POLECA
SEKURAK.PL

securitum

Krzysztof Wosiński

OSINT
NOWY WYMIAR POSZUKIWAŃ W SIECI

securitum

Projekt okładki: Krzysztof Kopciowski
Projekt typograficzny: Krzysztof Kopciowski
Redaktor: Tomasz Turba
Redakcja merytoryczna: Foxtrot Charlie

Redaktor prowadzący: Katarzyna Sajdak
Adiustacja językowa: Magdalena Anioł
Skład i łamanie: Krzysztof Kopciowski
Korekta: Magdalena Anioł, Ewa Budka, Paulina Lenar

ISBN: 978-83-974231-9-0

Wydanie II poszerzone
Kraków 2025

Securitum Wydawnictwo sp. z o.o.
ul. Siostry Zygmunty Zimmer 5
30-441 Kraków
e-mail: wydawnictwo@securitum.pl
securitum.pl

Zastrzeżenia prawne

Bezpieczeństwo IT ma coraz większe znaczenie. Nie można profesjonalnie zabezpieczyć aplikacji czy systemu, nie znając technik ich atakowania. Omawiamy je w tej książce, ponieważ to bardzo skuteczny sposób podnoszenia wiedzy i świadomości użytkowników, administratorów i twórców aplikacji.

Wszelkie podawane przez nas informacje powinny jednak być wykorzystywane wyłącznie w granicach prawa, co z reguły oznacza zakaz wykorzystywania omawianej tu wiedzy bez zgody dysponenta systemu czy sieci. Wyjście poza te granice może skutkować zarówno odpowiedzialnością cywilną (np. obowiązkiem naprawienia wyrządzonej szkody), jak i odpowiedzialnością karną. Przykładowo, zgodnie z polskim kodeksem karnym nieuprawnione uzyskanie dostępu do systemu informatycznego lub jego części podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2 (art. 267 §2 kodeksu karnego). Z kolei nieuprawnione zakłócenie w istotnym stopniu pracy systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych podlega karze pozbawienia wolności od 3 miesięcy do lat 5 (art. 269a kodeksu karnego).

Zwracamy na to uwagę, ponieważ **nie jest naszym zamiarem wspieranie jakichkolwiek bezprawnych działań**. Dlatego zastrzegamy, że w najszerszym prawnie dopuszczalnym zakresie wyłączamy naszą odpowiedzialność za skutki takich działań.

securITum

SEKURAK.ACADEMY

Miejsce, w którym rzetelna wiedza łączy się z dużą dawką pozytywnej energii i dobrego humoru. Świetna opcja na udaną inwestycję w siebie.

DOŁĄCZ DO NAS

sekurak.academy

-25%

z kodem: **e-akademia**

Od Redakcji

Seria książek i e-booków ukazujących się nakładem Securitum Wydawnictwo ma na celu przybliżanie wybranych zagadnień z szeroko rozumianego IT w jak najbardziej praktycznym podejściu.

Tworzymy ją dla osób, które potrzebują bodźca, żeby rozpocząć samodzielne zgłębianie jakiegoś tematu, ale albo trochę się wahają, albo nie mają pewności, że to droga dla nich.

Książki w tej serii będą też swoistymi poradnikami dla bardzo początkujących, szukających wprowadzenia w temat na poziomie podstawowym.

Są one różnymi ścieżkami prowadzącymi w świat bezpieczeństwa IT, na które zapraszamy Czytelników portalu sekurak.pl i słuchaczy Sekurak.Academy:

1. Adam Samson,
   Bezpieczeństwo domowego routera Wi-Fi. Wprowadzenie
2. Krzysztof Wosiński,
   OSINT: nowy wymiar poszukiwań w sieci
3. Grzegorz Trawiński,
   Certyfikacje ofensywne w cyberbezpieczeństwie
4. Maciej Góra, *Era cyberszpiegów*
5. Robert (ProXy) Kruczek, *Socjotechnika w praktyce. Triki i kruczki hackowania ludzi*

Spis treści

Krzysztof Wosiński. Certyfikowany tester bezpieczeństwa systemów IT (Certified Ethical Hacker) specjalizujący się w systemach militarnych oraz wywiadzie otwartoźródłowym (Open-Source Intelligence, OSINT), zwanym także „białym wywiadem".

Od kilkunastu lat zajmuje się zagadnieniami jakości oraz bezpieczeństwa sprzętu i oprogramowania o przeznaczeniu wojskowym, produkowanych dla polskich i amerykańskich odbiorców. Obecnie koncentruje się na cyberbezpieczeństwie systemów tworzonych dla Sił Zbrojnych RP.

Autor popularnych serii OSINT HINTS oraz Czwartki z OSINT-em w portalu sekurak.pl.

Współautor I tomu książki *Wprowadzenie do bezpieczeństwa IT:* rozdział *Bezpieczeństwo danych w spoczynku – szyfrowanie i usuwanie danych*[*].

W Securitum od 2020 roku prowadzi szkolenia z OSINT-u, bezpieczeństwa działań w sieci oraz z przeciwdziałania dezinformacji. Jest autorem serii szkoleń „OSINT master" (część 1: Poszukiwanie informacji o osobach, miejscach i pojazdach oraz część 2: Geolokalizacja osób – jak szukać informacji i jak nie dać się znaleźć) i OSINT dla każdego – podstawy poszukiwań informacji w Internecie.

Prowadzi także dwudniowe szkolenie OSINT/OPSEC – narzędzia, techniki śledcze, ochrona przed śledzeniem, podczas którego można bliżej zapoznać się z technikami i narzędziami, opisanymi w tej książce.

Jest również wykładowcą Akademii Sekuraka, gdzie przybliża uczestnikom tematy związane z OSINT-em i bezpieczeństwem pracy w Internecie.

W 2023 roku obronił doktorat z zakresu OSINT-u, który zwieńczyło wydanie książki *Bezpieczeństwo osób i systemów IT z wykorzystaniem białego wywiadu. OSINT* (Warszawa 2024).

Po godzinach zgłębia zagadnienia związane z socjotechniką i białym wywiadem, a także tworzy narzędzia usprawniające rozpoznanie otwartoźródłowe.

---

* K. Wosiński, *Bezpieczeństwo danych w spoczynku – szyfrowanie i usuwanie danych* [w:] *Wprowadzenie do bezpieczeństwa IT*, t. 1, Kraków 2023, s. 569–618.

OD AUTORA

Internet. Ostateczna granica. Oto zredagowane na nowo, uzupełnione i poszerzone zapiski z serii artykułów ukazujących się w portalu *sekurak.pl* dotyczących **OSINT-u (Open-Source Intelligence)**, czyli wywiadu prowadzonego z wykorzystaniem ogólnodostępnych źródeł danych. W przypadku opisywanych technik, narzędzi i śledztw są one głównie źródłami internetowymi, chociaż warto pamiętać, że OSINT może korzystać także z klasycznych kanałów informacyjnych, takich jak np. prasa, radio czy telewizja.

Teksty opublikowane w książce zostały uzupełnione i zaktualizowane do realiów Internetu z chwili oddawania do druku jej pierwszego wydania, choć może się okazać, że kiedy ją czytasz, jej otoczenie jest już w innym miejscu. W szczególności dotyczy to zagadnień dotyczących rozwoju sztucznej inteligencji. Z tego powodu w drugim wydaniu tej książki znalazł się nowy rozdział poświęcony śledzeniu zmian w świecie AI w kontekście białego wywiadu.

W pierwszej części, *OSINT – techniki* (rozdziały R1–R22), znaleźć można opis technik wykorzystywanych w ramach działań OSINT-owych, w drugiej, *OSINT – narzędzia* (rozdziały R23–R30), przedstawione zostały wybrane narzędzia najczęściej wykorzystywane w białym wywiadzie, a w trzeciej: *OSINT hints* (rozdziały R31–R34) – wskazówki, które w artykułach publikowanych w portalu *sekurak.pl* ukazywały się w ramach popularnej serii „OSINT Hints". Ostatnia, czwarta część książki, *OSINT w biznesie* (rozdziały R35–R36), dotyczy styku technologii z biznesem, a więc technik ataku i sposobów obrony przed działaniami wykorzystującymi OSINT oraz socjotechnikę.

Mam nadzieję, że Czytelnicy znajdą w tej publikacji wiele interesujących przypadków, dotyczących działań OSINT-owych, które spowodują zwiększenie apetytu na dalsze zgłębianie tej, bardzo ciekawej i coraz częściej wykorzystywanej w codziennym życiu i pracy, tematyki.

A tych, których przygoda z OSINT-em przyciąga jeszcze bardziej, zapraszam do lektury mojej książki: *Bezpieczeństwo osób i systemów IT z wykorzystaniem białego wywiadu. OSINT*[*].

---

* K. Wosiński, *Bezpieczeństwo osób i systemów IT z wykorzystaniem białego wywiadu. OSINT*, Warszawa 2024.

CZĘŚĆ I: OSINT – TECHNIKI

R1 OPSEC PRZEDE WSZYSTKIM

W tym rozdziale poruszę temat, który warto rozważyć jeszcze przed rozpoczęciem jakichkolwiek czynności OSINT-owych, dotyczący zapewnienia sobie odpowiedniego poziomu bezpieczeństwa w ramach prowadzonych działań (określanego często jako **OPSEC, czyli Operations Security**).

Jedną z historii, które dają pogląd na to, **jak ważne jest oddzielenie informacji na kontach wykorzystywanych do anonimowych działań od wszelkich elementów prawdziwej tożsamości**, jest przypadek domniemanego wyśledzenia konta dyrektora FBI, Jamesa Comeya. Domniemanego, gdyż nie udało się uzyskać potwierdzenia, że namierzone konto na Twitterze* naprawdę należy do niego, jednak wszystkie poszlaki na to wskazują, łącznie z komentarzem samego zainteresowanego. Przyjrzyjmy się zatem bliżej błędom, które zostały popełnione podczas zakładania i utrzymywania tego konkretnego konta.

Błąd 1: Przyznanie, że konta w ogóle istnieją

Wszystko zaczęło się od pewnego spotkania, a konkretnie od Intelligence and National Security Alliance Dinner, na którym pod koniec marca 2017 roku przemawiał właśnie James Comey. Podczas godzinnego wystąpienia, w którym przekazywał informacje o tym, jak ważne są różne aspekty bezpieczeństwa, a także starał się sprytnie unikać odpowiedzi na zbyt konkretne pytania, padło też stwierdzenie, że jemu „bardzo zależy na prywatności", więc jest, co prawda, na Twitterze oraz Instagramie, gdzie „ma jedynie dziewięciu obserwujących", jednak są to wyłącznie osoby należące do jego najbliższej rodziny i znajomych, gdyż nie lubi się dzielić prywatnymi zdjęciami z ludźmi spoza tego kręgu (dla zainteresowanych – dostępne jest nagranie z tego spotkania (rysunek 1)[1], a temat prywatności poruszany jest w 21. minucie).

* W książce będziemy używać obu nazw tej platformy: Twitter oraz X, w zależności od momentu, z którego pochodzą cytowane wpisy albo omawiane mechanizmy, traktując lipiec 2023 jako moment zmiany jej nazwy.

Rysunek 1. Dyrektor FBI zdradza informację o swoim koncie na Instagramie

Te skąpe informacje o posiadanych kontach, poparte niewielkim dodatkowym śledztwem dziennikarskim Ashley Feinberg[2], dotyczącym szczegółów życia i kariery dyrektora FBI, pozwoliły na odnalezienie informacji na temat jego syna, którego imię (niestety dla poszukiwaczy) jest takie samo, jak drugie imię jego ojca – Brien. Niemniej jednak, w końcu, poprzez wpisy na kontach szkolnych drużyn sportowych na Twitterze, możliwe było dotarcie do konta Briena na Instagramie.

Błąd 2. Powiązanie kont prywatnych z anonimowymi kontami

Znaleziony na Instagramie profil został jednak zamknięty, co znacznie utrudniło Ashley Feinberg dalsze poszukiwania. Tutaj jednak przydatna okazała się funkcjonalność, która umożliwiła odnalezienie innych powiązanych kont, a polegała ona na próbie śledzenia zablokowanego konta, a następnie na skorzystaniu z funkcjonalności podpowiedzi innych znajomości, które zostały dobrane na podstawie wcześniejszego wyboru.

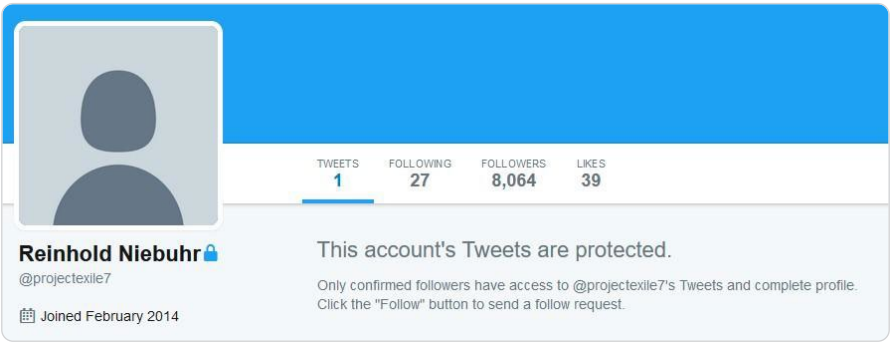
Planując takie działania, najlepiej stworzyć zupełnie nowe, „czyste" konto (ta technika ma zastosowanie w wypadku wielu portali społecznościowych, nie tylko Instagrama) i pozwolić, by algorytmy zaproponowały dodanie kolejnych znajomych na podstawie jednej tylko osoby. Można tu wykorzystać „czysty" (nieskonfigurowany) telefon, z wpisanym jednym kontaktem, do którego oczywiście damy dostęp apce społecznościowej, a sugerowane kontakty wskażą najprawdopodobniej powiązane z nią osoby (albo jej dane osobowe, jeśli np. posiadamy tylko numer telefonu). Zamiast telefonu można wykorzystać także maszynę wirtualną lub emulator.

Błąd 3. Używanie nazwy użytkownika związanej z wyszukiwaną osobą

W omawianym przypadku wśród znalezionych powiązanych kont było jedno, które nie do końca pasowało do innych kont osobistych znajomych i członków rodziny ze względu na dość unikatową nazwę: @reinholdniebuhr (rysunek 2). Tutaj przydało się szybkie przestudiowanie historii edukacji Jamesa Comeya, który, jak się okazało, swego czasu napisał pracę dyplomową m.in. o teologu nazwiskiem Reinhold Niebuhr. Ten szczegół wskazywał, że to konto może faktycznie być poszukiwanym profilem dyrektora FBI, tym bardziej że posiadało ono dziewięć obserwujących je osób, co pokrywało się dokładnie z oświadczeniem Comeya.

Na rysunku 3 widoczne jest konto Jamesa Comeya na Twitterze – tutaj, tak samo jak na Instagramie, jako Reinhold Niebuhr.

Rysunek 2. Konto dyrektora FBI na Instagramie już po jego „odkryciu"



Rysunek 3. Konto Jamesa Comeya na Twitterze – tutaj, tak samo jak na Instagramie, jako Reinhold Niebuhr (stan na 12 kwietnia 2017 roku)

Próba przeskoku z konta na Instagramie na konto na Twitterze nie była łatwa, gdyż profil o tej samej nazwie użytkownika nie wyglądał jak należący do głównego bohatera, więc Ashley Feinberg pozostało szukanie po nazwie użytkownika (a nie loginie). Jednym z kont, które wyglądało obiecująco ze względu na dość skryty profil, było konto: @projectexile7 (rysunek 4). I tutaj kolejny raz dał o sobie znać błąd polegający na wykorzystaniu nazwy, którą można było dość jednoznacznie powiązać z osobą dyrektora FBI, gdyż Project Exile* był jednym z projektów, które współprowadził.

Błąd 4. Komentarze w jednym temacie

Na odnalezionym koncie z Twittera można zauważyć, że znaczna liczba polubionych wpisów dotyczy osoby Jamesa Comeya, a jedyną osobą śledzącą to konto jest jego przyjaciel, Benjamin Wittes. Także analiza kont, które są śledzone przez @projectexile7, wskazuje na powiązania z upodobaniami dyrektora FBI w zakresie źródeł informacji.

Rysunek 4. Mała wskazówka – wpis zretweetowany przez konto @projectexile7 wskazuje, że jednak śledztwo zaimponowało jego właścicielowi

Te wszystkie drobne okruchy oczywiście nie dają pewności co do właściciela znalezionych kont. Należy pamiętać, że w ramach OSINT-u ważnym elementem jest analiza zgromadzonych dowodów i uczciwe odpowiedzenie sobie na

* Project Exile dotyczył zwalczania przestępstw z użyciem broni poprzez eskalację procesów osób nielegalnie posiadających broń na poziom federalny i, co za tym idzie, zwiększenie wyroków oraz tytułowe „wygnanie", czyli osadzenie skazanych z dala od ich miejsc zamieszkania.

pytanie: czy na pewno mogę wskazać daną osobę jako powiązaną z badaną sprawą? Nie można w tym miejscu, niestety, poddać się podświadomej chęci poskładania wszystkich elementów w bardzo medialną i robiącą wrażenie całość. Nie jest żadną ujmą przyznanie w pewnym momencie, że nie ma się pewności i podstaw do wydania konkretnych osądów. Niestety, często podświadomie ulegamy emocjom i układamy historię tak, jak chcielibyśmy, aby się ułożyła – wszystkie złe cechy przypisujemy osobom z łatką „tych złych", a zbyt mocno próbujemy wybielić osoby, które wydają nam się sympatyczne i co do których jesteśmy nastawieni bardziej przychylnie.

Na zakończenie

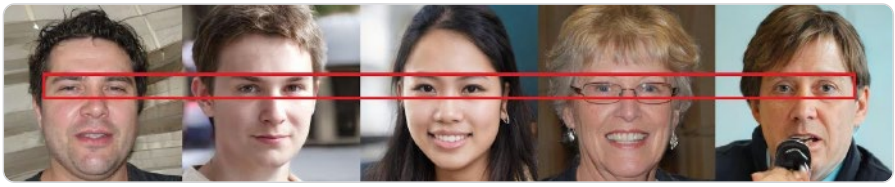
Przedstawiona historia pokazuje kilka błędów popełnianych w ramach przygotowywania środowiska i zasad bezpieczeństwa operacji, czyli OPSEC-u, a także bezpieczeństwa osobistego, czyli PERSEC-u. Po pierwsze, zawsze musimy sobie odpowiedzieć na pytanie, jaki zakres działań powinniśmy wykonać, aby uzyskać odpowiedni poziom bezpieczeństwa, gdyż nie każde śledztwo w Internecie wymaga takiego samego poziomu zabezpieczenia.

Musimy także powstrzymać się od informowania o tym, jakie konta są wykorzystywane do anonimowej pracy i w jakich działaniach biorą udział. Nawet dyrektor FBI nie powstrzymał się od uchylenia rąbka tajemnicy, ale taką pokusę ma też wiele innych osób, zwłaszcza pracujących w sferach życia dotyczących bezpieczeństwa, gdzie pojawia się sporo bardzo ciekawych historii. Niestety, lista osób, z którymi można na dany temat porozmawiać, niekiedy ogranicza się do wąskiego kręgu współpracowników lub – w skrajnych przypadkach – zaledwie jednego człowieka.

Tworząc środowisko do pracy, trzeba pamiętać o **technologicznej stronie OPSEC-u**, szczególnie w przypadku śledztw o wysokim poziomie ryzyka (czyli np. dotyczących przestępstw, terroryzmu lub mogących wpłynąć na czyjeś bezpieczeństwo osobiste). Począwszy od kwestii typowo **sprzętowo-systemowych** (jakiego komputera, telefonu, łącza internetowego będę używać), poprzez **oprogramowanie** (jaka przeglądarka, dodatki anonimizujące czy VPN), aż po takie elementy, jak **budowanie swoich „kukiełek"** (ang. *sock-puppets*, czyli fałszywych tożsamości, których konta będziemy wykorzystywać podczas prowadzenia śledztwa). Ten ostatni element ma jeszcze wiele dodatkowych kwestii do dopięcia, takich jak np. zdjęcia profilowe, których dobre przygotowanie wymaga odrobinę większego nakładu pracy niż tylko pobranie obrazu z serwisu *thispersondoesnotexist.com*.

Na rysunku 5 widoczne są **zdjęcia** wygenerowane przez model sztucznej inteligencji **GAN (Generative Adversarial Network, generatywne sieci przeciwstawne)**. Niekiedy są one używane jako zdjęcia profilowe dla fałszywych kont w mediach społecznościowych. Używanie obrazów generowanych przez

GAN dla kont w serwisach społecznościowych jest jednak dość łatwe do wychwycenia (rysunek 6). Obecnie dużo lepsze zdjęcia dla kont profilowych można generować za pomocą narzędzi AI, o czym piszę szerzej w rozdziale *Jak narzędzia AI zmieniają OSINT* (s. 166–173).



Rysunek 5. Zdjęcia wygenerowane przez model sztucznej inteligencji GAN niekiedy są używane jako zdjęcia profilowe dla fałszywych kont w mediach społecznościowych. Jednym z elementów ułatwiających ich rozpoznanie jest umieszczanie oczu zawsze w tym samym miejscu zdjęcia

Rysunek 6. Przykład fałszywego konta rzekomego ukraińskiego dziennikarza

Dla konta-kukiełki należy także wygenerować odpowiednie dane osobowe, przemyśleć sposoby ukrywania się, a w przypadku posiadania wielu kont także zarządzania ich tożsamościami i ich utrzymywania.

Podsumowanie i rady

- Nie ujawniaj istnienia kont, których „spalenie" może narazić całą operację na porażkę.
- Nie twórz powiązań pomiędzy kontami prywatnymi a tymi wykorzystywanymi do działań OSINT-owych (w momencie kiedy otrzymasz na swoim anonimowym koncie propozycję znajomych z kręgu twoich krewnych lub przyjaciół, już jest za późno).

- Nie wykorzystuj do tworzenia anonimowych kont informacji, które można łatwo powiązać z Tobą.
- Nie zdradzaj swojej prawdziwej tożsamości przez aktywność związaną z Twoimi rzeczywistymi zainteresowaniami lub nawiązaniami do Ciebie.

R2 GOOGLE'A SZKIEŁKO I OKO, CZYLI CO NOWEGO W WYSZUKIWANIU ZAWARTOŚCIĄ OBRAZÓW

Kiedy w 2021 roku przeprowadziłem badanie *Jak wyszukiwarki radzą sobie z analizą zawartości obrazów*[3], najpopularniejsze z nich: **Google** i **Bing**, wypadły dość blado na tle wyszukiwarki **Yandex**. Od tego czasu Google zrobiło duży krok naprzód, integrując stopniowo narzędzie Obiektyw Google (Google Lens) ze swoją wyszukiwarką grafiki. Od listopada 2022 roku narzędzie to jest już domyślnie stosowane w przypadku korzystania z funkcjonalności wyszukiwania za pomocą obrazu w Google. Czas więc na sprawdzenie, jak zabieg ten zmienił układ sił wśród trzech najpopularniejszych wyszukiwarek.

