniu miejsca, w którym materiał został uchwycony.

Numer kierunkowy numeru telefonu na billboardzie to dobry początek, ale w połączeniu z masztem telefonicznym gdzieś w tle i unikalnym kolorowym dachem w ciekawym kształcie, mamy znacznie większą szansę na rozpoznanie lokalizacji.

Motywacja

Dlaczego treść została w ogóle stworzona, a potem opublikowana?

Ten rozdział jest najkrótszy, ponieważ prawie niemożliwe jest zweryfikowanie, dlaczego ktoś uchwycił jakiś obraz, czy sytuację, albo udostępnił fragment treści. Zawsze możesz ich zapytać, a czasami nawet to nie przyniesie prawdy. Jednak zrozumienie motywacji, a przynajmniej jej wycucie, może być bardzo pomocne w dalszej części procesu weryfikacji.



Oto kilka podstawowych pytań dotyczących motywacji:

- Czy w przypadku zdjęć i filmów osoba, która uchwyciła treść była przypadkowym, naocznym świadkiem?
- Czy profil osoby lub korzystanie z mediów społecznościowych sugeruje, że jest ona aktywistą lub agitatorem?
- Czy dana osoba uczestniczyła w wydarzeniu, aby uchwycić je z określonej perspektywy?
- Czy dana osoba jest powiązana z rządem, korporacją lub organizacją badawczą?
- Czy dana osoba jest członkiem społeczności internetowej, która wspiera lub promuje określoną sprawę?

Przypomnienie o zachowaniu rygorystycznych standardów

Pamiętaj, że cytaty lub wyjaśnienia zamieszczone w sieci nie są tak wiarygodne, jak bezpośredni wywiad ze źródłem. Jeśli to możliwe i bezpieczne, skontaktuj się bezpośrednio z osobą, która stworzyła analizowaną przez Ciebie treść lub informacje.

Informacje o autorce

Shaydanay Urbani jest menedżerem ds. partnerstw i programów First Draft w Nowym Jorku, gdzie zajmuje się dezinformacją i szkoleniem dziennikarzy na całym świecie w zakresie weryfikacji i odpowiedzialnego raportowania. Ma doświadczenie w sprawozdawczości w sprawach karnych, językach i polityce Bliskiego Wschodu oraz polityce żywnościowej. Uzyskała tytuł licencjata na Uniwersytecie Kalifornijskim w Los Angeles oraz tytuł magistra na Craig Newmark Graduate School of Journalism na CUNY w Nowym Jorku.