> Google – wyszukiwarka od firmy Google, umożliwiająca m.in. wyszukiwania tekstowe oraz wyszukiwanie obrazem, realizowane z wykorzystaniem narzędzia Obiektyw Google (Google Lens), które zastąpiło Grafikę Google (Google Images).
>
> Bing – wyszukiwarka od firmy Microsoft, umożliwiająca m.in. wyszukiwanie tekstowe oraz wyszukiwanie obrazem (tzw. wyszukiwanie wizualne).
>
> Yandex – rosyjski portal, będący od lutego 2024 roku w pełni w posiadaniu rosyjskich inwestorów (wcześniej był częścią holenderskiego Yandex N.V.), oferujący m.in. wyszukiwanie tekstowe oraz na podstawie obrazu. W tym drugim zakresie przez długi czas przewyższał swoich zachodnich rywali.

Zanim zagłębimy się w świat analizy zawartości obrazów przez silniki wyszukiwania, chciałbym zaznaczyć, że **badanie to nie obejmuje serwisu TinEye**. Pomijam go celowo, gdyż – mimo bardzo dobrych wyników w wyszukiwaniu obrazów – nie analizuje on ich zawartości, a jedynie sprawdza, czy konkretny obraz nie został umieszczony gdzieś w Internecie (na tyle, na ile oczywiście pozwalają mu na to jego bazy obrazów). **TinEye polecam zatem do wyszukiwania konkretnych zdjęć czy grafik np. w celu odnalezienia ich źródła**, a pod lupę po raz kolejny wezmę trzy najpopularniejsze serwisy: Google, Bing i Yandex. Do badania posłużą te same obrazy, które zostały wykorzystane za pierwszym razem, w celu weryfikacji, czy i w jakim stopniu zmieniły się wyniki wyszukiwania. Dodatkowo wykorzystamy także inne, nowe obrazy, aby upewnić się co do otrzymanego wyniku. Rezultaty poszukiwań poszczególnych wyszukiwarek zostaną porównane, aby zobaczyć, która z nich obecnie radzi sobie najlepiej i która zanotowała największy progres lub regres.

Zasada wyszukiwania za pomocą **Google Lens** jest taka sama jak w przypadku tradycyjnej wersji Grafiki Google – wskazujemy link do pliku graficznego, wybieramy plik z obrazem z dysku lub przeciągamy go do okna z otwartą wyszukiwarką Google (nawet z poziomu strony wyszukiwarki tekstowej, niekoniecznie zakładki: GRAFIKA) i upuszczamy we wskazanym polu, aby otrzymać wynik wyszukiwania. Jeśli chcemy skorzystać z tradycyjnej wersji wyszukiwania obrazem (a nie analizy jego zawartości przez Google Lens), musimy po wyszukaniu kliknąć przycisk ZNAJDŹ ŹRÓDŁO OBRAZU usytuowany nad przesłanym przez nas obrazem.

W poszczególnych kategoriach brane były pod uwagę następujące możliwości wyszukiwarek:

- identyfikacja miejsca na podstawie zdjęcia miasta,
- umiejętność odczytania tekstu w różnych językach na podstawie zdjęć zawierających napisy,
- rozpoznawanie marki i modelu na podstawie zdjęcia samochodu (w zakresie rzadko spotykanych marek samochodów osobowych oraz typowych busów),
- identyfikacja gatunków na podstawie zdjęć owoców,
- rozpoznawanie marek na zdjęciach zawierających logotypy,
- rozpoznawanie osób (wskazywanie imienia i nazwiska danej osoby) na zdjęciach, które zawierały twarze.

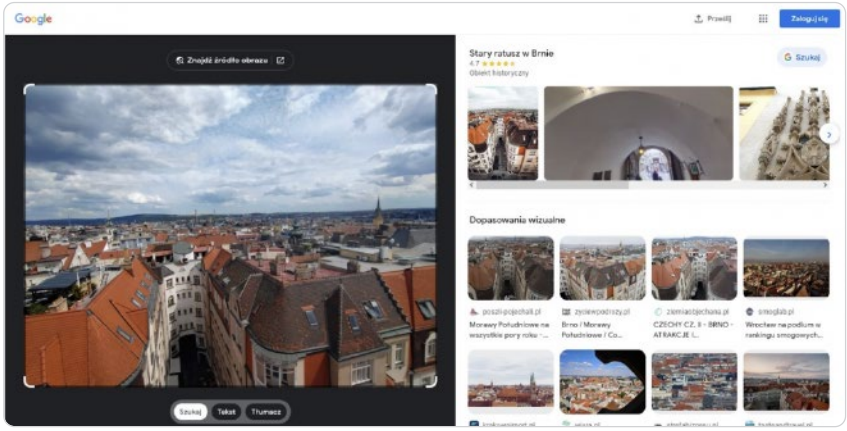
W ostatniej kategorii brane były pod uwagę także zdjęcia przedstawione w skali szarości oraz obrócone o 90 i 180 stopni.

Miejsca

Jako przykład zdjęcia miejsca w poprzednim badaniu posłużyła fotografia paryskiej Statuy Wolności. Wyszukiwarka Google była wówczas w stanie wskazać inne obrazy przedstawiające to miejsce, chociaż trzeba było się im przyjrzeć, aby nie popełnić błędu. Bing nie poradził sobie w ogóle, a Yandex odnalazł miejsce bezbłędnie.

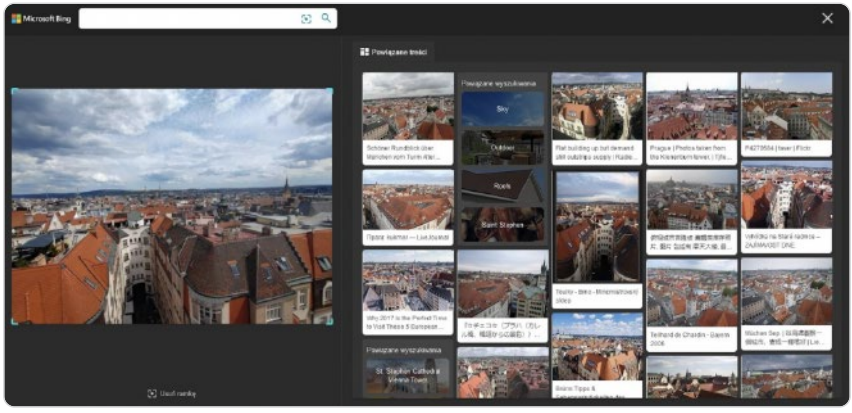
W 2023 roku **Grafika Google** (przy użyciu Google Lens) nie miała już najmniejszego problemu, aby rozpoznać, co znajduje się na zdjęciu, i wskazać od razu nazwę obiektu. W celu sprawdzenia, jak radzi sobie klasyczna wersja wyszukiwania graficznego od Google, kliknąłem w opisywany wcześniej przycisk ZNAJDŹ ŹRÓDŁO OBRAZU. Wśród wyszukanych wyników królowały linki do portalu *sekurak.pl* (ze względu na obecność tam zdjęcia zamieszczonego we wspomnianym już artykule *Jak wyszukiwarki radzą sobie…*, opisującym wzmiankowane na wstępie badanie, z 2021 roku), a zdjęcia podobne wizualnie pokazywały różne miasta nad wodą, jednak żadne z nich nie przypominało poszukiwanego paryskiego widoku.

Równie dobrze Google Lens poradziło sobie ze zdjęciem dachów kamienic na starówce w Brnie (rysunek 7): tutaj także bezbłędnie wskazane zostało miasto, a nawet konkretne miejsce wykonania zdjęcia.



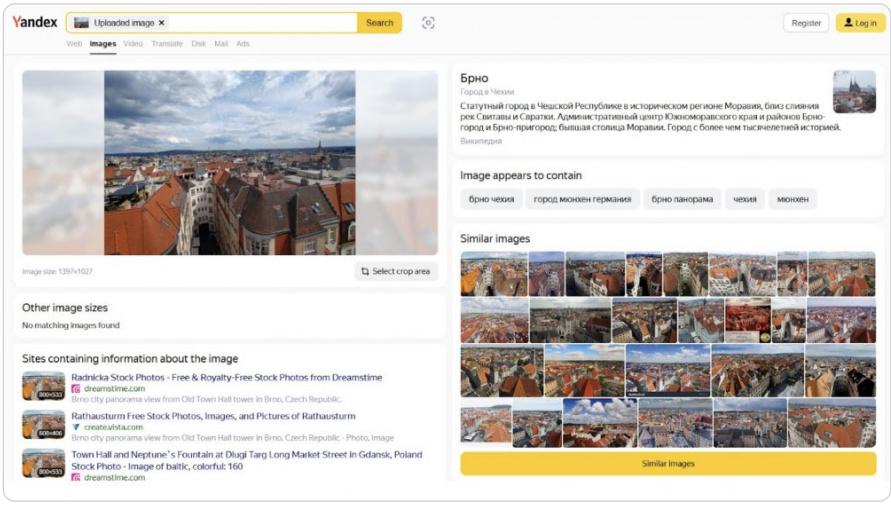
Rysunek 7. Wyszukiwanie w wyszukiwarce Google przy użyciu zdjęcia miasta

Bing (rysunek 8) poradził sobie lepiej niż poprzednio – tym razem wśród podobnych wizualnie obrazów znalazły się zdjęcia miejsc zgodnych z tym, co przedstawiają zdjęcia. Wyszukiwarka ta uzyskuje jednak lepsze wyniki, jeśli użyjemy opcji WYSZUKIWANIE WIZUALNE, dostępnej pod zdjęciem, które zostało przesłane. Mimo tego w przypadku zdjęcia brneńskiej starówki wyniki były zdecydowanie niezadowalające. Wśród wskazanych stron z obrazami znalazły się wprawdzie takie, które dotyczyły tego samego miasta, jednak na liście były także zdjęcia m.in. Monachium czy Pragi. Uzyskując takie wyniki, osoba poszukująca danej lokalizacji musi włożyć dodatkowy wysiłek w znalezienie poprawnych odpowiedzi, a nie zweryfikować jedynie otrzymane informacje.



Rysunek 8. Wyszukiwanie w Bing przy użyciu zdjęcia miasta

Yandex poradził sobie równie dobrze, jak Google – zidentyfikował miejsce łącznie z jego nazwą oraz pokazał zdjęcia poszukiwanego obiektu. W przypadku zdjęcia z Brna dodatkowo opis był dłuższy, jednak pomimo korzystania z anglojęzycznej wersji serwisu tekst był dostępny jedynie w cyrylicy, co może nieco utrudniać analizę osobom, które nie są obeznane z tego typu zapisem (rysunek 9), chociaż można zaznaczyć otrzymany opis i skopiować go do tłumacza *online* lub wykorzystać funkcje przeglądarki służące do tłumaczenia tekstów.



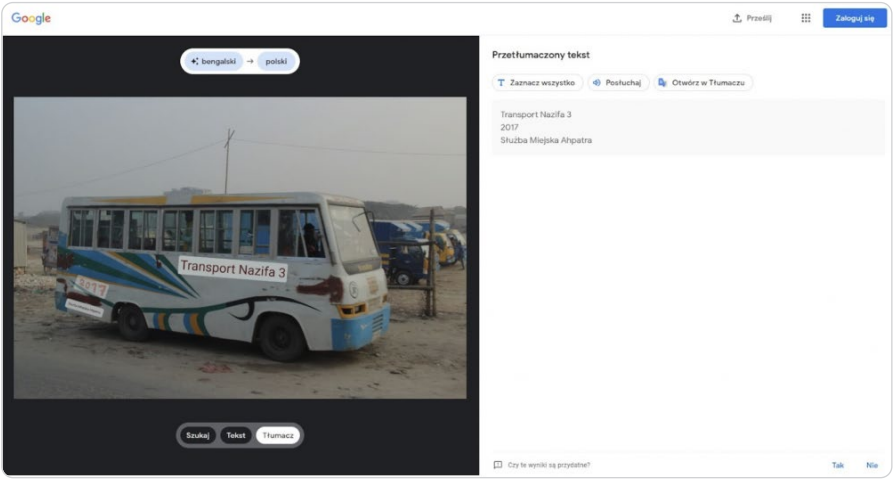
Rysunek 9. Wyszukiwanie w silniku Yandex przy użyciu zdjęcia miasta

Tekst

W analizie z 2021 roku rozpoznawanie tekstu badane było z wykorzystaniem zdjęcia tablicy informacyjnej zapisanej głównie tajskim alfabetem. Najlepiej poradził sobie wtedy Yandex, który był w stanie rozpoznać tekst i przetworzyć go tak, aby możliwe było jego skopiowanie i przetłumaczenie. Dość dobrze poradził sobie Bing, natomiast wyszukiwarka Google wypadła najsłabiej.

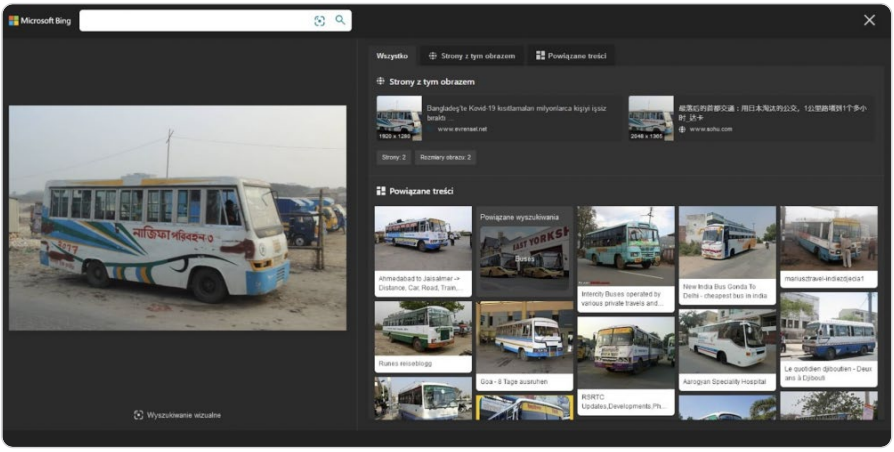
Tym razem **Google** nie miał już najmniejszych problemów z rozpoznaniem tekstu na zdjęciu. Jeśli obraz zawiera jakikolwiek tekst i chcemy go dalej przetwarzać (np. skopiować lub od razu przetłumaczyć), możemy skorzystać z przycisku TEKST znajdującego się poniżej przesłanego obrazu. Dodatkowo w przypadku badanego zdjęcia Google od razu wskazał, jakie to miejsce, dodając opinie i zdjęcia, jednak mogło to być głównie pokłosiem rozpoznanej nazwy, zapisanej w alfabecie łacińskim na zdjęciu. Niemniej skok jakościowy w tym przypadku jest naprawdę znaczny. W celu dodatkowej weryfikacji przeprowadziłem także test z rozpoznawaniem napisu w języku bengalskim (jako przykład dość rzadko spotykanego języka, rysunek 10) oraz umiejętnością odczytywania drogowskazów zapisanych pismem chińskim. W obu przypadkach

Google nie miał problemu z odczytaniem napisu, a dodatkowo dla drogowskazów od razu wskazywał dane miejsce na mapie lub wyświetlał wskazówki dotarcia do niego.



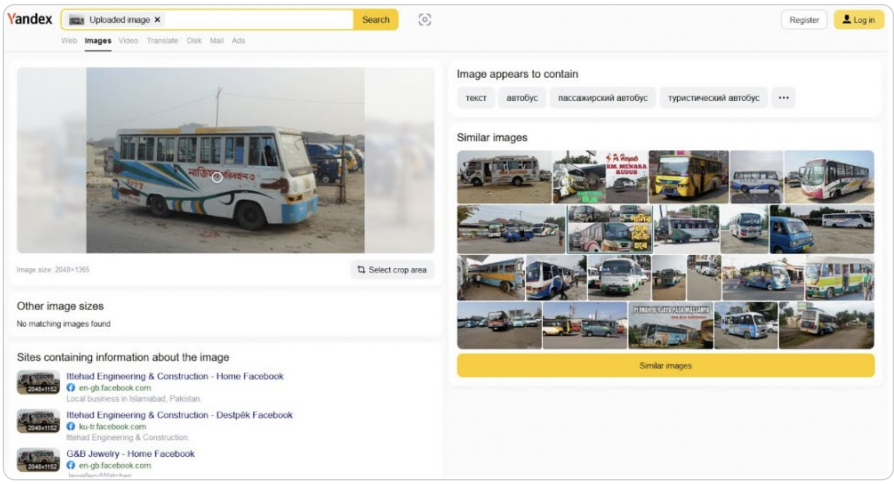
Rysunek 10. Analiza bengalskich napisów w wyszukiwarce Google

Bing, który dość dobrze radzi sobie z rozpoznawaniem tekstu w alfabecie łacińskim, niestety cały czas pozostaje w tyle, jeśli chodzi o inne systemy pisma. Biorąc pod uwagę postępy konkurencji, Microsoft powinien pomyśleć nad aktualizacją i rozwojem tej funkcji, tym bardziej że jej fundament ma już gotowy. Dla wskazanych zdjęć odnalezione zostały poprawnie ich wystąpienia na powiązanych stronach internetowych, co dało pewną wskazówkę odnośnie do poszukiwanej lokalizacji (rysunek 11). Tym razem Bing dostaje tylko mały plus.



Rysunek 11. Analiza bengalskich napisów w wyszukiwarce Bing

Dla wyszukiwarki **Yandex** alfabety inne niż łaciński nie stanowią zazwyczaj problemu. Dlaczego zazwyczaj? Otóż podczas badania odkryłem, że nie radzi sobie ona z alfabetem bengalskim (rysunek 12). Po dalszych dociekaniach okazało się, że wyszukiwarka ta ma problemy z wieloma systemami pisma z tego rejonu świata, ponieważ nie była w stanie rozpoznać także pisma dewanagari używanego w Indiach. To niestety zaniżyło jej ocenę w tym zestawieniu.



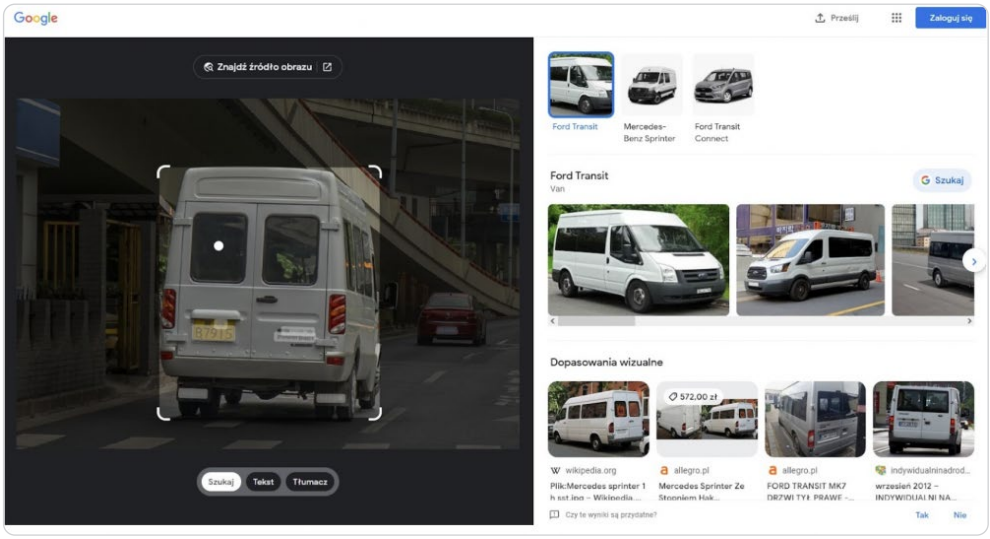
Rysunek 12. Analiza bengalskich napisów w wyszukiwarce Yandex

Samochody

W badaniu z 2021 roku z rozpoznawaniem samochodów najlepiej poradziły sobie wyszukiwarki Google i Yandex, a Bing pozostał w tyle. W tym zakresie wszystkie silniki wyszukiwania zanotowały duży progres i poprawiły swoje wyniki.

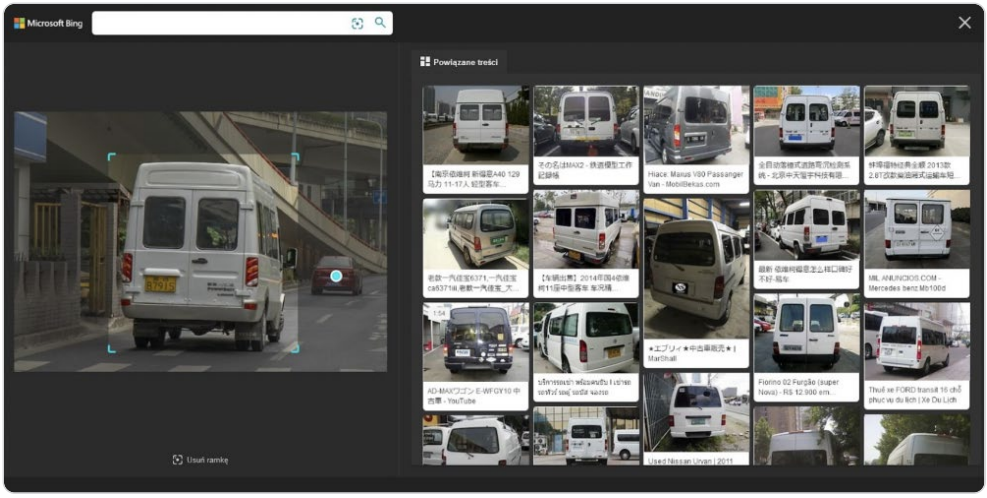
Zacznijmy standardowo od wyszukiwarki **Google**. Zdjęcie zawierające przód klasycznego samochodu zostało tym razem bezbłędnie rozpoznane, a dodatkowo w bocznym panelu wyświetliły się informacje dotyczące marki i modelu pojazdu wraz ze zdjęciami przedstawiającymi inne egzemplarze poszukiwanego samochodu. W celu dodatkowej weryfikacji umiejętności Google Lens zostały sprawdzone także na kilku innych egzemplarzach, m.in. na takich „klasykach", jak Fiat 126p, oraz na przykładzie innowacyjnej myśli brytyjskiej motoryzacji, jaki stanowi Bond Bug. W obu przypadkach wyszukiwarka nie miała problemu z rozpoznaniem marki i modelu oraz zaprezentowaniem informacji o nich. Kiedy już myślałem, że Google radzi sobie z rozpoznawaniem samochodów naprawdę dobrze, sprawdziłem jego mechanizmy na zdjęciu, na którym było widać tył busa Iveco Power Daily (rysunek 13). I tutaj niestety nastąpił moment rozczarowania, połączony z pewnym zdziwieniem, ponieważ pomimo odczytania marki na tylnych drzwiach wyszukiwarka podała, iż jest

to... Mercedes Sprinter albo Ford Transit (w zależności od kadrowania, gdyż ten zabieg potrafi zmienić wyniki, jakie otrzymamy).



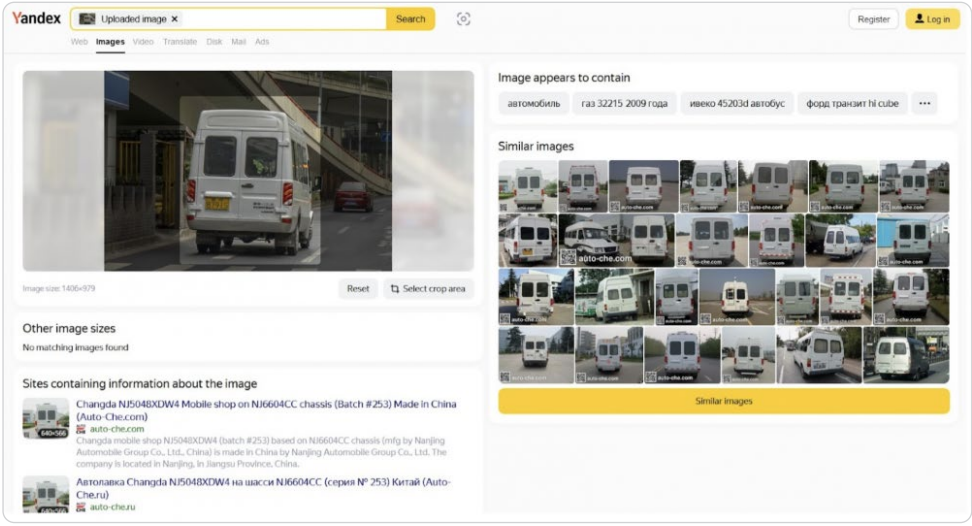
Rysunek 13. Analiza marki samochodu w wyszukiwarce Google

W wyszukiwarce **Bing** (rysunek 14) za każdym razem możliwe było odnalezienie na liście podobnych obrazów, linków do stron dotyczących danego modelu. Tylko w przypadku Fiata 126p jasno wskazane zostały marka i model. Rozpoznanie busa wyszło wyszukiwarce Microsoftu gorzej, gdy włączony został tryb wyszukiwania wizualnego, który teoretycznie powinien poprawić osiągane rezultaty.



Rysunek 14. Analiza marki samochodu w wyszukiwarce Bing

Yandex poradził sobie dość dobrze ze wszystkimi obrazami, poprawnie wskazując modele samochodów i dodatkowe informacje o nich, jednak, tak samo jak Google, poległ na przykładzie busa marki Iveco (rysunek 15). Co prawda wśród podobnych grafik znalazły się przykłady tego modelu, jednak w informacjach tekstowych na pierwszym miejscu Yandex wskazał, że może to być Gaz 32215 z 2009 roku, Iveco 45203d lub Ford Transit Hi Cube. Przy włączonym trybie wyszukiwania graficznego wyszukiwarka sugeruje, że na zdjęciu może znajdować się samochód dostawczy Mercedes.



Rysunek 15. Analiza marki samochodu w wyszukiwarce Yandex

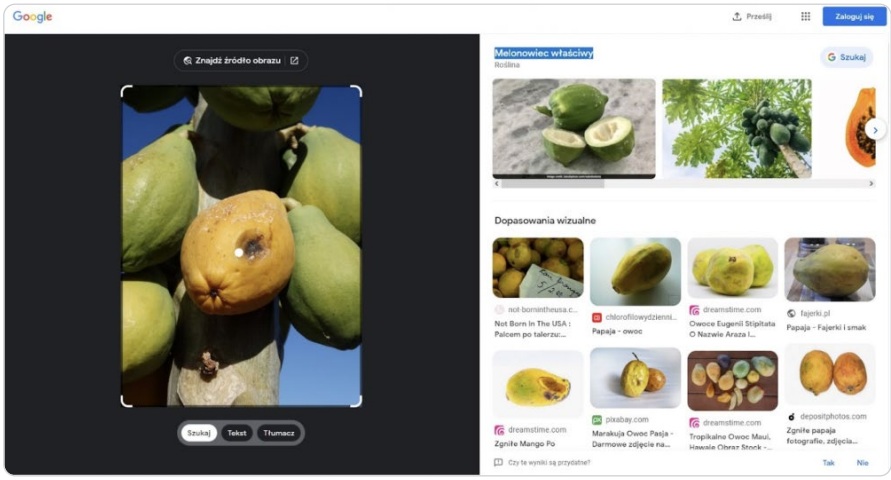
W związku z tym, że Bing nie wskazał konkretnego modelu samochodu dostawczego, nie pomylił się tak, jak Google czy Yandex. Być może takie podejście jest lepsze niż prezentowanie błędnej odpowiedzi przy niskim poziomie dopasowania?

Na pewno oznacza to, że nawet jeśli otrzymamy jakiś wynik podany „na tacy" przez wyszukiwarkę, powinniśmy go jeszcze zweryfikować, gdyż, jak widać, surowy efekt pracy samego narzędzia to jeszcze nie wszystko.

Owoce

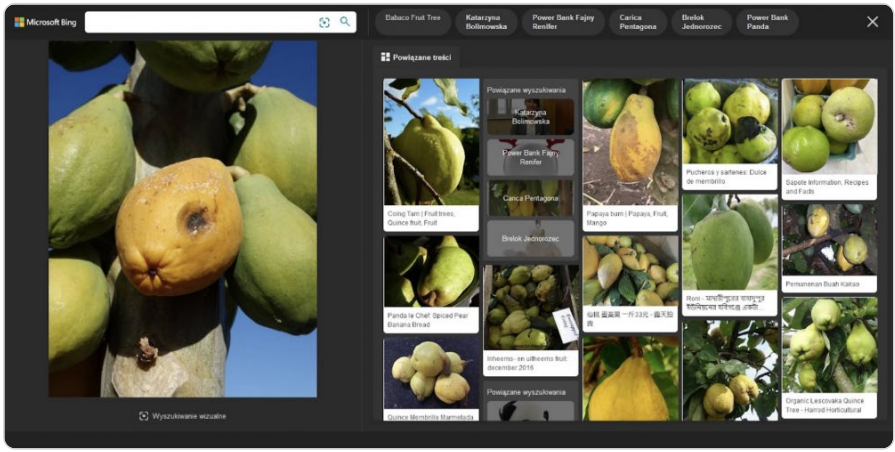
Zdjęcia owoców za pierwszym razem sprawiły trudność jedynie wyszukiwarce **Google**. Tym razem, tak jak i w innych punktach, wykorzystanie mechanizmów Google Lens znacznie poprawiło efektywność wyszukiwania, gdyż wskazane zostały nazwy owoców pokazanych na zdjęciach wraz z innymi przykładowymi zdjęciami danego owocu oraz (w niektórych przypadkach) nawet ich ceny. Wśród zbliżonych wizualnie obrazów znalazły się także inne, podobne owoce (rysunek 16), ale ze względu na fakt, że Google potrafi się mylić

co do obiektu przedstawionego na zdjęciu, może dobrze, że takie wyniki też się pojawiają.



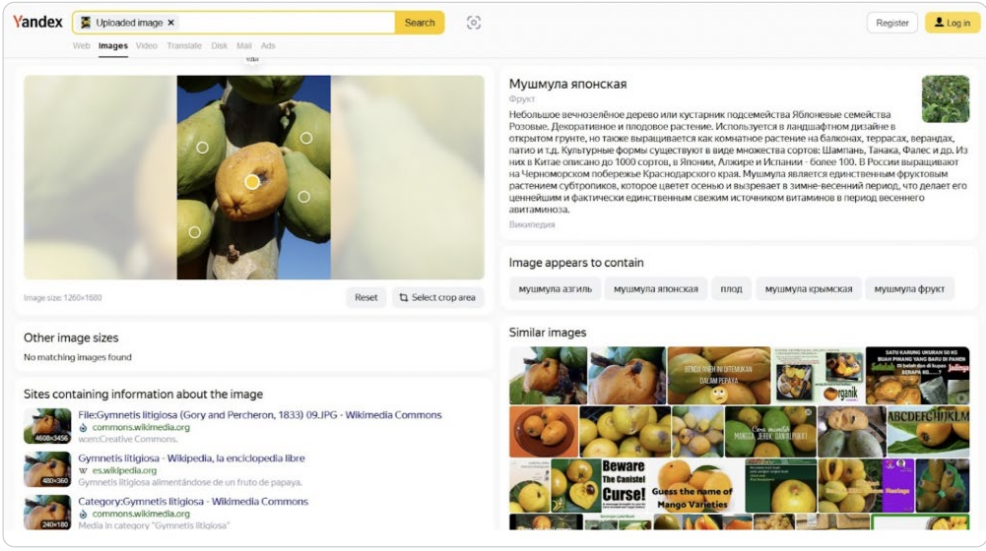
Rysunek 16. Rozpoznawanie owoców w wyszukiwarce Google

Dla **Bing** (rysunek 17) wyniki były niesatysfakcjonujące, np. w przypadku granatów powiązane strony zawierały poszukiwane owoce, a w dwóch przypadkach odnalezione zostały strony konkretnie ze zdjęciem, za pomocą którego wyszukiwano. Kiedy na zdjęciu znajdowała się papaja, wyniki nie były już takie dobre i Bing, oprócz jednego zdjęcia papai, wskazywał całą serię różnych owoców, podpowiadając przy okazji hasła takie jak: „babaco fruit tree" (blisko), „Power Bank Fajny Renifer" lub „Brelok jednorożec" (chyba dość daleko). Włączenie trybu wyszukiwania wizualnego praktycznie nic nie zmieniło.



Rysunek 17. Rozpoznawanie owoców w wyszukiwarce Bing

Yandex (rysunek 18) co prawda rozpoznał granaty, jednak nie wyświetlił w bocznym panelu informacji o tych owocach, a jedynie wskazał, że obrazy mogą je zawierać. W przypadku zdjęć papai taka szczegółowa informacja już została wyświetlona, jednak wystąpiła jedna zastanawiająca sytuacja. Wyszukiwarka Yandex dla rozpoznanych elementów obrazu wskazuje możliwość wyszukania informacji o nich. Niekiedy jest to informacja ogólna (np. budynek lub samochód), a niekiedy konkretne rodzaje przedmiotów (w tym przypadku był to konkretny owoc). Niestety, pomimo pierwotnego poprawnego rozpoznania owocu, kliknięcie w okrągły przycisk na samym zdjęciu, oznaczający wyszukiwanie informacji o danym obiekcie, przyniosło w efekcie wyświetlenie informacji o… nieśpliku japońskim. Szybka analiza wykazała wprawdzie pewne pokrewieństwo tej rośliny z papają, ale zbyt dalekie, by uznać wynik wyszukania za poprawny. Po raz kolejny więc doszło do sytuacji, kiedy wyszukiwarka dla tego samego zdjęcia wskazała różne wyniki.

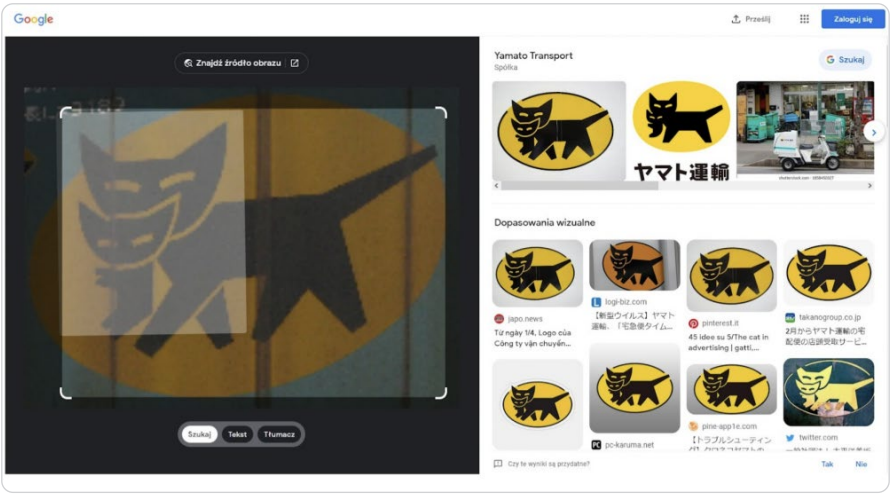


Rysunek 18. Rozpoznawanie owoców w wyszukiwarce Yandex

Logo

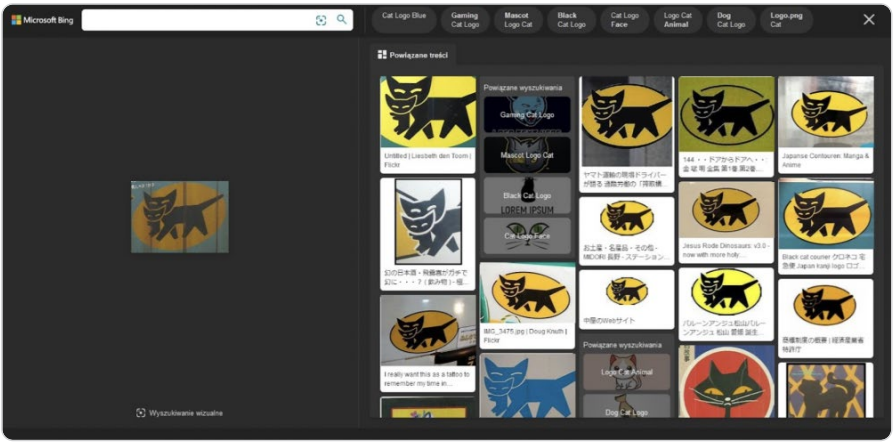
W rozpoznawaniu znaków graficznych znanych marek lub wydarzeń w poprzednim badaniu najgorzej zaprezentował się Bing, mający problemy z rozpoznawaniem tego typu obrazów. Google i Yandex wypadły podobnie do siebie i nieco lepiej od Binga.

W nowej odsłonie wyszukiwarka **Google** (rysunek 19) poradziła sobie najlepiej ze wszystkich. Bez problemu rozpoznała zarówno znak japońskiej firmy kurierskiej, igrzysk w Pekinie, jak i jednej z polskich cukierni (w formie z nazwą i bez niej). Nawet słaba jakość obrazu nie uniemożliwiła odczytania nazwy ze zdjęcia.



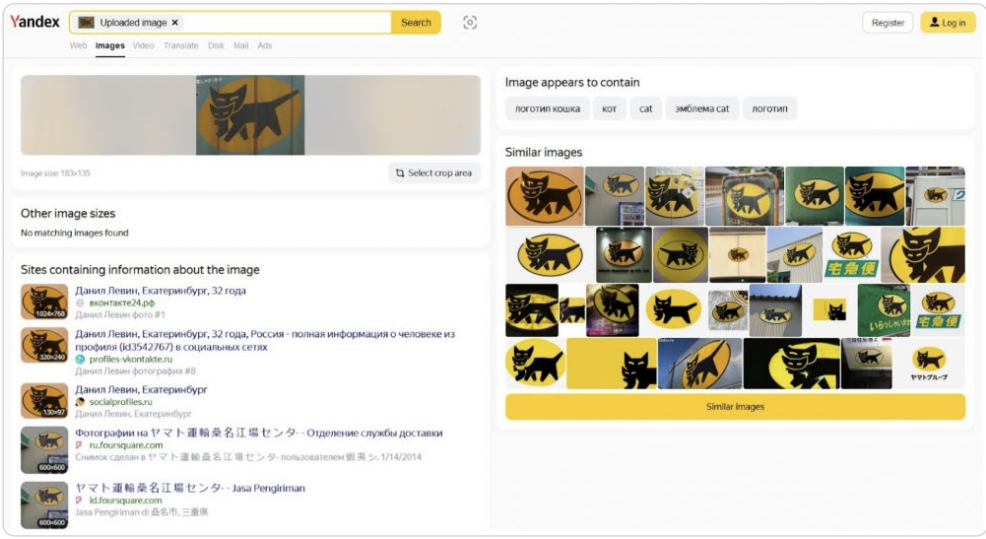
Rysunek 19. Rozpoznawanie logotypu w wyszukiwarce Google

Bing (rysunek 20) radził sobie dużo lepiej niż poprzednim razem, ale duża liczba błędnych wyników dla logo igrzysk, a także brak wyszukania powiązanych treści – nawet pomimo odczytania tekstu ze zdjęcia szyldu cukierni – sprawiły, że wynik tego badania w wykonaniu wyszukiwarki Microsoftu można uznać za niesatysfakcjonujący.



Rysunek 20. Rozpoznawanie logotypu w wyszukiwarce Bing

Dla wyszukiwarki **Yandex** (rysunek 21) nie stanowiło problemu odnalezienie stron z logo cukierni i igrzysk, ale w przypadku szyldu odczytanie napisu ją przerosło i nie była w stanie wskazać dobrego wyniku. Logo firmy kurierskiej zostało za to poprawnie dopasowane do innych obrazów z sieci.

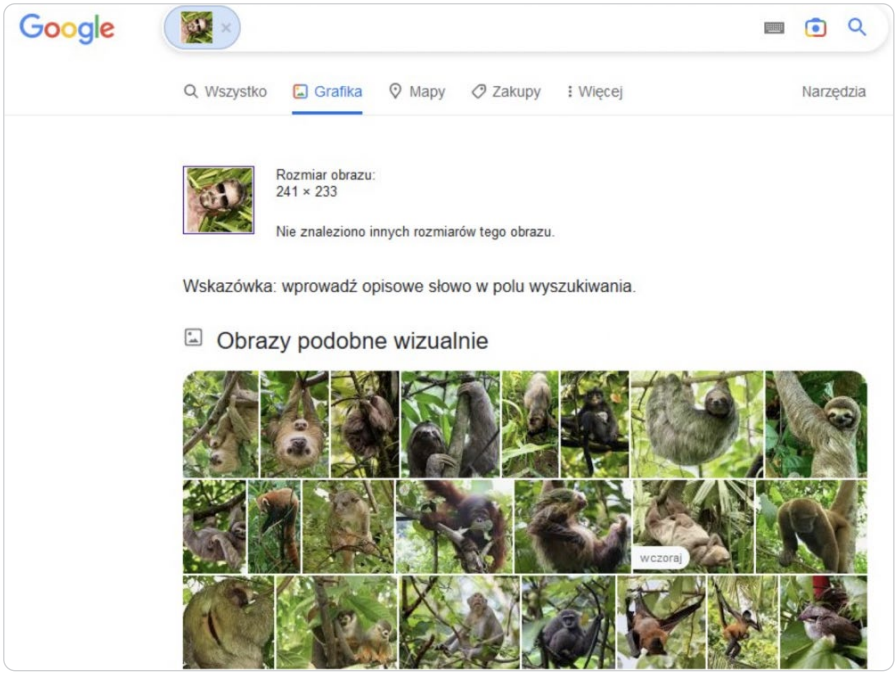


Rysunek 21. Rozpoznawanie logotypu w wyszukiwarce Yandex

Twarze

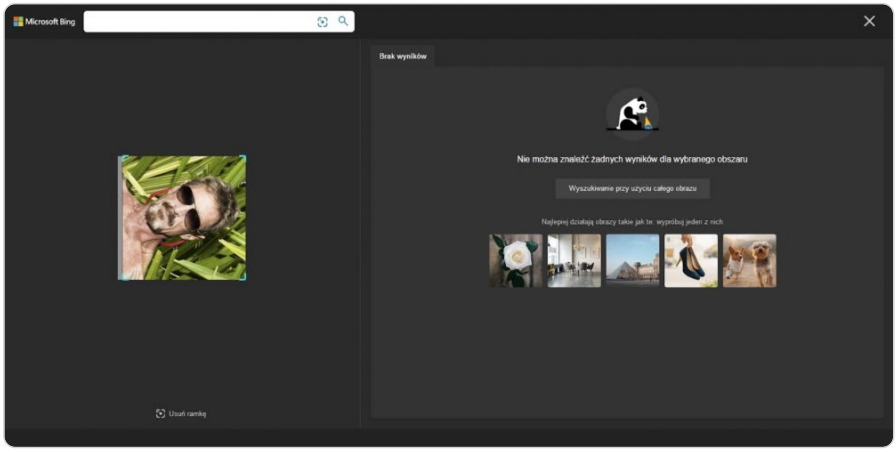
Ostatnim elementem badania było rozpoznawanie twarzy – i tutaj w badaniu z 2021 roku nastąpiło największe zaskoczenie, gdy Bing zwyciężył w tej kategorii, z dużą przewagą nad konkurencją.

Narzędzie **Google Lens** przyzwyczaiło użytkowników do dobrych wyników, jednak w zakresie rozpoznawania twarzy poległo. To zdecydowanie najsłabsza strona tego mechanizmu. Przy wyszukiwaniu zdjęciem Johna McAfee'ego przekonwertowanym do skali szarości Google Lens pochwaliło się, że znalazło na zdjęciu… okulary! Dopiero powrót do tradycyjnej **Grafiki Google** (Google Images) uratował honor tej wyszukiwarki, gdyż wskazana została prawidłowa osoba. Niestety, w przypadku obrócenia zdjęcia o 90 stopni było tylko gorzej – wyszukiwanie wizualne nadal twierdziło, że widzi tylko okulary, a tradycyjny silnik wyszukiwania tym razem zobaczył głównie… leniwce oraz różne gatunki małp i małpiatek (rysunek 22), a także pandę małą. Podobnie było z twarzami dwóch szwajcarskich skoczków narciarskich. Wizualnie byli oni (według wyszukiwarki Google) podobni do bluz sportowych, a Grafika Google nie mogła się zdecydować, czy na zdjęciu znajduje się ktoś z Uniwersytetu w Miami, czy piłkarz ręczny. Wyszukiwanie stockowego obrazu dziewczyny przyniosło zaskakująco mało wyników jak na tego typu grafikę.



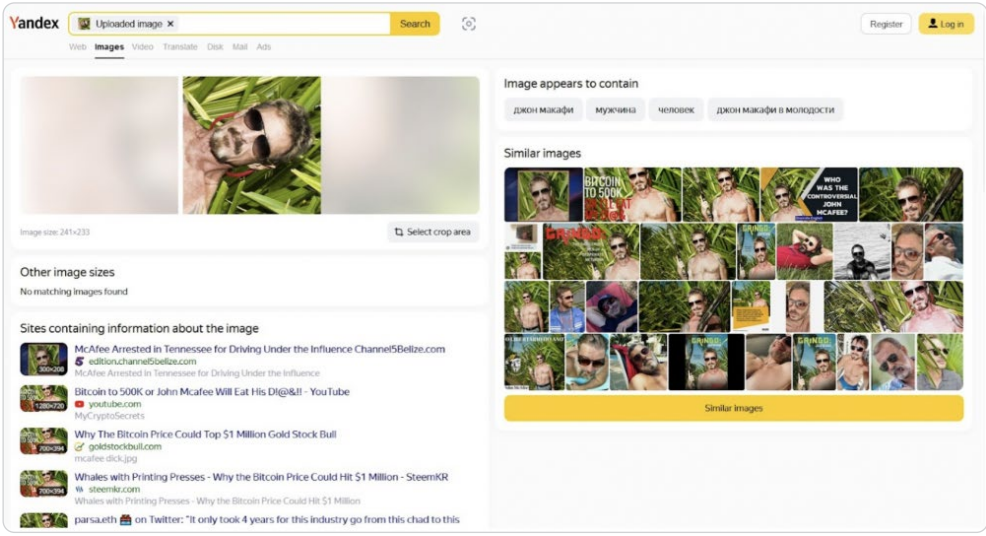
Rysunek 22. Rozpoznawanie twarzy w wyszukiwarce Google Grafika

Bing po raz kolejny dobrze poradził sobie z wizerunkami skoczków i jako jedyny wskazał z imienia i nazwiska, kto znajduje się na zdjęciu, a także rozpoznał, że na obrazie w skali szarości widnieje John McAfee (rysunek 23). Co do stockowego zdjęcia dziewczyny: wskazał więcej stron z wyszukiwaną grafiką niż Google. Najgorzej jednak wypadło wyszukiwanie zdjęciem obróconym o 90 stopni – tutaj wyszukiwarka się poddała i nie wskazała żadnych wyników.



Rysunek 23. Rozpoznawanie twarzy w wyszukiwarce Bing

Yandex nie rozpoznał wprawdzie żadnego ze skoczków, wskazując w obu przypadkach, że na zdjęciu mogą znajdować się osoby o nazwisku Schumacher, jednak był w stanie wyszukać dużą liczbę powiązanych stron, na których wykorzystano stockowe zdjęcie dziewczyny. Także wyszukiwanie zdjęciem Johna McAfee'ego, zarówno w skali szarości, jak i w przypadku obrócenia go o 90 stopni, dało poprawny wynik. Z tym ostatnim zadaniem Yandex poradził sobie jako jedyny (rysunek 24).



Rysunek 24. Rozpoznawanie twarzy w wyszukiwarce Yandex

W zakresie rozpoznawania twarzy dużo bardziej skuteczne będą chociażby takie narzędzia, jak PimEyes czy search4faces, tym bardziej jeśli np. zostaną użyte w połączeniu z narzędziami AI do postarzania twarzy, jak można było to zobaczyć w przypadku osób poszukiwanych od 30 lat w Niemczech[4].

Podsumowanie i rady

Aby podsumować badanie i przedstawić graficznie, jak duże zmiany zaszły w popularnych wyszukiwarkach graficznych w ciągu niemal dwóch lat, musiałem nieco zmienić skalę ocen.

Za pierwszym razem brak umiejętności poprawnego wyszukania oznaczałem znakiem minus (–), poprawne wyszukanie – znakiem plus (+), a wyszukanie pełne, ze wskazaniem szczegółów, oznaczone było podwójnym plusem (++).

Tym razem, aby zwiększyć gradację, posłużyłem się skalą od 1 do 5, przy czym 1 oznacza brak umiejętności wyszukania, 3 – poprawne wyszukanie, a 5 – informację pełną, podaną ze szczegółami. Nie jest to rozwiązanie idealne, ale pozwala odnieść wyniki z 2023 roku do tych z 2021 roku (tabela 1).

Tabela 1. Różnice w wynikach działania wyszukiwarek pomiędzy badaniami z 2021 i 2023 roku

	GOOGLE			BING			YANDEX		
	2021	2023	ZMIANA	2021	2023	ZMIANA	2021	2023	ZMIANA
Miejsca	3	5	+2	1	3	+2	3	5	+2
Tekst	1	5	+4	3	2	-1	5	4	-1
Samochody	3	4	+1	1	3	+2	5	4	-1
Owoce	1	5	+4	3	3	0	3	4	+1
Logo	3	4	+1	1	3	+2	3	3	0
Twarze	1	2	+1	5	4	-1	3	4	+1
Suma	**12**	**25**	**+13**	**14**	**18**	**+4**	**22**	**24**	**+2**

Podsumowując wyszukiwanie za pomocą obrazów przy użyciu omawianych tu wyszukiwarek, warto przytoczyć ranking porównawczy wyszukiwarek oferujących funkcję wyszukiwania na podstawie zawartości obrazu (ang. *reverse image search*) (rysunek 25).

Rysunek 25. Ranking porównawczy wyszukiwarek oferujących funkcję *reverse image search* (im więcej kropek, tym lepszy wynik). Materiały własne

Jak widać, wdrożenie mechanizmów Google Lens do wyszukiwarki grafiki Google było dobrą decyzją. Dzięki tym usprawnieniom wyszukiwarka Google z ostatniego miejsca w poprzedniej klasyfikacji przeskoczyła na pierwsze. Nie jest to oczywiście rozwiązanie idealne, gdyż istnieje jeszcze sporo obszarów do poprawy, np. w zakresie rozpoznawania osób, ale skok jakości wyszukiwania jest naprawdę znaczący. W tyle została wyszukiwarka Bing, która cały czas najlepiej radzi sobie z rozpoznawaniem twarzy, jednak pozostałe wyniki są co najwyżej zadowalające lub średnie (ocena 4 lub 3). Yandex w stosunku do 2021 roku stracił najwięcej. Tracąc pozycję wiodącej wyszukiwarki graficznej, pozostał nadal do-

brym narzędziem, ale mającym pewne niedociągnięcia. **Przy wyszukiwaniu wizualnym, gdzie mamy możliwość zmiany wielkości obszaru zdjęcia, które jest analizowane, warto sprawdzić, jakie inne wyniki zostaną wyświetlone dla różnych ustawień**. Czasami nawet niewielka zmiana w tym zakresie może mieć duży wpływ na zwracane wyniki. Warto też w tym przypadku zapisywać interesujące nas zestawy wyszukanych danych (np. poprzez zapisanie linku do wyników aktualnego wyszukiwania lub wykorzystanie innego narzędzia, które zapisze dostępne na stronie odnośniki), gdyż z doświadczenia mogę powiedzieć, że niekiedy naprawdę trudno jest tak zmienić obszar zaznaczenia, aby trafić w wyniki, które jeszcze przed chwilą udało nam się uzyskać.

Należy mieć na uwadze fakt, że mechanizmy wyszukiwania są cały czas poprawiane – i już niedługo powyższa klasyfikacja może znowu się zmienić. Przy każdym wyszukiwaniu jednak konieczne jest sprawdzenie i analiza wyników, gdyż ślepe zawierzenie narzędziom, nawet tym najlepszym, może skończyć się ogromną pomyłką. O weryfikacji otrzymywanych informacji piszę więcej w rozdziale: *OSINT^2, czyli kilka słów o weryfikacji danych* (s. 100–105).

R3 PASYWNY REKONESANS KONT GOOGLE I MICROSOFT

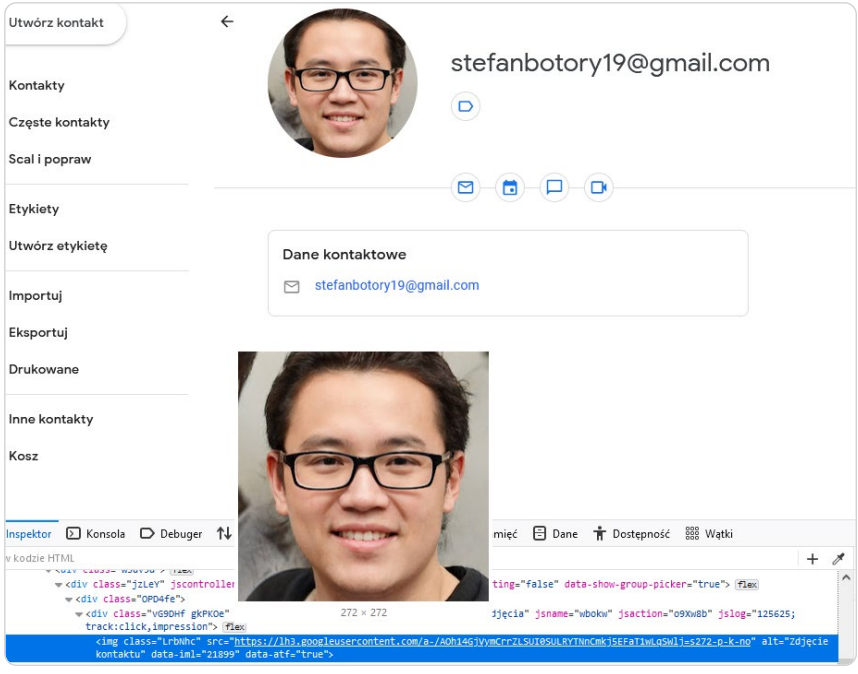
Jedną z szybkich i efektywnych technik rekonesansu OSINT-owego jest zdobywanie szczegółowych informacji o osobie i jej zdjęciu profilowym na podstawie adresu e-mail. Jeśli jest to konto Google, można skorzystać z takich narzędzi, jak te opisywane w rozdziale: *GHunt, czyli jak wycisnąć jak najwięcej informacji z profilu Google* (s. 149–151). Można też użyć narzędzia, którego nie trzeba instalować, czyli wyszukiwarki informacji o koncie Google na stronie Epieos. Problem z narzędziami jest jednak taki, że nie zawsze działają lub przechodzą na model płatnej subskrypcji. Niekiedy łatwiej (i szybciej) można zdobyć większą wiedzę o właścicielu konta po skorzystaniu z funkcjonalności serwisów Google czy Microsoft. W tym rozdziale chcę przybliżyć temat zdjęć profilowych, które mogą posłużyć do dalszej analizy, np. z wykorzystaniem wyszukiwania obrazem (co zostało omówione również w poprzednim rozdziale), a także temat identyfikatorów kont Google.

Google

Każdy użytkownik konta Google może przypisać do swojego konta zdjęcie profilowe. Nie jest to niczym nadzwyczajnym. Ale nie wszystkie serwisy tak chętnie jak Google dzielą się zdjęciami profilowymi podczas rekonesansu pasywnego, tzn. bez jakiejkolwiek interakcji z badanym obiektem.

Zdjęcie profilowe z konta Google można odnaleźć na wiele różnych sposobów. Pierwszym z nich może być **dodanie osoby o znanym adresie e-mail**

do kontaktów swojego konta Google. Wystarczy przy tworzeniu nowego kontaktu wpisać ten adres poczty elektronicznej, a Google automatycznie pokaże, jaki awatar ten konkretny użytkownik przypisał do swojego konta. W celu analizy grupy osób (adresów) można zaimportować kontakty do konta i w ten sposób uzyskać zestawienie wszystkich zdjęć profilowych. Aby wyodrębnić samo zdjęcie w nieco lepszej rozdzielczości, musimy już zagłębić się w kod strony. Przydatne do osiągnięcia tego celu będą narzędzia deweloperskie wbudowane w przeglądarki. Wystarczy kliknąć prawym przyciskiem myszy na zdjęciu wyświetlonego kontaktu i wybrać opcję ZBADAJ (lub WYKONAJ INSPEKCJĘ w MS Edge). To uwidoczni tag `img` z adresem, pod jakim można pobrać zdjęcie profilowe. Po skopiowaniu adresu z kodu strony można np. wkleić go do kolejnej karty w przeglądarce. W wypadku zdjęć profilowych kont Google adres takiego zdjęcia będzie zaczynał się od *https://lh3.googleusercontent.com* (przy czym nie musi to być *lh3*, może tam być też inna cyfra), jak to widać na rysunku 26. Jedyna dostępna tu rozdzielczość to 272 × 272 piksele. Niedużo jak na zdjęcie, jednak w końcówce adresu widać coś, co może pomóc uzyskać nieco większą rozdzielczość, a mianowicie *s272*. Zgodnie z informacją o konstrukcji adresów[5] zdjęć profilowych kont Google „s" oznacza parametr wielkości dłuższego boku obrazka (w pikselach), więc zmiana wartości stojącej za tą literą spowoduje wyświetlenie obrazu o wyższej rozdzielczości. Jeśli podamy zbyt dużą wartość, otrzymamy obraz w takiej rozdzielczości, jaką oryginalnie posiadał ten obrazek.

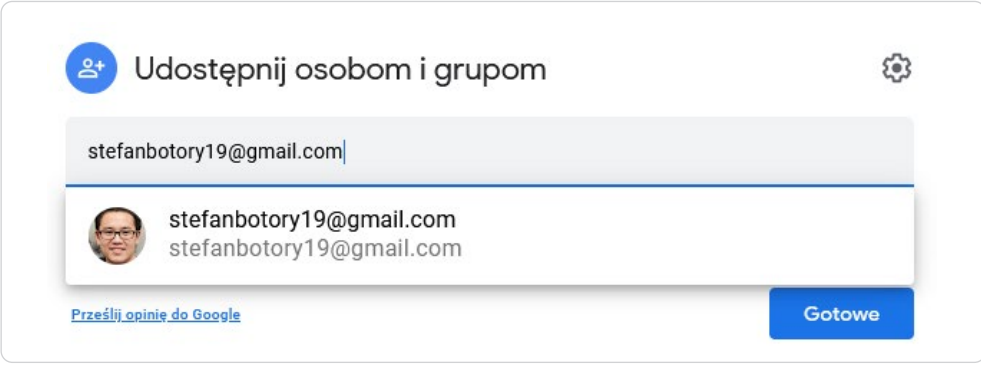


Rysunek 26. Istnieje wiele metod pozyskiwania zdjęć profilowych kont Google

Jednak nie tylko obraz jesteśmy w stanie pozyskać, zaglądając w kod strony. Wyszukując w nim adres e-mail poszukiwanej osoby, trafimy w pewnym momencie na zbiór różnych danych z nią związanych, a zebranych w jednym ze skryptów (umieszczonych w tagu `<script>`). Najistotniejszą z informacji tam zawartych jest **identyfikator konta**, który może być później wykorzystany do uzyskania kolejnych danych o osobie. Jest to ciąg cyfr rozpoczynający się zazwyczaj od 10 lub 11. Na jego podstawie możemy np. uzyskać dostęp do opinii pozostawionych przez daną osobę na mapach Google. Wystarczy w tym celu skonstruować link według następującej reguły: `https://www.google.com/maps/contrib/ID_KONTA/reviews` – i zobaczyć, czy i gdzie dana osoba zostawiła opinie.

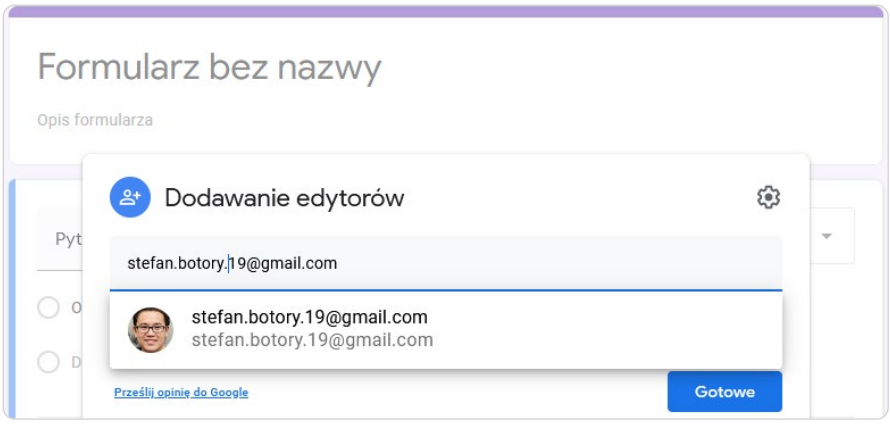
Metod na wykorzystanie identyfikatora konta Google jest więcej. Wystarczy przywołać opisane przez użytkownika Sector035[6] łączenie osoby z jej kontem na YouTube.

Kolejnym ze sposobów na uzyskanie zdjęcia profilowego jest udostępnianie dokumentów Google (rysunek 27). Wpisanie adresu e-mailowego w oknie udostępniania spowoduje ukazanie się podpowiedzi z awatarem przypisanym do konta o podanym adresie. Oczywiście, nie należy udostępniać dokumentu tej osobie (po analizie najlepiej usunąć wpisany adres), aby nie powiadomić jej o fakcie poszukiwania informacji na jej temat.



Rysunek 27. Uakatywnienie mechanizmu podpowiedzi podczas udostępniania dokumentów Google

Ten sposób jest uniwersalny dla różnych serwisów Google i możemy go użyć także w Formularzach Google (rysunek 28).



Rysunek 28. Podpowiedzi podczas udostępniania dokumentów Google w Formularzach Google

Ten sam mechanizm działa w czasie dodawania osoby do czatów Google Chat (ale ciągle bez wysyłania jakiejkolwiek informacji do właściciela konta, aby rekonesans pozostał pasywny – rysunek 29) – bez problemu uzyskujemy dostęp do podglądu zdjęcia profilowego. Jak widać na rysunku 28, Google nie zwraca uwagi na to, w jakich miejscach stawiamy kropki w loginie konta.

Rysunek 29. Mechanizm podpowiadania działa również w czasie dodawania osoby do czatów

UWAGA

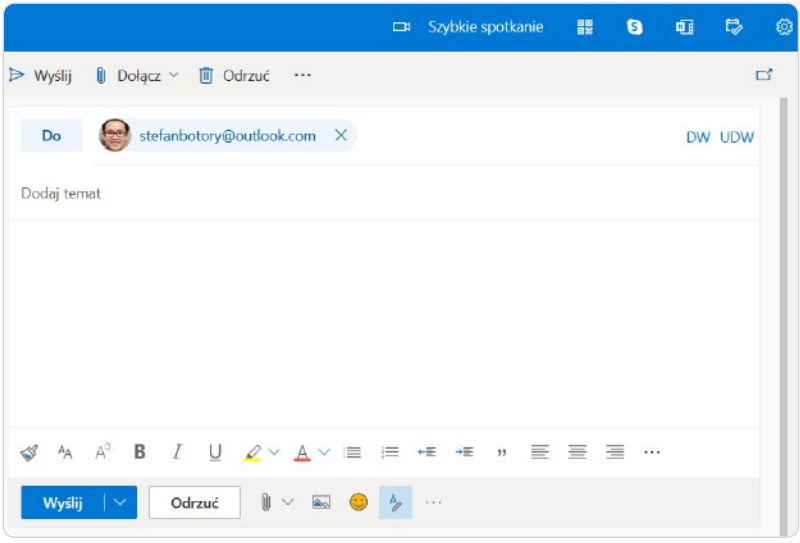
Aby takie poszukiwania były owocne, analizowany adres e-mail nie musi znajdować się w domenie *gmail.com*. Może to być dowolny adres poczty elektronicznej, wystarczy, że został przypisany do konta Google, które ma uzupełnione takie informacje, jak zdjęcie profilowe.

Punktem wyjścia nie musi być adres e-mail, a np. numer telefonu. Jednak w tym przypadku dużo łatwiejsze wydaje się wyszukanie numeru bezpośrednio w wyszukiwarce Google, co da dostęp do pełnego profilu, jeśli jest to konto firmowe z (co ważne) udostępnionym numerem telefonu.

Microsoft

A jeśli analizowany adres poczty elektronicznej nie jest adresem powiązanym z kontem Google, tylko z jego microsoftowym odpowiednikiem, czyli adresem w domenie *outlook.com*? W tym przypadku Microsoft również pozwala na podejrzenie zdjęcia profilowego w podobny, choć nieco uboższy niż w przypadku Google, sposób.

Możemy zobaczyć zdjęcie profilowe podczas dodawania adresatów e-maila (oczywiście bez jego wysyłania) lub osób do wydarzenia w Kalendarzu (rysunek 30). W wypadku Microsoftu mają już jednak znaczenie liczba i umiejscowienie kropek w loginie, tzn. nie możemy ich wstawiać w dowolne miejsca jak w przypadku Google.



Rysunek 30. Microsoft również pozwala na podejrzenie zdjęcia profilowego użytkownika

Gravatar

Jeśli punktem wyjścia w czasie rekonesansu pasywnego jest adres e-mail, możemy również skorzystać z usługi Gravatar, która dla zarejestrowanego w niej adresu e-mailowego pozwala dodać zdjęcie profilowe, wyświetlane następnie w wielu serwisach w sieci (np. takich jak: Slack, GitHub, a także… sekurak). Adres zdjęcia profilowego to po prostu:
`https://www.gravatar.com/avatar/SKRÓT_MD5_ADRESU_EMAIL`

Hash MD5 dla danego adresu można liczyć osobno, jednak na stronie Gravatara istnieje specjalna formatka Email Checker do weryfikacji, jaki obraz został przypisany (o ile został) do konkretnego adresu e-mail.

Podsumowanie i rady

To tylko niektóre z przykładów uzyskiwania zdjęć profilowych osób metodami OSINT-owymi. Chciałem pokazać, w jaki sposób różne firmy (a raczej: my sami) udostępniają bez naszej wiedzy informacje o nas każdemu, kto o nie zapyta. Oczywiście, wrzucając swoje zdjęcie na „profilówkę" do Internetu, musimy pogodzić się z faktem, że tak naprawdę staje się ono publicznie dostępne. Wiele osób jest tego świadomych i jest dla nich czymś naturalnym, że każdy może zobaczyć ich awatar w różnych serwisach. W dobie coraz większego i świadomego dążenia do ochrony prywatności warto jednak wiedzieć, kto i kiedy może to zrobić.

R4 ĆWIERKAJĄC W CZASIE I PRZESTRZENI, CZYLI ANALIZA GEOLOKALIZACJI WPISÓW NA TWITTERZE/X

W tym rozdziale chciałbym skupić się na wpisach twitterowych pod kątem zawartych w nich metadanych. Nie mam tutaj na myśli uzyskiwania geolokalizacji na podstawie danych EXIF ze zdjęć, bo te są automatycznie usuwane przed ich opublikowaniem. Przedmiotem mojego zainteresowania jest **obserwowanie lokalizacji dodawanej do tweetów** (lub jakkolwiek określa się aktualnie wpisy na portalu X) oraz czasu, kiedy te są zamieszczane w sieci.

Domyślnie w kontach na Twitterze/X* dodawanie lokalizacji do wpisów jest wyłączone, więc teoretycznie wszystkie posty są jej pozbawione. Jeśli opcja zostanie włączona, każdy wpis będzie niósł ze sobą informację o miejscu, w którym był jego autor w momencie publikowania go.

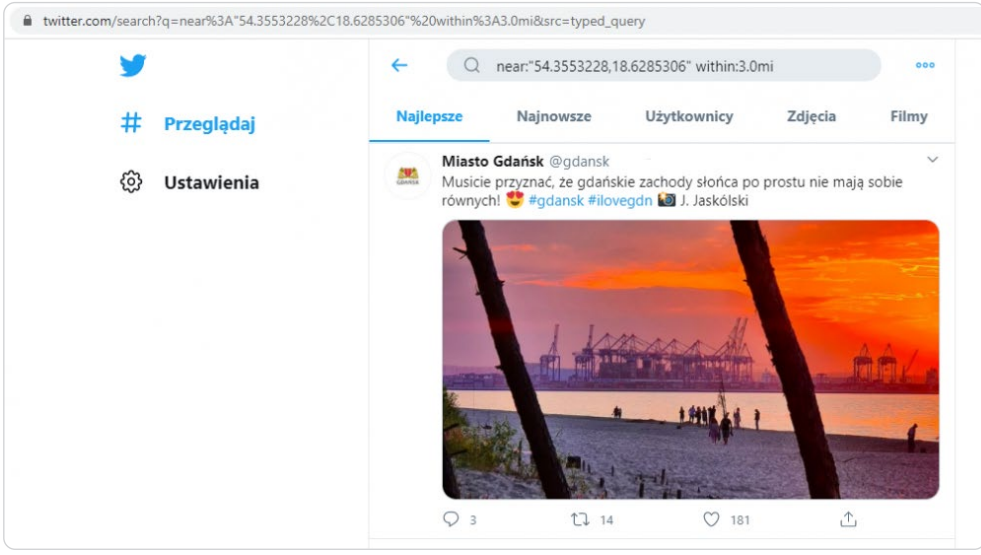
Twitter/X może pozyskiwać dane o lokalizacji z trzech miejsc (rysunek 31):

1. aktualnego położenia publikującego,
2. przybliżonej lokalizacji na podstawie nazw użytych w tekście,
3. lokalizacji z opisu bio autora.

Takie metadane umożliwiają np. weryfikację, czy informacje, którymi dzieli się dana osoba, nie są nieprawdziwe (jak wpis *Wakacje na Majorce* z lokalizacją w Chałupach), czy też w jakich miejscach ona bywa. Takie dane mogą też powiedzieć więcej o kontekście wypowiedzi – przykładowo osoba pisząca

* Będę tutaj stosował to nazewnictwo, żeby wszyscy mieli świadomość, o jakim portalu mowa. Wskazanie Twittera na pierwszym miejscu oznacza, że omawiam mechanizm, który został zaprojektowany i wdrożony na tej platformie jeszcze przed połową 2023 roku i działa w niej nadal do czasu publikacji tej książki.

negatywne opinie o lekarzu bez wymieniania nazwiska czy placówki, ale oznaczająca swój wpis geolokalizacją, zdradza mimowolnie informację, kogo ma na myśli.



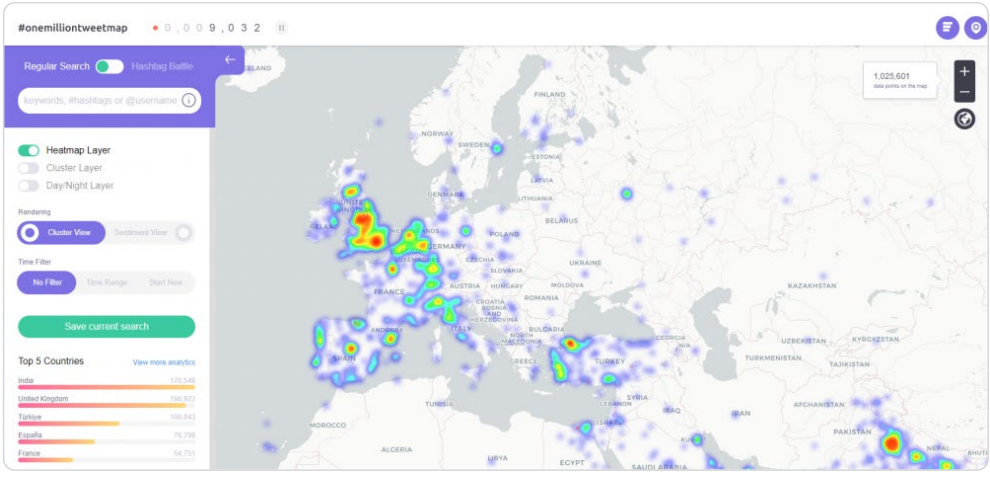
Rysunek 31. Przykład wyszukiwania tweetów z okolic gdańskiego Neptuna

Twitter/X sam w sobie udostępnia możliwość wyszukiwania wpisów z danej lokalizacji i jej okolic. Do tego służy operator `geocode:`, po którym podajemy dane w formacie: `latitude,longitude,radius`, czyli kolejno: szerokość i długość geograficzną w formie dziesiętnej (a nie w stopniach, minutach i sekundach) oraz promień. Wpisanie `geocode:50.0530183,19.9313958,1km` pokaże nam wszystkie wpisy z okolicy jednego kilometra od rzeźby Smoka Wawelskiego w Krakowie. Taki sam efekt przyniesie użycie operatora `near:` w połączeniu z `within:`, gdzie po „near" musimy podać albo koordynaty w cudzysłowie, albo nazwę miasta, a po „within" opcjonalnie podajemy promień wyszukiwania w kilometrach lub milach. Koordynaty – szerokość i długość geograficzną – można łatwo skopiować z adresu URL na stronie map Google, który w adresie URL stosuje także zapis dziesiętny tych wartości, po znalezieniu tam poszukiwanego miejsca (to dwie pierwsze wartości po znaku `@`, trzecia to zoom map Google, do pominięcia w tym przypadku). Przykładowy adres URL z Google Maps (z wyróżnionymi koordynatami) wygląda następująco:
`https://www.google.pl/maps/@50.0530183,19.9313958,17z?entry=ttu`

Jeśli mamy włączoną lokalizację urządzenia, to najprostszym sposobem na znalezienie wpisów w naszej okolicy jest wpisanie zwrotu `near:me` w polu wyszukiwania.

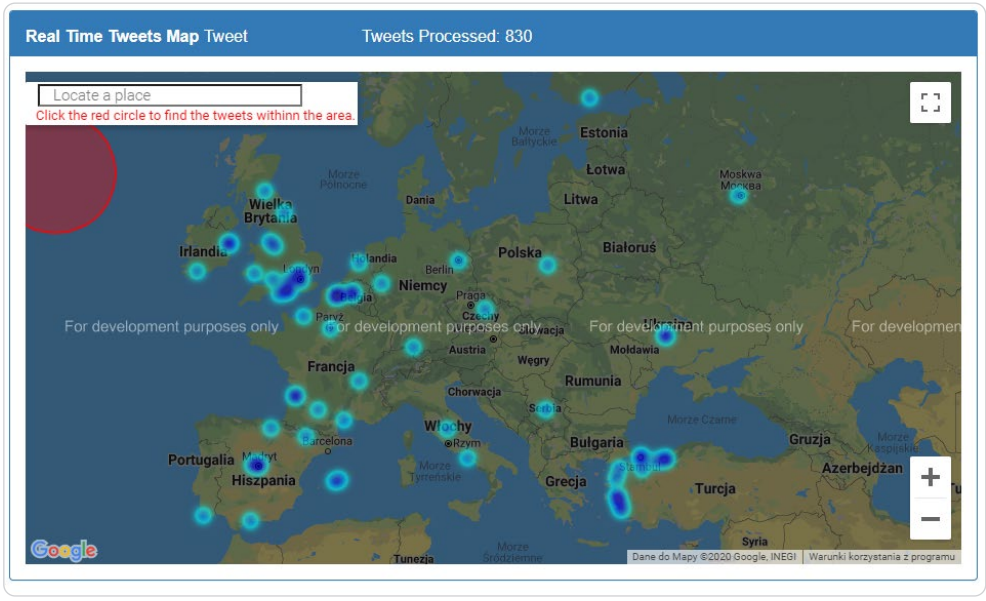
Narzędzia dostępne w sieci

Jeśli chcemy skorzystać z narzędzi dostępnych w sieci, warto spojrzeć na wersję demonstracyjną usług reprezentacji *big data* na mapach, która (jak na demo) daje pewne możliwości filtrowania. Jest to *onemilliontweetmap*. Mamy tu możliwość przeszukania bazy wpisów z ostatnich 24 godzin, co daje (wbrew nazwie) około dwa miliony pozycji. Baza jest aktualizowana na bieżąco, więc co chwila jesteśmy bombardowani efektownymi animacjami czerwonych okręgów pokazujących lokalizację nowych wpisów. Filtry pozwalają na wyświetlenie tylko określonych hashtagów, autorów lub ograniczenie jeszcze bardziej okna czasowego. Dla lubiących ciekawostki jest też możliwość włączenia widoku analizy wpisów pod kątem zawartości słów pozytywnych lub negatywnych (*sentiment view*), a także „walki hashtagów", gdzie możemy podać dwa tagi i zobaczyć, który z nich jest aktualnie popularniejszy. Rysunek 32 zawiera mapę pokazującą aktualne miejsca, z których wysyłane są wpisy z geolokalizacją w Europie.



Rysunek 32. Mapa pokazująca aktualne miejsca, z których wysyłane są tweety z geolokalizacją w Europie (za: onemilliontweetmap.com)

Innym użytecznym portalem może być Tweeplers, z którego można przejść do Twittera/X, wyszukując wpisy w okolicy kliknięte miejsca (rysunek 33). Niestety, strona ta nie oferuje już możliwości zobaczenia mapy ciepła (ang. *heatmap*) z wyświetlanymi na żywo wpisami w konkretnych lokalizacjach.



Rysunek 33. Tweeplers jeszcze niedawno pokazywał mapę wpisów. Obecnie może służyć już tylko do wyszukiwania z kliknięte lokalizacji

Podsumowanie

Od czasu przejęcia Twittera przez Elona Muska i przemianowania go na portal o enigmatycznej nazwie X, możliwości wyszukiwania w nim treści są systematycznie ograniczane. Już teraz nie jest możliwe wyszukiwanie wpisów bez zalogowania się, a kanały dostępowe, wykorzystywane przez zewnętrzne narzędzia, zostały niemal zlikwidowane. Wiele narzędzi, które służą do analizy wpisów na tym portalu, wymaga zalogowania się na konto X, w celu wykonywania jakichkolwiek działań. Coraz więcej narzędzi staje się płatnych lub niedostępnych i, być może, z czasem nie będzie innej możliwości niż tylko przeglądanie bieżącej treści podawanej przez serwis lub dostęp do danych jedynie przez mechanizmy samego portalu X. Czas pokaże, dokąd zmierzają wprowadzane zmiany.

R5 INVID – *IN VIDEO VERITAS*. CIEKAWE NARZĘDZIE PRZYDATNE W BIAŁYM WYWIADZIE

W dobie zalewających nas co chwilę fal fake newsów często trudno jest odróżnić prawdę od prawie prawdy i zupełnych absurdów (czyli od półprawdy i od… fekalioprawdy). Tym bardziej że w Internecie coraz więcej jest treści, które bazując na prawdziwych danych, jednocześnie przeinaczają je w tak diametralny

sposób, że dotarcie do źródła okazuje się niemal niemożliwe. Co więcej, nawet korzystanie z tzw. zaufanych źródeł, czyli oficjalnych serwisów informacyjnych, nie uchroni nas przed fake newsami – i to nawet wówczas, gdy serwisy te nie działają w złej woli, jak miało to miejsce chociażby w przypadku rzekomego ataku z użyciem pistoletu we Wrocławiu[7] czy informacji o odnalezieniu poszukiwanej osoby poprzez analizę pudełka po pizzy (sprawa szerzej opisana w rozdziale *OSINT^2, czyli kilka słów o weryfikacji danych*, s. 100–105). Pośpiech, by zdążyć z „gorącym tematem" przed innymi mediami, często poparty dodatkowo clickbaitowym tytułem, lub zwyczajny brak wiedzy regularnie doprowadzają do publikacji albo całkiem nieprawdziwych informacji, albo np. wiadomości zilustrowanych niewłaściwymi fotografiami.

I wtedy wchodzi on, cały na biało:

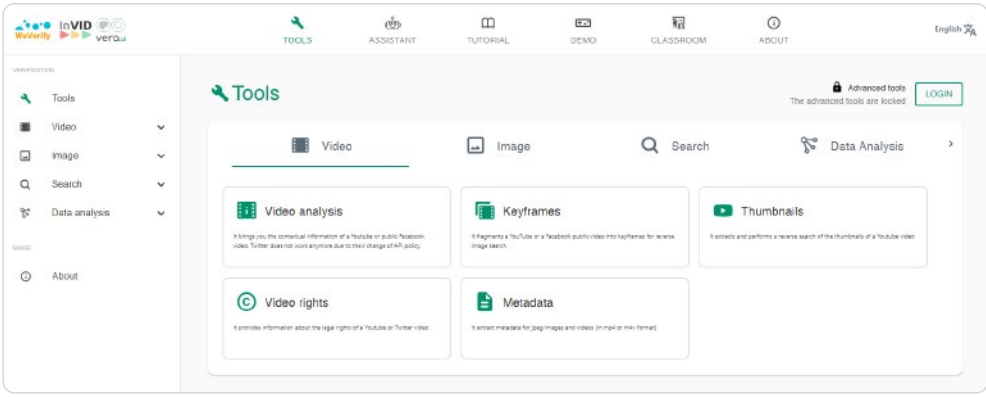
Projekt InVID

InVID jest europejskim projektem mającym na celu pomóc dziennikarzom w dotarciu do prawdziwych źródeł informacji i zdemaskować fałszywe przekazy udostępniane w ramach mediów społecznościowych. Jednym z elementów tego projektu jest bardzo poręczna wtyczka[8] do przeglądarek Chrome i Firefox, która daje garść przydatnych narzędzi OSINT do analizy obrazów oraz filmów. Dzięki niej można zweryfikować, czy nie mamy do czynienia z fake newsem typu *manipulated content* (np. obraz celowo zmodyfikowany na potrzeby newsa) lub *false context* (tu dane są prawdziwe, ale zostały użyte w innym kontekście).

Po zainstalowaniu pluginu jego ikona pojawia się w przeglądarce i umożliwia wybór spośród trzech opcji. Są to:

1. Open InVID – otwarcie zestawu narzędzi (o których bardziej szczegółowo poniżej) w nowej karcie,
2. Video Urls – lista wszystkich filmów zawartych na aktualnie otwartej stronie z możliwością skopiowania ich adresów URL,
3. Images Urls – lista obrazów na aktualnie otwartej stronie (z ich podglądem), umożliwiająca otwarcie ich w osobnej karcie w celu np. skopiowania ich adresu URL.

Ponadto w menu kontekstowym dla obrazów pojawia się dodatkowa lista opcji: powiększenie części obrazu w narzędziu Magnifier, analiza obrazu w narzędziu Forensic oraz możliwość automatycznego uruchomienia wyszukiwania danym obrazem w jednej wybranej wyszukiwarce lub we wszystkich dostępnych w narzędziu wyszukiwarkach (rysunek 34).



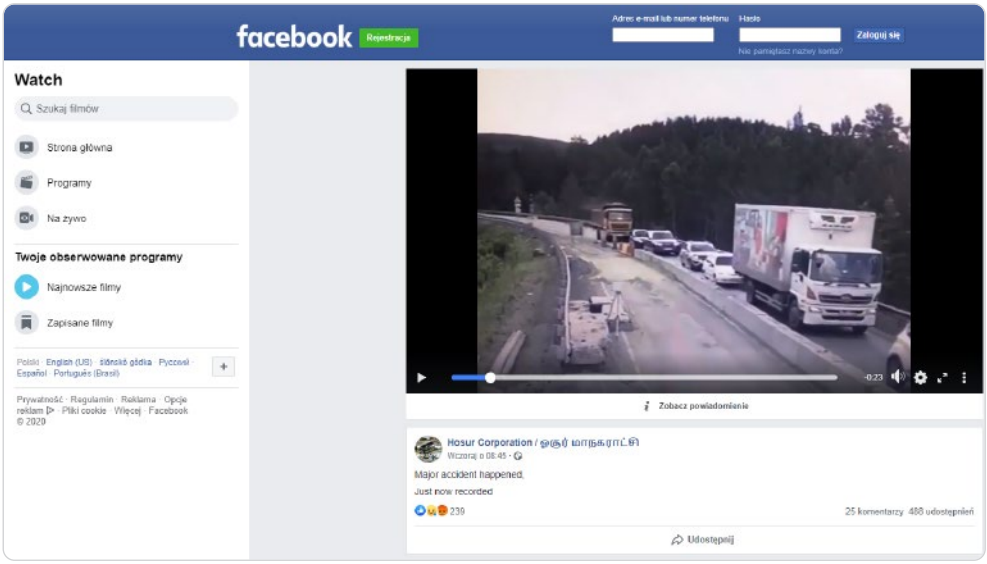
Rysunek 34. Panel z narzędziami InVID

Po wybraniu opcji OPEN INVID z menu pojawiającego się po kliknięciu ikony pluginu mamy możliwość przejścia do zakładki z dostępnymi wszystkimi narzędziami do tropienia fałszywych newsów, Asystenta analizy (ogólnego lub dla strony, na której się znajdujemy) lub samouczka.

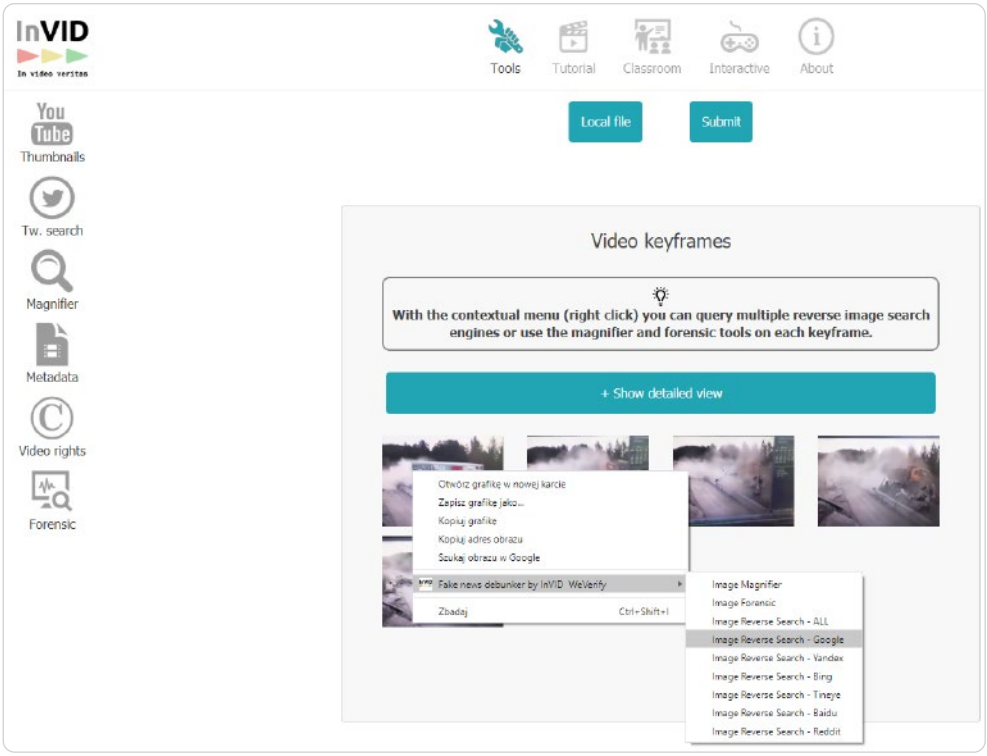
Analiza materiałów wideo

Pierwszym narzędziem jest **Video Analysis**, gdzie można wkleić adres filmu z Facebooka, YouTube lub Twittera. Po jego analizie mamy dostęp do zawartych w nim metadanych, łącznie z wyfiltrowanymi komentarzami, które mogą sugerować, że nagranie jest fałszywe (czyli np. zawierają słowo *fake*). Można tu także przeglądać pobrane klatki kluczowe (czyli wybrane klatki skompresowanego materiału wideo, które zawierają w sobie pełny obraz – pozostałe są jedynie wskazaniem różnic od klatki kluczowej i nie zawierają pełnego obrazu) i automatycznie używać ich do wyszukiwania obrazem w wyszukiwarkach takich jak Google, Yandex i TinEye (lub w innych – jeśli użyjemy opcji z menu kontekstowego dla obrazów opisanych powyżej). Dodatkowo, aby upewnić się, czy przypadkiem nie mamy do czynienia z wykorzystaniem materiału z zupełnie innego, dawniejszego zdarzenia, można w ramach wyszukiwania obrazem, np. w Google, zawęzić wyniki do okresu przed wystąpieniem zdarzenia, które jest przedstawione na danym filmie, gdyż może się okazać, że dana sytuacja tak naprawdę miała miejsce wcześniej i dotyczyła zupełnie innej sprawy.

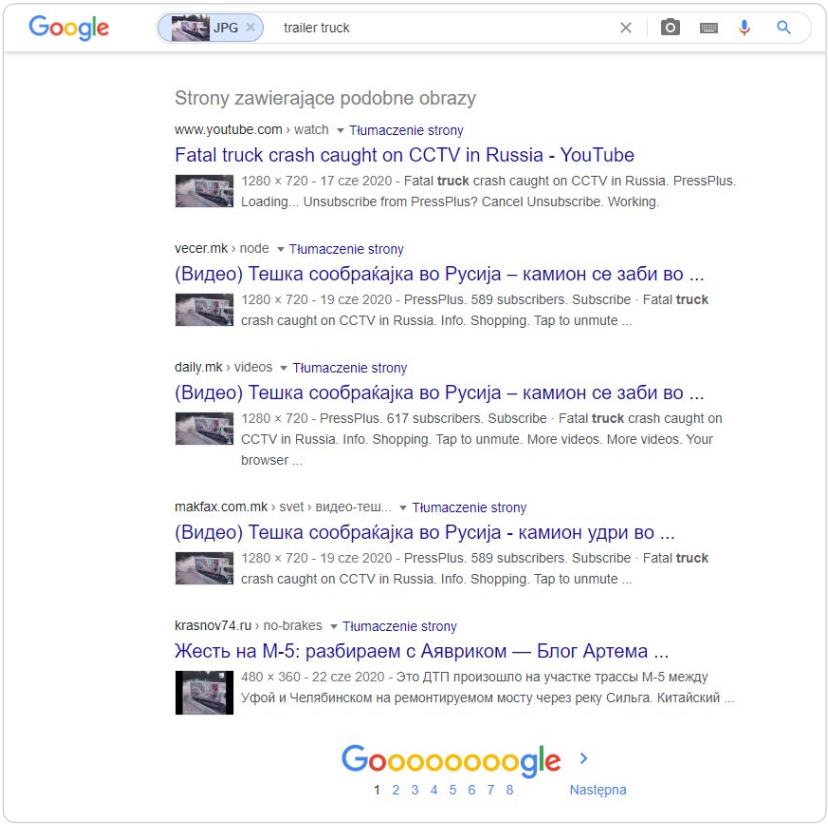
Drugie narzędzie, **Keyframes**, jest nieco rozszerzoną wersją tego z Analysis: tutaj można wkleić link do nagrania lub – czego nie oferowało poprzednie narzędzie – zaczytać lokalny plik. Dodatkowo jest tu do wyboru większa liczba klatek, w przypadku których można wykonać opcję szukania obrazem lub ich analizę. Dzięki temu narzędziu możliwe było szybkie stwierdzenie, że nagranie rzekomego karambolu na jednej z indyjskich dróg w rzeczywistości dotyczy drogi M-5 w Rosji (rysunki: 35, 36 i 37).



Rysunek 35. Wypadek, który rzekomo miał mieć miejsce w Indiach (aktualnie jest już oznaczony przez serwis Facebook jako *fake news*)



Rysunek 36. Szybki *reverse image search*



Rysunek 37. A nie, to jednak w Rosji

Kolejne narzędzie to **Thumbnails**, które wyszukuje jednocześnie czterema obrazami – miniaturkami nagrania z YouTube w wybranej wyszukiwarce: Google, Yandex, Bing lub TinEye.

Narzędzie **X search** to z kolei po prostu zestaw zaawansowanych filtrów dla portalu X. Możemy dzięki niemu wyfiltrować np. wszystkie wpisy dotyczące jakiegoś zdarzenia, czyli nakręcone w tym samym miejscu i czasie, a dodatkowo zawierające np. określone słowo kluczowe. Szersze spojrzenie na niektóre wydarzenia pozwala zweryfikować, czy jedna z relacji nie została zmanipulowana.

Inne narzędzia

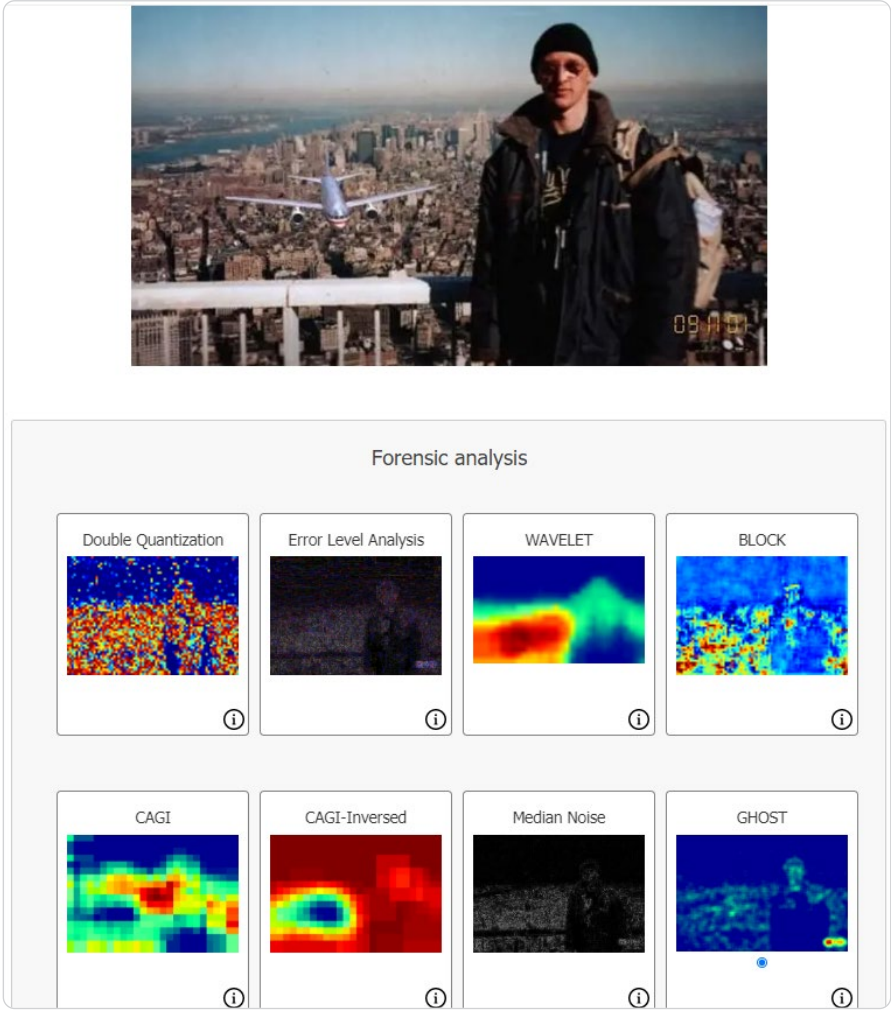
Kolejnym i jednym z ciekawszych – moim zdaniem – narzędzi jest **Magnifier** w sekcji **Image**, czyli, jak sama nazwa wskazuje, szkło powiększające, dzięki któremu możemy dowolnie przybliżać wybrany element obrazu (rysunek 38). Jest to szczególnie pomocne w szybkiej analizie np. zdjęć z niewyraźnymi napisami w tle, które mogą zdradzić miejsce ich wykonania – bez konieczności używania programów graficznych. Dostępne są tu także opcje: wyostrzania,

odwracania poziomego, skalowania i przycinania. Tutaj także można wskazywać adres URL pliku graficznego lub wgrać obrazek z dysku.

Rysunek 38. Tutaj widać, że na nagraniu z wypadku dni tygodnia w panelu CCTV są zapisane cyrylicą

Narzędziem **Metadata** możemy podejrzeć, jak sama nazwa wskazuje, metadane pliku graficznego (JPEG) lub materiałów video (MP4/M4V). Z kolei **Video rights** pobiera po prostu informacje o prawach autorskich z filmów z YouTube lub Facebooka na podstawie podanego linku.

Dość rozbudowany zakres opcji ma ostatnie opisane tu przeze mnie narzędzie: **Forensic**. Możemy w nim analizować obrazy, podając jedynie ich adres URL lub wgrywając je z dysku. Dzięki takim procesom, jak chociażby podwójna kwantyzacja, transformata DWT czy analiza bloków, z których tworzony jest plik w formacie JPEG, jesteśmy w stanie stwierdzić, czy któryś element obrazu nie został dodany do niego w celu manipulacji przedstawianymi faktami. I tak podwójna kwantyzacja wskaże nam obszary, które zostały skompresowane tylko raz, podczas gdy reszta obrazu została skompresowana dwukrotnie, co oznacza, że do już istniejącego pliku w formacie JPEG dodano nowy element. Podobnie analiza bloków formatu JPEG wskaże miejsca, w których występują zakłócenia w danym bloku, co także oznacza, że jego część nie należy do oryginalnego obrazu. Jako przykład można tu podać zdjęcie turysty, rzekomo wykonane na wieży World Trade Center w momencie, kiedy zbliżał się do niej samolot. Widoczne zakłócenia w miejscu, w którym na zdjęciu widoczny jest ów samolot, wskazują na manipulację (rysunek 39).



Rysunek 39. Analiza zdjęcia turysty na WTC – widoczne anomalie w okolicach samolotu

InVID cały czas mocno się zmienia. Pomimo dodania do niego filmów instruktażowych widać, że przedstawiają one inny wygląd interfejsu niż ten aktualny. Może się oczywiście w pewnym momencie okazać, że niektóre opcje przestaną działać, jeśli np. zmieni się API któregoś z wykorzystywanych serwisów. Możliwości narzędzia Forensic stale się jednak zwiększają, więc pozostaje mieć nadzieję, że będzie ono rozszerzać swój wachlarz usług w zakresie oddzielania prawdy od fake newsów.

Podsumowanie

Zestaw narzędzi do weryfikacji materiałów audiowizualnych, zawarty we wtyczce, która w 2023 roku, po kilku zmianach po drodze, dostępna jest pod pełną nazwą **Fake news debunker by InVID & WeVerify** (ze względu na różne

projekty zaangażowane w jej rozwój w poszczególnych latach), stał się takim „szwajcarskim scyzorykiem" dla dziennikarzy i wszystkich innych użytkowników Internetu chcących odpowiedzialnie mierzyć się z coraz większą falą fałszywych informacji rozpowszechnianych w sieci. Część z jego funkcjonalności (narzędzia Twitter SNA oraz CheckGif) wymaga aktualnie rejestracji, a dostęp do nich mogą uzyskać jedynie dziennikarze, factcheckerzy i badacze, jednak nawet jeśli chcemy używać tej wtyczki bez rejestracji, jej możliwości pozostają bardzo szerokie.

R6: SHERLOCK I DOKTOR WHATSMYNAME – WYSZUKIWANIE PROFILI PO NAZWIE UŻYTKOWNIKA

Pisałem już o wyszukiwaniu informacji w jednym serwisie po adresie e-mailowym. W tym rozdziale chciałbym opowiedzieć o sposobach wyszukiwania informacji o tym, w jakich serwisach istnieje konto o danej nazwie użytkownika.

Sherlock

Pierwszym z narzędzi, którym warto się bliżej przyjrzeć, jest Sherlock[9] (rysunek 40) – pythonowy skrypt, który można pobrać z GitHuba i uruchomić na własnej maszynie lub (wersja dla leniwych) odpalić bezpośrednio w przeglądarce, wykorzystując do tego Google Cloud Shell czy serwis repl.it.

Rysunek 40. Sherlock – powitanie

We wszystkich trzech przypadkach musimy jeszcze skonfigurować środowisko, instalując potrzebne zależności, ale sprowadza się to do jednej komendy, którą można znaleźć w informacjach o projekcie na jego stronie na GitHubie.

Korzystanie z Sherlocka jest banalnie proste: uruchamiamy go, podając jako argument jedną lub więcej nazw użytkownika, które chcemy wyszukać, a wynik otrzymujemy na ekranie oraz w plikach tekstowych – po jednym pliku dla każdej nazwy (rysunek 41).

```
kali@kali:~/sherlock/sherlock$ python3 sherlock.py --print-all drwatson
[*] Checking username drwatson on:
[-] ResearchGate: Illegal Username Format For This Site!
[-] 2Dimensions: Not Found!
[-] 3dnews: Not Found!
[+] 4pda: https://4pda.ru/forum/index.php?act=search&source=pst&noform=1&username=drwatson
[+] 7Cups: https://www.7cups.com/@drwatson
[+] 9GAG: https://www.9gag.com/u/drwatson
[+] About.me: https://about.me/drwatson
[+] Academia.edu: https://independent.academia.edu/drwatson
[-] Alik.cz: Not Found!
[-] AllTrails: Not Found!
[-] Anobii: Not Found!
[+] Archive.org: https://archive.org/details/@drwatson
[-] Asciinema: Not Found!
[-] Ask Fedora: Not Found!
[+] AskFM: https://ask.fm/drwatson
[+] Audiojungle: https://audiojungle.net/user/drwatson
[+] Avizo: https://www.avizo.cz/drwatson/
[+] BLIP.fm: https://blip.fm/drwatson
[-] BOOTH: Not Found!
[+] Badoo: https://badoo.com/profile/drwatson
[+] Bandcamp: https://www.bandcamp.com/drwatson
[-] Bazar.cz: Not Found!
[+] Behance: https://www.behance.net/drwatson
[-] BinarySearch: Not Found!
[+] BitBucket: https://bitbucket.org/drwatson/
[-] BitCoinForum: Not Found!
[+] Blogger: https://drwatson.blogspot.com
[+] BodyBuilding: https://bodyspace.bodybuilding.com/drwatson
[+] Bookcrossing: https://www.bookcrossing.com/mybookshelf/drwatson/
[-] BuyMeACoffee: Not Found!
[+] BuzzFeed: https://buzzfeed.com/drwatson
[+] CNET: https://www.cnet.com/profiles/drwatson/
[-] CapFriendly: Not Found!
[-] Carbonmade: Not Found!
```

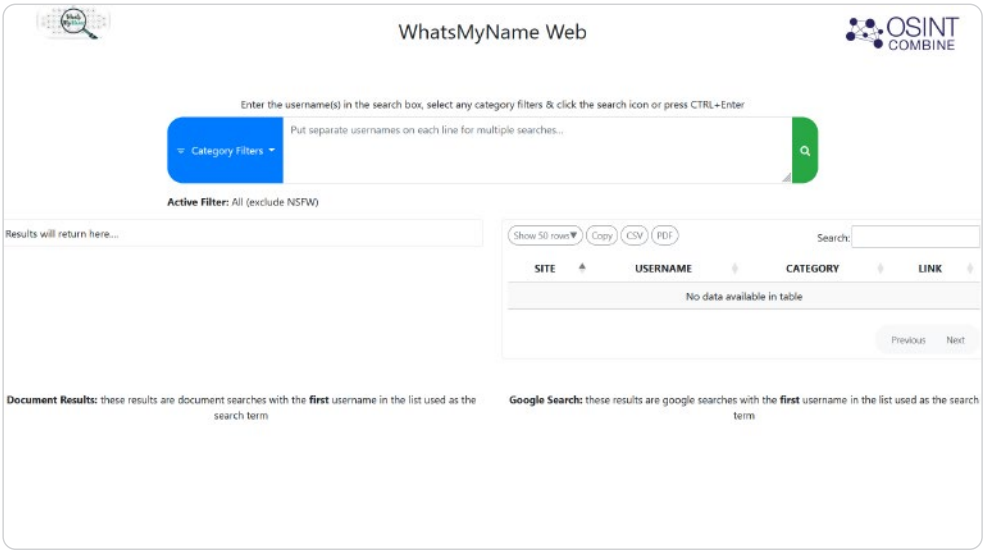
Rysunek 41. Sherlock poszukuje doktora Watsona – kilku udało się znaleźć

Narzędzie wyszukuje i podaje adresy profili z zakresu niemal 300 stron, włączając w to serwisy takie jak: X, Facebook, GitHub, HackTheBox, Reddit czy Tinder, zatem, jak widać, rozstrzał analizy jest ogromny. W wypadku prostszych nazw użytkownika jest więc duże pole do analizy. Ciekawym zasobem informacji do przejrzenia okazuje się też lista stron nieobsługiwanych z różnych powodów (dostępna z opisem w pliku `removed_sites.md`). Można tu znaleźć informacje o tym, jakie odpowiedzi dają serwisy, na których nie można sprawdzić profilu po nazwie użytkownika lub odpowiedź nie jest jednoznaczna. Sherlock pozwala także na skanowanie przez sieć Tor albo serwery proxy, zawężenie listy przeszukiwanych serwisów oraz wyświetlanie wyników dla stron, na których nie znaleziono danego użytkownika, z podaniem przyczyny (tą może być nie tylko brak konta, ale np. niedozwolony format nazwy użytkownika dla danej witryny).

WhatsMyName

Podobne narzędzie, występujące początkowo także w postaci skryptu Pythona i pozwalające przeszukać pokaźną bazę serwisów, to *WhatsMyName*[10] (rysunek 42). Wprawdzie w maju 2023 roku projekt został zawieszony i skrypt pythonowy nie jest już dostępny, jednak od tego czasu istnieje możliwość użycia wyszukiwarki w formie *online*, ponieważ na stronie *whatsmyname.app* dostępny jest bardzo przejrzysty interfejs webowy tego narzędzia. Pokazuje on

wyniki poszukiwań wraz z hasłowym opisem serwisu oraz daje dodatkowo możliwość filtrowania i eksportowania danych.



Rysunek 42. Interfejs narzędzia na stronie *whatsmyname.app* – warto zwrócić uwagę na fakt, że domyślnie pewne strony (NSFW – Not Safe For Work) są wykluczane z wyszukiwania

Podsumowanie i rady

Podczas używania narzędzi przeszukujących np. po nazwie użytkownika warto pamiętać, że konto o tej samej nazwie na różnych serwisach nie musi koniecznie należeć do tej samej osoby, więc przed wyciągnięciem pochopnych wniosków trzeba się upewnić, czy nie mamy do czynienia z taką sytuacją.

Narzędzia wyszukujące profile użytkowników powinny być jedynie początkiem dalszych poszukiwań i skrupulatnej analizy.

R7 NA OSINT-OWYM TROPIE TAJNEJ NIEMIECKIEJ ORGANIZACJI

Centralna Agencja Wywiadowcza, CIA (Central Intelligence Agency), ma swoje tajne budynki na Litwie[11], które pokazała ponad 16 lat po ujawnieniu faktu ich istnienia przez „The Washington Post". Brytyjska służba specjalna Government Communications Headquarters (GCHQ) sama podała[12] lokalizację swojej tajnej miejscówki po wyprowadzeniu się z niej. Tymczasem w Niemczech… na przełomie 2021 i 2022 roku głośnym echem odbiła się sprawa Federalnej Służby Telekomunikacyjnej, BST (Bundesservice Telekommunikation), która bardzo szybko zaczęła znikać z wszelkich oficjalnych rejestrów po tym, jak Lilith Wittmann, aktywistka i specjalistka z dziedziny IT, zaczęła o nią wypytywać.

Akt I. Wykopki

Wszystko zaczęło się w grudniu 2021 roku[13] podczas przeszukiwania listy wszystkich organów władzy federalnej w Niemczech, dostępnej na rządowej platformie *service.bund.de*. Ilość danych zawartych w tego rodzaju portalach jest przeogromna i podczas poszukiwań OSINT-owych są one bardzo dobrym źródłem wiedzy, szczególnie jeśli poszukujemy informacji o organizacjach rządowych lub firmach. To właśnie część tzw. deep webu, czyli baz danych niezindeksowanych przez wyszukiwarki takie jak Google czy Bing.

Lilith Wittmann zauważyła tam kilka nazw, które wzbudziły jej podejrzenia. Szczególnie ciekawa okazała się właśnie Bundesservice Telekommunikation (rysunki 43 i 44), o której istnieniu dowiedziała się dopiero wtedy, mimo że jest osobą z branży IT na co dzień zajmującą się kwestiami cyfryzacji w organach państwowych. Takiej informacji nie wychwyciłoby żadne narzędzie, a jedynie wprawne oko badacza.

Rysunek 43. Profil Bundesservice Telekommunikation na Twitterze, założony dla żartu w styczniu 2022 roku

Po krótkiej analizie wpisów na portalu FragDenStaat okazało się, że Bundesservice Telekommunikation istnieje w bazach rządowych już od co najmniej 10 lat, ma teoretycznie swoją stronę internetową (aczkolwiek zarejestrowano ją dopiero w styczniu 2022 roku!), adres e-mailowy, numer telefonu oraz faks. Ma także swój opis, jednak stwierdzenia typu (w wolnym tłumaczeniu): „Organ [...] wykonuje różne zadania wyłącznie dla ministerstw federalnych i ich jednostek. Należą do nich zadania specjalistyczne, zadania przekrojowe

i pomocnicze oraz środki modernizacji", brzmią, jak gdyby pochodziły ze średniej klasy generatora opisów dla dowolnych organizacji, niekoniecznie rządowych. Weryfikacja numeru telefonu pokazuje, że prefiks 030 to faktycznie numer kierunkowy do Berlina.

Warto w tym momencie zwrócić uwagę na element, który nie umknął także Wittmann – identyfikator wpisu na portalu FragDenStaat. Jego wartość była bardzo niska w porównaniu z innymi, co potwierdzało, że organizacja ta została wprowadzona do bazy już jakiś czas temu. Oczywiście nie zawsze identyfikatory muszą być generowane przyrostowo – w niektórych bazach zamiast kolejnych liczb stosowane są losowe GUID-y* lub hashe. Dodatkowym czynnikiem, który warto zweryfikować, są wpisy poprzedzające analizowany element i następujące po nim. To może wskazać, z jakiej kategorii lub zbioru danych pochodzi interesujący nas wpis.

Bundespolizeidirektion Sankt Augustin	Bundesgrenzschutzstraße 100 53757 Sankt Augustin
Bundesservice Telekommunikation	Heidelberger Straße 63 - 64 12435 Berlin
Bundesverwaltungsamt	Barbarastraße 1 50735 Köln
Bundeszentrale für politische Bildung	Adenauer Allee 86 53113 Bonn

Rysunek 44. Fragment listy jednostek rządowych – dostępny już tylko w archiwum Internetu[14] (The Wayback Machine)

Wróćmy jednak do poszukiwań, które w tym momencie przeszły z trybu pasywnego w aktywny, gdyż poszukiwaczka postanowiła zadzwonić pod numer telefonu teoretycznie należący do BST. Usłyszała jednak dźwięk faksu. W takiej sytuacji nie pozostało nic innego, jak zadzwonić pod numer faksu, pod którym… nie odezwał się już dźwięk faksu, ale także nie odebrał go żaden człowiek ani automat. Takim samym ślepym zaułkiem okazał się adres e-mail, gdyż próba wysłania wiadomości elektronicznej zakończyła się komunikatem zwrotnym: „Nie znaleziono skrzynki". Także pytanie rzucone na Twitterze[15] nie przyniosło

* GUID (Globally Unique IDentifier) – globalny identyfikator jednoznaczny.

żadnego przełomu w śledztwie, które tym samym było już w pełni jawne i aktywne. Nikt ani nie potwierdził istnienia instytucji, ani nie zaprzeczył temu, że została ona utworzona. Na szczęście, dzięki pomocy osób przebywających w okolicy adresu, pod którym miało mieścić się biuro BST, udało się zdobyć zdjęcia pokazujące, że faktycznie znajduje się tu instytucja o takiej nazwie.

Ciekawszym wątkiem okazała się próba uzyskania odpowiedzi na pytania przesłane do Federalnego Biura Administracji, BVA (Bundesvervaltungsamt), odpowiedzialnego za portal, na którym pierwotnie Wittmann natrafiła na informacje o BST. Zapytanie o szczegóły było możliwe dzięki obowiązującemu w Niemczech od 2006 roku prawu dostępu do informacji publicznej. Podobne przepisy dotyczą niemal wszystkich krajów europejskich, także Polski, i dają każdemu obywatelowi możliwość uzyskania odpowiedzi na nurtujące go pytania o szczegóły działalności organów publicznych. Co ciekawe, nie wszystkie landy wprowadziły to prawo, co sprawia, że Niemcy są pod tym względem w tyle za resztą Europy.

Uzyskane odpowiedzi nie wyjaśniały w żaden sposób sytuacji, ale tym razem OSINT-owym tropem wartym uwagi okazały się metadane zawarte w e-mailu, a konkretnie – w polu kopii jawnej, CC (Carbon Copy). Widniało tam imię i nazwisko osoby, której adres e-mailowy został dodany do listy odbiorców przez urzędnika odpowiadającego na zapytanie, a także informacja o tym, że ów adresat jest oficerem bezpieczeństwa. Sytuacja zaczęła się więc robić coraz bardziej dynamiczna. Dodatkowo próba telefonicznego wyjaśnienia sprawy okazała się niemożliwa, a pracownik, który odebrał telefon, zdawał się czuć bardzo niekomfortowo (Wittmann użyła nawet stwierdzenia, że niemal spanikował) i przekierował rozmowę do swojego przełożonego, który jednak nic nowego nie wniósł.

Kilka dni później przyszła kolejna odpowiedź na zapytanie, ucinająca kwestię stwierdzeniem, że (w uproszczeniu) „to nie nasza sprawa", a informacja o Bundesservice Telekommunikation zniknęła ze stron rządowych. Jedyna pozostałość po niej to wpis w serwisie rządowym[16] służącym do wyszukiwania danych teleadresowych (nie licząc oczywiście stron zarchiwizowanych w Web Archive[17]). To pokazuje też, jak trudno jest całkowicie usunąć informacje, które zostały opublikowane w Internecie.

Pomocną dłoń w tym momencie wyciągnęła Heidi Reichinnek, zasiadająca w Bundestagu. Jest to o tyle ważne, że odpowiedzi na zapytania przesyłane przez polityków muszą być przygotowane w ciągu tygodnia. To daje im dużą przewagę nad działaniami prowadzonymi przez osobę spoza uprzywilejowanych kręgów. Jedyną informacją, jaką udało się uzyskać, był budżet poszukiwanej organizacji, który w ciągu ostatnich pięciu lat wyniósł… całe 0 euro. Mało, jak na służbę zajmującą się łącznością. Chyba że owa służba tak naprawdę nie istnieje.

Punktem zaczepienia w tym momencie stała się osoba, która udzielała odpowiedzi na powyższe pytanie (oraz drugie, wysłane w celu potwierdzenia, czy na pewno BST nie miało budżetu). Był to sekretarz stanu Hans-Georg Engelke, wcześniej odpowiedzialny m.in. za tematy porządku publicznego czy policji federalnej.

W tym momencie należy podkreślić (i stwierdza to też Lilith Wittmann w swoim pierwszym artykule, o którym jest mowa na początku tego rozdziału), że wszystkie powyższe informacje zostały zdobyte w wyniku zwyczajnych działań OSINT-owych. Pozyskane dane były dostępne dla każdego w Internecie, a jedynie złożenie ich w całość zdaje się łamigłówką dla wytrwałych i upartych detektywów.

Akt II. Wejście

Kilkanaście dni po opublikowaniu powyższych wyników śledztwa Lilith Wittmann opisała[18] swoje kolejne odkrycia w temacie tajemniczej służby. Także ten artykuł obfituje w informacje o technikach OSINT-owych, którym warto przyjrzeć się bliżej.

Po opisaniu znaleziska przez Wittmann na jej blogu konieczne okazało się przeanalizowanie informacji, które spłynęły od czytelników tego tekstu. I tu chciałbym się na chwilę zatrzymać, ponieważ samo zbieranie informacji w ogólnodostępnych źródłach to jeszcze nie OSINT.

> Jak sama nazwa wskazuje, do **Open-Source Intelligence**, czyli pełnego wywiadu otwartoźródłowego, trzeba jeszcze wykonać pracę analityczną. Jest to bardzo istotny aspekt, który zawsze objaśniam na szkoleniach OSINT-owych, gdyż bez odpowiedniego przygotowania i znajomości ograniczeń umysłu oraz „utartych szlaków" myślenia, jakie są zaprogramowane w mózgach, nie będziemy w stanie wyciągnąć prawidłowych wniosków. Niestety, wiele osób nie zdaje sobie sprawy, jak bardzo te ograniczenia, łącznie ze spolaryzowaniem osądów, wpływają na wynik badań i śledztw.

Wracając jednak do tajemniczej niemieckiej służby, warto wspomnieć, że jednym z kolejnych tropów w tej sprawie było odszukanie nowych informacji na stronie firmy wynajmującej biura pod adresem przypisanym BST, znalezionym wcześniej na stronach rządowych. Firma ta jako referencje pokazuje nadal, że wynajmuje 2500 m^2 w dzielnicy Berlin-Treptow Federalnemu Ministerstwu (rysunek 45). Dłuższa analiza innych firm operujących w tym samym kompleksie i uzyskany przez to zbiór dość dziwnych elementów z nimi związanych (jak np. dość niespotykane zakresy ich działania lub brak możliwości zdobycia informacji o kierownictwie tych firm), skłoniły autorkę do konkluzji, że potwierdza to założenie, iż BST należy do tajnych służb.

Po dłuższym namyśle Wittmann doszła jednak do wniosku, że większość budynków w Berlinie stanowi podobną mieszankę i bardzo łatwo jest wpaść w „pułapkę umysłu", jeśli pierwszorzędnym celem jest jedynie potwierdzenie, a nie zweryfikowanie śmiałej tezy.

Rysunek 45. Widok budynku, w którym miało mieścić się biuro BST w berlińskiej dzielnicy Treptow. Niestety, na terenie Niemiec zasoby Google Street View są bardzo ubogie – to zdjęcie pochodzi z 2008 roku

Brak dalszych możliwości zdalnego zbadania tematu skłonił Wittmann do osobistego odwiedzenia budynku. Jednym z elementów, które zaobserwowała w podziemnym parkingu, były samochody marki Volkswagen (model Volkswagen Transporter), które lśniły czystością pomimo panującej akurat zimy. Podobnych samochodów używa m.in. niemiecka służba kontrwywiadu cywilnego, jednak to także była tylko poszlaka.

Akt III. Namierzanie

Kolejną metodą weryfikacji, kto stoi za BST, było sprawdzenie danych w bazie RIPE[19]. RIPE Network Coordination Centre jest niezależną organizacją z główną siedzibą w Amsterdamie, która zajmuje się m.in. przydzielaniem publicznych adresów IPv4 i IPv6 w ramach Regionalnego Rejestru Internetowego, RIR (Regional Internet Registry), dla obszaru Europy, Bliskiego Wschodu i części Azji Centralnej. W wyniku zapytania wysłanego do bazy RIPE Wittmann uzyskała jeden adres e-mailowy należący do Federalnego Ministerstwa Spraw Wewnętrznych i Rodziny. Analiza konstrukcji loginu tego e-maila pozwoliła jej wyciągnąć wniosek, że jest on przypisany do nieistniejącej (przynajmniej według oficjalnych rejestrów) komórki ministerialnej. Tak oto do nieistniejącej

służby dołączyło kolejne nieistniejące biuro innego ministerstwa. Dalsze poszukiwania w bazie RIPE uwidoczniły następne teoretycznie nieistniejące biura Ministerstwa Spraw Wewnętrznych, a wszystko zdawało się łączyć z Federalnym Biurem Ochrony Konstytucji, czyli wspomnianą już wcześniej służbą kontrwywiadu cywilnego.

Poprzez kolejne wyszukiwania w bazie RIPE i kolejne komórki niefigurujące w oficjalnych strukturach autorka dotarła nawet do adresów IP serwerów należących prawdopodobnie do wspomnianej służby, wykorzystywanych, być może, do szpiegowania obywateli, a ukrytych we francuskim centrum danych amerykańskiego providera GoDaddy. Takich zwrotów akcji nie powstydziłby się niejeden reżyser filmów o tematyce szpiegowskiej.

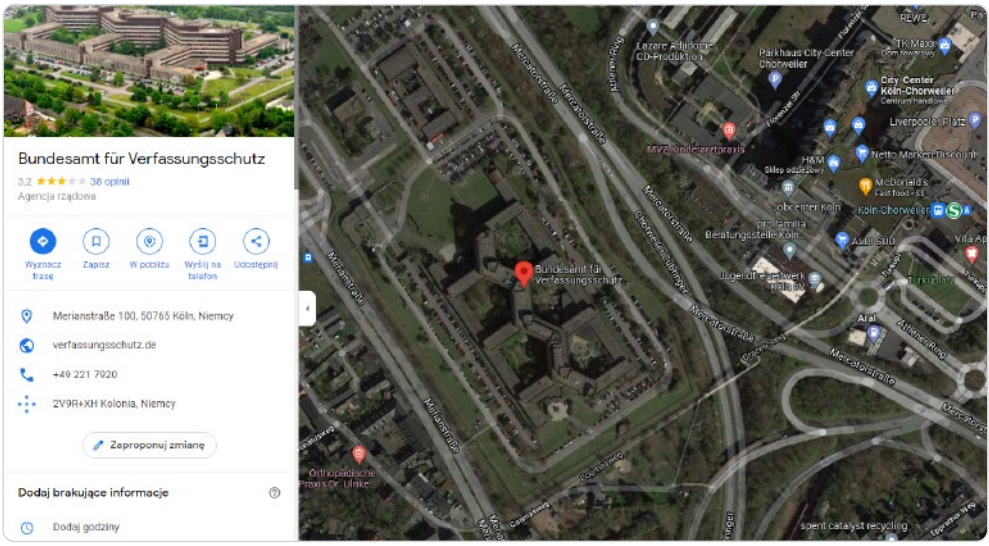
Smaczku całej sprawie dodaje kolejne spostrzeżenie Wittmann, dotyczące imion i nazwisk osób powiązanych z przedmiotem poszukiwań, znalezionych przez badaczkę w bazie RIPE. Personalia te brzmią tak, jakby wszystkie zostały stworzone za pomocą generatora danych osobowych (pamiętacie jeszcze motyw opisu służby z początku tekstu?). Także analiza adresów korespondencyjnych przyniosła ciekawe efekty – dwie komórki miały skrytki pocztowe tuż obok siebie.

Akcja poszukiwań nie zwalnia ani na chwilę, gdyż kolejnym odkryciem Wittmann był brak jakichkolwiek informacji o domenach użytych w adresach e-mailowych. Ministerstwo Spraw Wewnętrznych używa domeny *bmi.bund.de*, a wersji *bmi-treptow.bund.de* nie znają nawet pracownicy rządowego CERT-u!

To jeszcze nie koniec tej sprawy. Podczas konferencji prasowej 17 stycznia 2022 roku[20] przedstawiciel Ministerstwa Spraw Wewnętrznych zaprzeczył istnieniu BST w strukturach ministerialnych. Następnego dnia przed godziną drugą w nocy Wittmann przeszła do bezpośredniej interakcji i zadzwoniła pod berliński numer telefonu znaleziony w bazie RIPE. O dziwo, telefon od razu odebrał jakiś mężczyzna, jednak po krótkiej wymianie zdań rozłączył się i odtąd numer ten nie był już dostępny. Wittmann wysłała więc e-maile na prawdopodobne kombinacje loginów i domen, które znalazła. Jeden z nich dotarł do adresata, więc skrzynka tej osoby istniała. Kolejny numer telefonu i kolejne połączenia dawały coraz więcej dziwnych wyników – zawsze ktoś był obecny pod numerem powiązanym z (nieistniejącym!) biurem MSW w Kolonii. Żadnych odpowiedzi jednak nie udało jej się uzyskać. Jak zatem powiązać BST z Federalnym Biurem Ochrony Konstytucji?

Skoro nie można było prześledzić drogi e-maila (chociaż, moim skromnym zdaniem, można było spróbować wykorzystać zdalną zawartość, jak piksele/obrazki śledzące lub inne *canary tokens*), autorka postanowiła wysłać fizyczny nadajnik. Cóż innego nadaje się do tego lepiej niż AirTag (przypomnijcie sobie sprawę przesyłki do króla Niderlandów[21]). Nadajnik trafił do grubej gazety o tematyce podróżniczej, a ta została wysłana pocztą do (przypominam –

nieistniejącego) biura MSW w Kolonii. Póki sygnał był jeszcze odbierany, wskazywał trasę podróży przesyłki, aż do… budynku Biura Ochrony Konstytucji w Kolonii (rysunek 46). W pewnym momencie jednak trop się urwał, a lokalizacja AirTaga nie była już aktualizowana. Wszystkie opisane powyżej instytucje zdaje się jednak łączyć Federalna Służba Telekomunikacyjna, która była zalążkiem całego śledztwa.



Rysunek 46. W tym budynku po raz ostatni nawiązano kontakt z wysłanym AirTagiem

Akt IV. Finał?

Powiązań jest więcej i Czytelnikom zainteresowanym szczegółowym przebiegiem całej sprawy polecam wczytanie się we wpisy na blogu Lilith Wittmann (dostępne w języku niemieckim).

Co jakiś czas pojawiają się jednak nowe tropy i zdaje się, że Wittmann nie powiedziała jeszcze ostatniego słowa w tym temacie. Może więc, dzięki nieustępliwości internetowych detektywów, uda się w końcu uzyskać pełniejsze informacje lub obalić mit o nie do końca odpowiednio zakamuflowanej komórce niemieckiego rządu? A może „królicza nora" sięga jeszcze głębiej?

Post scriptum

Przeszkodą dla niektórych osób może być fakt, że dużo informacji o tej sprawie dostępnych jest wyłącznie w języku niemieckim, a translatory nie zawsze oddają sens zdań oraz niekiedy gubią całe akapity. Dobrym rozwiązaniem jest w tym przypadku zarówno skorzystanie z automatycznego tłumaczenia stron przez przeglądarki, np. Chrome lub Firefox (ikona tłumacza pojawia się w pasku adresu) na język angielski i/lub polski, jak również, w niektórych

przypadkach, skopiowanie tekstu i wklejenie go do translatora w celu zrozumienia określonych części zdań.

Część informacji zawarta jest wyłącznie na zrzutach ekranu, ale i na to jest rada. Taki obraz, wyświetlony w osobnej karcie lub zapisany na dysku, można następnie przesłać do wyszukiwania obrazem w wyszukiwarkach grafiki, jak Google lub Yandex, które potrafią rozpoznawać tekst na obrazie i radzą sobie z tym naprawdę nieźle. W celu lepszego zrozumienia sprawy warto też zaznajomić się z podziałem niemieckich komórek rządowych, co mnie na początku sprawiało najwięcej trudności ze względu na fakt, że nie zajmuję się tym obszarem geograficznym na co dzień.

Podsumowanie i rady

Każdy obywatel może żądać dostępu do informacji o działalności organów publicznych – i warto z takiej możliwości korzystać, aby poszerzać swoją wiedzę o interesujących nas tematach. Umożliwi to każdemu z nas lepszą ocenę rzeczywistej sytuacji.

Umysł ludzki jest tak skonstruowany, że lubi podążać utartymi ścieżkami. Dlatego ważne jest, aby przed przystąpieniem do analizy jakiejkolwiek sprawy mieć na uwadze to, w jaki sposób sami siebie ograniczamy i co będzie stanowiło przeszkodę w uzyskaniu obiektywnej odpowiedzi na zadawane sobie pytania.

Wiele informacji można zdobyć w Internecie w sposób pasywny, ale jeśli nie ogranicza nas konieczność zachowania dyskrecji podczas śledztwa, warto przejść do trybu aktywnego: zadawać pytania, odwiedzać dane lokalizacje itp.

W prowadzeniu śledztw OSINT-owych bardzo pomocna jest choćby podstawowa wiedza z różnych dziedzin (głównie IT, ale nie tylko), gdyż w wielu przypadkach ułatwia to połączenie faktów lub wyciągnięcie odpowiednich wniosków. W przypadku omawianego śledztwa było to chociażby rozszyfrowywanie znaczenia loginów w adresach e-mail do kontaktu.

R8 OSINT W PANDEMII, CZYLI CO WYNIKAŁO Z WYNIKÓW TESTÓW

Całkiem niedawno musieliśmy zmagać się ze skutkami pandemii i, chcąc nie chcąc, dostosowywać nasze aktywności do ówczesnej rzeczywistości. Przeniesienie wielu jej elementów do Internetu oraz nowe procedury społeczne, skutkujące stworzeniem całkiem nowych dokumentów, jak chociażby certyfikaty COVID-owe (rysunek 47), znalazło swoje odzwierciedlenie w zbieraniu danych OSINT-owych. W tym rozdziale przeanalizuję przypadki możliwych manipulacji związanych z tą tematyką.

Rysunek 47. Certyfikat COVID-owy z kodem QR

Przypadek Jacka Kurskiego

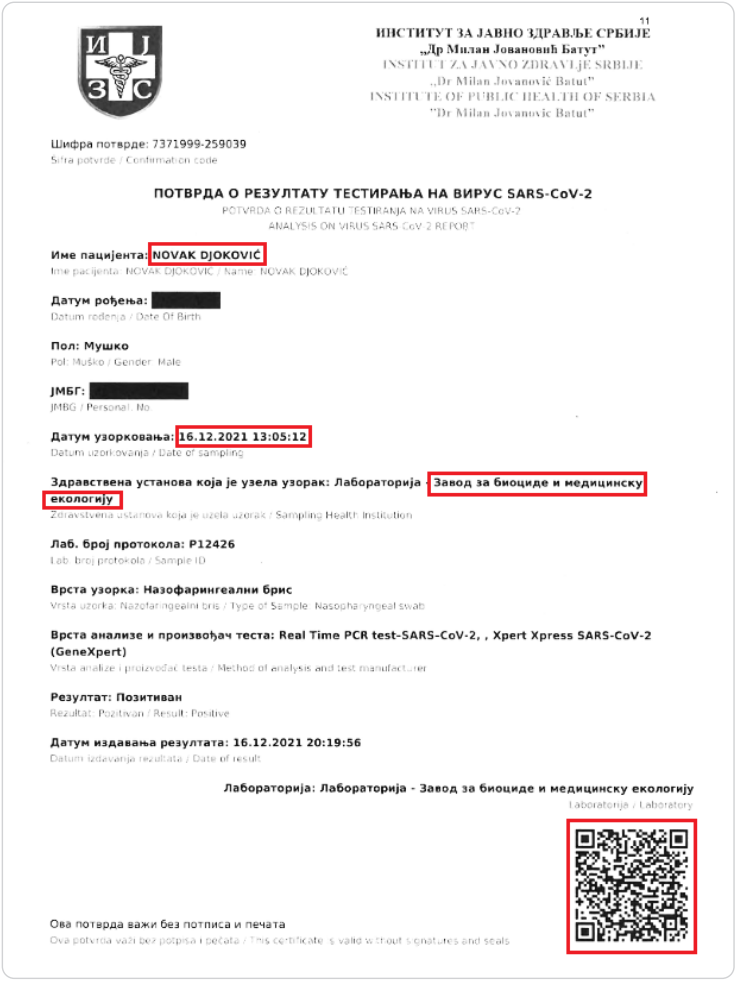
Bez wikłania się w kontekst polityczny wspomnę tylko z kronikarskiego obowiązku o rodzimym przypadku Jacka Kurskiego i jego wyjazdu na Eurowizję Junior w grudniu 2021 roku po otrzymaniu pozytywnego wyniku testu PCR kilka dni wcześniej. Z oświadczenia[22] Centralnego Szpitala Klinicznego MSWiA (CSK MSWiA) w Warszawie wynika, że: „Badanie to zostało wykonane po okresie aktywnej fazy choroby w celu potwierdzenia statusu ozdrowieńca, tzn. czy wydalane jeszcze RNA wirusa (fragmenty łańcucha RNA) jest czy też nie jest patogenne (zaraźliwe)".

Analiza zasad działania testów PCR, których cykle oznaczają po prostu kolejne etapy namnażania się elementów wirusa w pobranym materiale, pokazuje, że wynik pomiędzy 30. a 35. cyklem badania to już prawie końcówka testu (zazwyczaj dochodzi się maksymalnie do 40. cyklu), co oznacza, że śladów RNA wirusa jest mało i warto ponowić test np. następnego dnia, żeby dowiedzieć się, czy wartości te będą wzrastać (początek choroby), czy maleć (koniec choroby). Zakładam jednak, że we wspomnianym przypadku także inne, dostępne dla lekarzy, sposoby weryfikacji etapu rozwoju choroby rozwiały wszelkie wątpliwości.

Przypadek Novaka Djokovicia

Nieco ciekawszym, bo i bogatszym w dowody, przypadkiem była sprawa Novaka Djokovicia, która z OSINT-owego punktu widzenia została opisana na stronach Brigada OSINT[23]. W swoim artykule autor przybliżył po kolei wszystkie elementy związane z zamieszaniem wokół serbskiego tenisisty, który próbował wystąpić w Australian Open bez szczepienia, jedynie posiadając testy PCR – jeden, pozytywny, z 16 grudnia, a drugi, negatywny, z 22 grudnia. Dostęp

do wyników testów jest możliwy *online*, więc nawet dzisiaj możemy dowiedzieć się, czy na pewno drugi test był negatywny, sprawdzając to na stronie serbskiego Instytutu Zdrowia Publicznego[24]. Dostępny tam jest także wynik pierwszego testu[25]. I tutaj zaczyna się prawdziwy rollercoaster, jeśli chodzi o weryfikację danych (rysunek 48).



ИНСТИТУТ ЗА ЈАВНО ЗДРАВЉЕ СРБИЈЕ
„Др Милан Јовановић Батут"
INSTITUT ZA JAVNO ZDRAVLJE SRBIJE
„Dr Milan Jovanović Batut"
INSTITUTE OF PUBLIC HEALTH OF SERBIA
"Dr Milan Jovanovic Batut"

Шифра потврде: 7371999-259039
Šifra potvrde / Confirmation code

ПОТВРДА О РЕЗУЛТАТУ ТЕСТИРАЊА НА ВИРУС SARS-CoV-2
POTVRDA O REZULTATU TESTIRANJA NA VIRUS SARS-CoV-2
ANALYSIS ON VIRUS SARS CoV 2 REPORT

Име пацијента: NOVAK DJOKOVIĆ
Ime pacijenta: NOVAK DJOKOVIĆ / Name: NOVAK DJOKOVIĆ

Датум рођења: [redacted]
Datum rođenja / Date Of Birth

Пол: Мушко
Pol: Muško / Gender: Male

ЈМБГ: [redacted]
JMBG / Personal: No

Датум узорковања: 16.12.2021 13:05:12
Datum uzorkovanja / Date of sampling

Здравствена установа која је узела узорак: Лабораторија - Завод за биоциде и медицинску екологију
Zdravstvena ustanova koja je uzela uzorak / Sampling Health Institution

Лаб. број протокола: P12426
Lab. broj protokola / Sample ID

Врста узорка: Назофарингеални брис
Vrsta uzorka: Nazofaringealni bris / Type of Sample: Nasopharyngeal swab

Врста анализе и произвођач теста: Real Time PCR test-SARS-CoV-2, , Xpert Xpress SARS-CoV-2 (GeneXpert)
Vrsta analize i proizvođač testa / Method of analysis and test manufacturer

Резултат: Позитиван
Rezultat: Pozitivan / Result: Positive

Датум издавања резултата: 16.12.2021 20:19:56
Datum izdavanja rezultata / Date of result

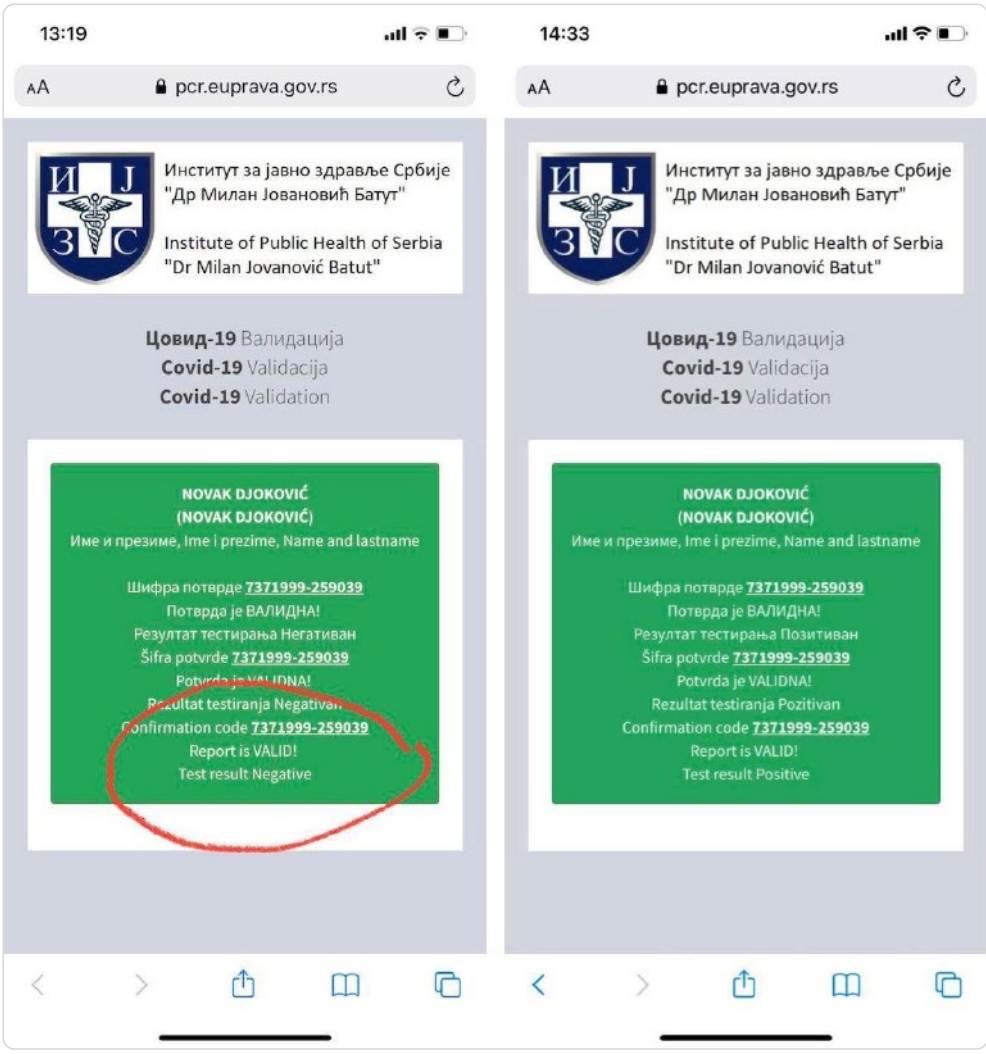
Лабораторија: Лабораторија - Завод за биоциде и медицинску екологију
Laboratorija / Laboratory

Ова потврда важи без потписа и печата
Ova potvrda važi bez potpisa i pečata / This certificate is valid without signatures and seals

Rysunek 48. Zrzut ekranu strony serbskiego Instytutu Zdrowia Publicznego z danymi o teście Novaka Djokovicia (Institute of Public Health of Serbia "Dr Milan Jovanovic Batut")

Jak sądził Djoković, w celu bezproblemowego wjazdu na teren Australii potrzebował dwóch wyników: pozytywnego i negatywnego (w dużym uproszczeniu, ponieważ po drodze pojawił się jeszcze temat możliwej kwarantanny w Nowej Południowej Walii, gdzie przepisy są nieco mniej restrykcyjne niż w Melbourne). Jak zauważyli w swoim artykule autorzy piszący do magazynu „Der Spiegel"[26], wynik pierwszego testu był najpierw negatywny (weryfikacja

tego faktu nastąpiła o godzinie 13.19), by o godzinie 14.33 tego samego dnia stać się wynikiem pozytywnym (rysunek 49[27]).

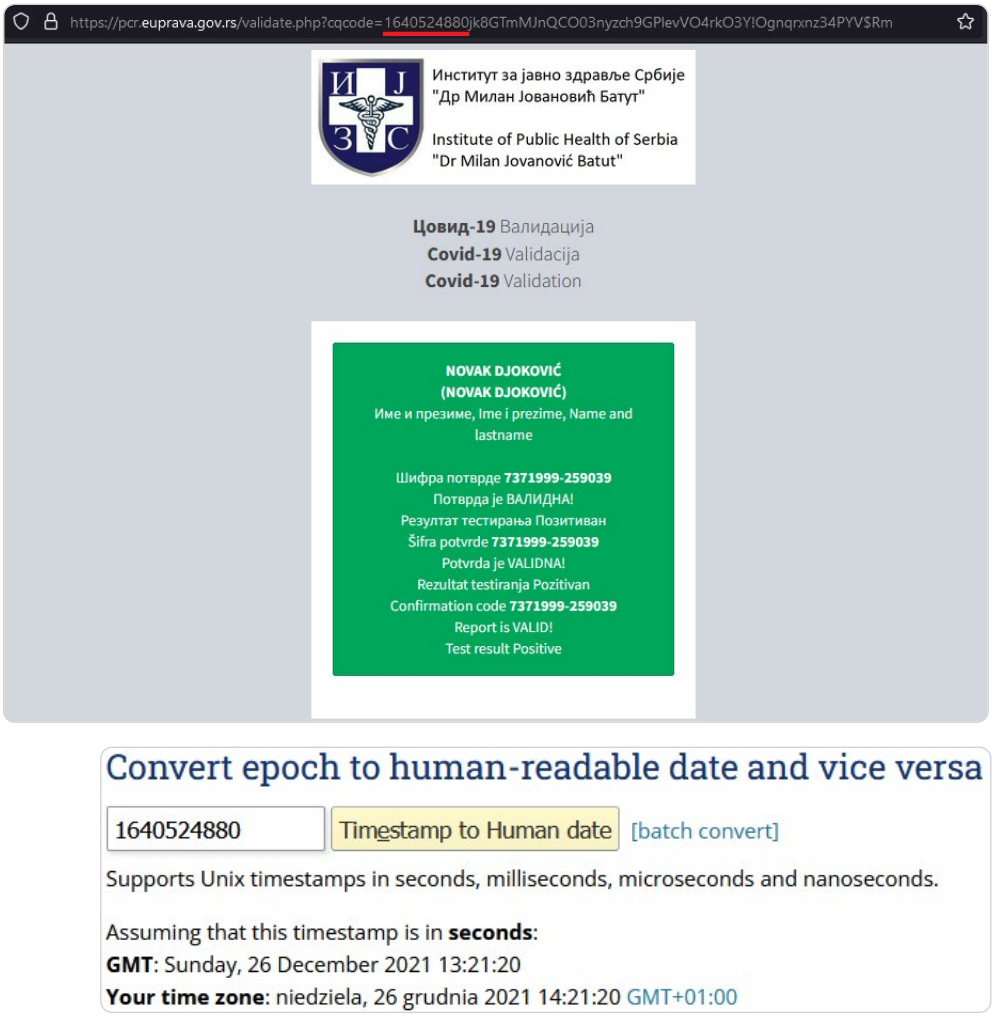


Rysunek 49. Zmieniający się w czasie wynik pierwszego testu Novaka Djokovicia

Czy było to spowodowane tym, że z dwoma negatywnymi wynikami tenisista nie miałby żadnych szans na udział w Australian Open, czy też był to zwykły błąd systemu? Dzisiaj trudno to stwierdzić.

Ciekawym aspektem w tej historii są także identyfikatory testów oraz elementy kodów QR. Zacznijmy od identyfikatorów. Pierwszy test posiada numer 7371999-259039. Pierwsza część to najprawdopodobniej kolejne ID, a druga to oznaczenie pacjenta – takie wnioski można wyciągnąć na podstawie analizy innych testów. Jednak kiedy przeanalizujemy numer drugiego testu:

7320919-259039, sprawy przestają być takie oczywiste, ponieważ pomimo faktu, że drugi test wykonany był sześć dni później, ma wcześniejszy identyfikator. Dodatkowym smaczkiem są znaczniki czasu (ang. *timestamp*), występujące na początku kodu zapisanego w formie QR. *Timestamp*, który został zapisany w formie czasu uniksowego (ang. *Unix epoch time*), czyli liczby sekund, które upłynęły od 1 stycznia 1970 roku UTC, dla drugiego testu się zgadzał – środa, 22 grudnia 2021 16:43:12 GMT. W wypadku pierwszego testu był to jednak nie 16 grudnia, ale niedziela 26 grudnia 2021 14:21:20 GMT (rysunek 50[28]).



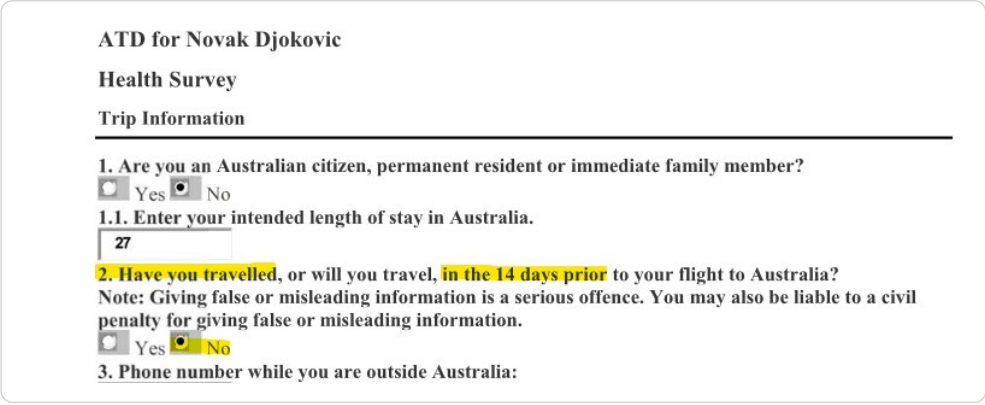
Rysunek 50. Dane dotyczące testu Novaka Djokovicia

Może to być związane z ponownym generowaniem timestampów[29] w momencie pobierania kodu QR z serwera, jednak trudno jest jednoznacznie wyjaśnić, dlaczego identyfikator drugiego testu jest niższy od identyfikatora pierwszego

testu, i to aż o ponad 50 tysięcy, a wszystko wskazuje na to, że identyfikatory są nadawane sekwencyjnie. Być może jednak „pierwszy" test został wykonany 26 grudnia 2021 roku, co zgadzałoby się z całkowitą liczbą wykonanych w tym momencie w Serbii testów…

Mnie osobiście dodatkowo zastanawia końcówka identyfikatora pierwszego testu – 999, która może oznaczać (ale wcale nie musi!) ostatni dostępny numer z danej puli, przydzielonej laboratorium, co mogłoby wskazywać, że starano się nadać temu konkretnemu testowi numer, który na pewno się nie zdubluje. Ale to tylko domysły, a wyciąganie wniosków należy do organów za to odpowiedzialnych.

Dokumenty[30] związane z przylotem Djokovicia do Australii wykazują więcej nieścisłości. Jako data drugiego testu figuruje tam 22 grudnia, jednak może to być zwykła pomyłka. Inne dokumenty[31], tym razem już dotyczące oczekiwania na wyjaśnienie sprawy niewpuszczenia tenisisty, pokazują, że podane przez niego (lub jego agenta) informacje o niepodróżowaniu w ciągu dwóch tygodni poprzedzających przylot do Australii (rysunek 51) także są nieprawdziwe (w odróżnieniu od deklaracji z wcześniej wspomnianych dokumentów, gdzie jest mowa o pobycie w Hiszpanii).



ATD for Novak Djokovic

Health Survey

Trip Information

1. Are you an Australian citizen, permanent resident or immediate family member?

○ Yes ◉ No

1.1. Enter your intended length of stay in Australia.

27

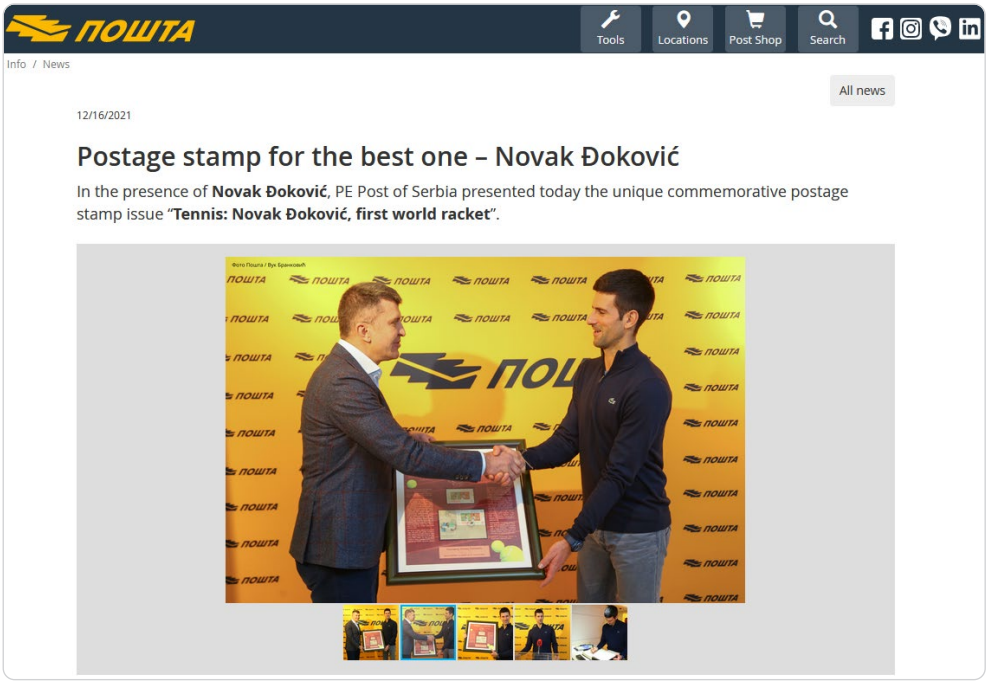
2. Have you travelled, or will you travel, in the 14 days prior to your flight to Australia?
Note: Giving false or misleading information is a serious offence. You may also be liable to a civil penalty for giving false or misleading information.

○ Yes ◉ No

3. Phone number while you are outside Australia:

Rysunek 51. Fragment jednego z dokumentów wypełnianych przed przylotem do Australii

W artykule zamieszczonym w serwisie Brigada Osint autor Aimery Parekh wskazuje na jeszcze jeden aspekt. Skoro test, który dał wynik pozytywny, został wykonany 16 grudnia, to w kolejnych dniach Djoković powinien przebywać na kwarantannie. Jak jednak sam przyznał na swoim koncie w serwisie Twitter[32] (rysunek 52), był w tym czasie na uroczystej prezentacji znaczków ze swoją podobizną, wyemitowanych przez serbską Pocztę.



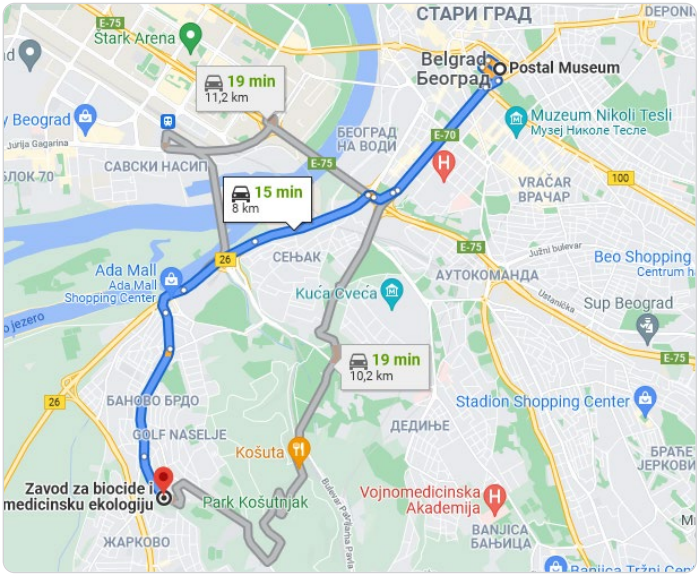
Rysunek 52. Strona serbskiej poczty z informacją o spotkaniu z Novakiem Djokoviciem 16 grudnia 2021 roku

Weryfikując datę spotkania na stronie fundacji Djokovicia oraz Poczty[33], możemy stwierdzić, że miało to miejsce 16 grudnia, a więc tego samego dnia, co test. Spróbujmy zatem skorelować czas wykonania testu (13:05:12 – zakładam, że czasu lokalnego, skoro certyfikat jest serbski) z czasem wykonania zdjęć z prezentacji.

Na stronie Poczty zdjęcia pozbawione są metadanych, ale wyszukanie tych samych zdjęć na innych stronach prowadzi do pełnego zdjęcia, które nie zostało ich pozbawione. Oczywiście nie można im wierzyć w stu procentach, ale to zawsze jeden z wielu tropów, które należy wziąć pod uwagę. Zdjęcie w polu DateTimeOriginal ma wartość 2021:12:16 14:49:21 (zakładam także czas lokalny, skoro fotograf jest z serbskiej agencji). Dodatkowo na jednym ze zdjęć widać zegarek Novaka Djokovicia (prawdopodobnie Hublot Big Bang Meca-10 Blue Ceramic), który wydaje się wskazywać podobną godzinę (wskazówka minutowa jest nieco zasłonięta, co sprawia wrażenie, że jest wskazówką krótszą – godzinową; rysunek 53).

Rysunek 53. Wskazanie czasu na zegarku Novaka Djokovicia ze zdjęcia wykonanego w czasie prezentacji znaczków i opublikowanego przez Post of Serbia

Można stąd wysnuć wniosek, że tenisista przyjechał na miejsce prezentacji, tzn. do Muzeum Poczty w Belgradzie, prosto z laboratorium w instytucie Zavod Za Biocide i Medicinsku Ekologiju, gdzie wykonywany był test. Przejazd samochodem z jednego miejsca do drugiego zajmuje co najmniej 15 minut (rysunek 54), więc jest to zadanie wykonalne.



Rysunek 54. Trasa wytyczona przez Google Maps z laboratorium w instytucie Zavod Za Biocide i Medicinsku Ekologiju do Muzeum Poczty w Belgradzie

Czy jednak Djoković miał już wtedy podejrzenia, że wynik może być pozytywny? Czy wynik na pewno był pozytywny? Po co robił test, skoro dwa wyniki negatywne nie dawałyby mu możliwości pojawienia się w Australii? Dlaczego poszedł na prezentację w miejscu publicznym, skoro oczekiwał na wynik testu, być może pozytywny? Te pytania najprawdopodobniej pozostaną bez odpowiedzi.

Jak widać, publiczny dostęp do dokumentacji oraz informacji różnego typu publikowanych przez wiele osób w Internecie daje ogromne możliwości weryfikacji zdarzeń i wygłaszanych tez. Z jednej strony można by stwierdzić, że to godzi w prywatność, z drugiej zaś – często sami zainteresowani publikują tyle danych (nie tylko w mediach społecznościowych), że OSINT polega w tych przypadkach jedynie na odpowiednim skatalogowaniu informacji i połączeniu faktów.

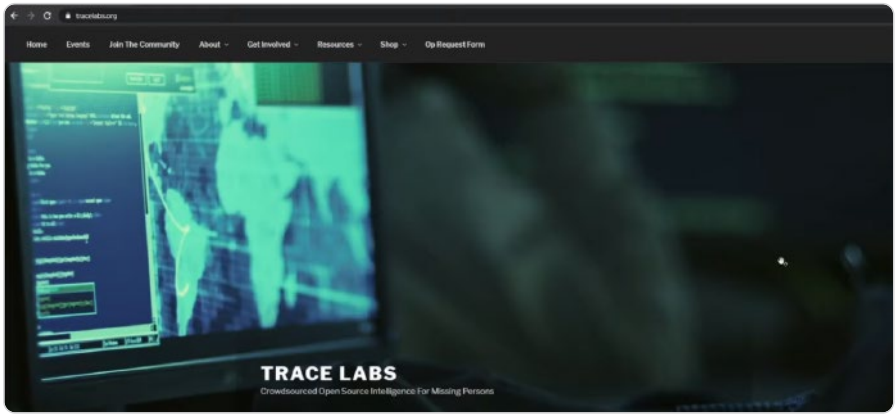
Podsumowanie i rady

Nie tylko w przypadku testów i certyfikatów COVID-owych, ale w każdej dziedzinie życia publicznego możliwa jest weryfikacja wątpliwych dowodów i wydarzeń na podstawie informacji ogólnodostępnych w sieci. W każdym badaniu należy uważać na utarte szlaki, jakimi podążają myśli, gdyż łatwo dojść do wniosków opartych na przekonaniach, dotychczasowych doświadczeniach i emocjach, a nie na faktach. Trzeba zawsze dążyć do weryfikacji informacji na podstawie jak największej liczby niezależnych źródeł, aby uniknąć pomyłek.

R9 #OSINTFORGOOD, CZYLI ŚLEDZTWA W SŁUSZNEJ SPRAWIE

OSINT, czyli umiejętność wykorzystania narzędzi i technik poszukiwania informacji w ogólnodostępnych źródłach, można zastosować zarówno do prywatnych celów, jak i do celów służących ogółowi, hobbystycznie i zawodowo, ze złych lub dobrych pobudek.

W tym rozdziale zajmę się szczególnym przypadkiem: śledztwami prowadzonymi po to, aby pomóc osobom, które szukają zaginionych bliskich, lub tym, które stały się ofiarami przemytu i handlu ludźmi (rysunek 55).



Rysunek 55. Jedną z najszerzej znanych organizacji prowadzących śledztwa OSINT-owe w celu poszukiwania zaginionych osób jest Trace Labs

Odczarowywanie OSINT-u

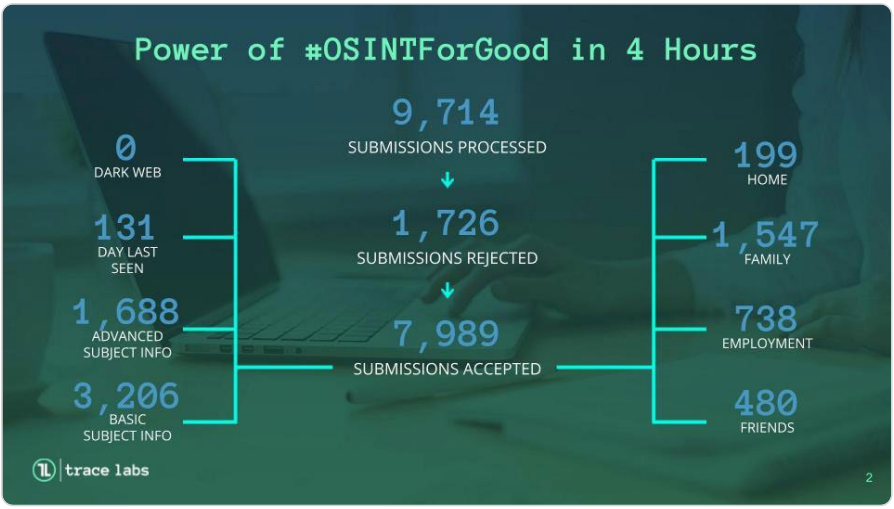
OSINT, zwany także niekiedy „białym wywiadem", najczęściej kojarzy się z działaniami wymierzonymi w ujawnienie tajemnic dostępnych w odmętach Internetu, a skrywających działania różnych organizacji, rządów i służb. Coraz częściej jednak bywa „odczarowywany" przez organizacje wykorzystujące umiejętności poszukiwaczy ogólnodostępnych informacji do pomagania organom ścigania w wyjaśnianiu spraw, które być może bez takiej pomocy utknęłyby w martwym punkcie z powodu braku możliwości technicznych i personalnych.

Jedną z nich jest Trace Labs, kanadyjska organizacja *non profit*, której udało się zamienić takie śledztwa w formę CTF (Capture The Flag), czyli *de facto* konkursu, w którym flagami są wszelkie informacje o faktycznie zaginionych osobach. Wyniki są następnie przekazywane organom ścigania, co uzupełnia posiadane przez nie informacje i przybliża śledczych do odnalezienia poszukiwanych osób (rysunek 56).

Do tej pory organizacja Trace Labs zorganizowała już ponad kilkadziesiąt wydarzeń The Search Party CTF[34], w których uczestnicy pomagali rozwiązać kilkaset spraw z całego świata*. Należy tutaj jednak zaznaczyć, że konkursy tego typu mają kilka zasad i uczestnicy muszą przestrzegać ich nie tylko w celu zdobycia jak największej liczby punktów i, co za tym idzie, zajęcia jak najwyższego miejsca w danej edycji, ale także pozostania niewykrytym. Jest to chyba najważniejsza z zasad, która zakazuje jakiegokolwiek kontaktu z osobami będącymi obiektem śledztwa lub mającymi z nim jakiś związek.

Służy to, po pierwsze, niekomplikowaniu dochodzeń, które prowadzą organy ścigania, gdyż tworzenie dodatkowych powiązań poprzez komunikowanie się z weryfikowanymi osobami lub jakiekolwiek interakcje z udostępnianymi przez nie informacjami, np. w mediach społecznościowych (jak komentowanie lub lajkowanie), może niepotrzebnie wprowadzić konieczność weryfikacji tych informacji przez śledczych. Po drugie, takie działania mogą mieć negatywny wpływ na odczucia rodzin, poszukujących wszelkich informacji o swoich bliskich. Za interakcję, ale też za próby ataków na konta (np. poprzez reset hasła lub nawet odwiedzenie strony do tego służącej), grozi natychmiastowa dyskwalifikacja. To samo dotyczy korzystania z baz danych zawierających hasła, np. z wycieków. Zarówno uczestnicy, jak i sama organizacja nie starają się w żaden sposób wyciągać wniosków czy snuć teorii na temat poszukiwanych. Ich jedynym zadaniem jest zgromadzenie i przekazanie jak największej ilości informacji. To oczywiście tylko podstawowe zasady.

* Jego ostatnia edycja przed publikacją tej książki miała miejsce 27 stycznia 2024 roku.



Rysunek 56. Liczba zgłoszonych flag z podziałem na kategorie – infografika z jednej z ostatnich edycji The Search Party CTF organizowanej przez Trace Labs

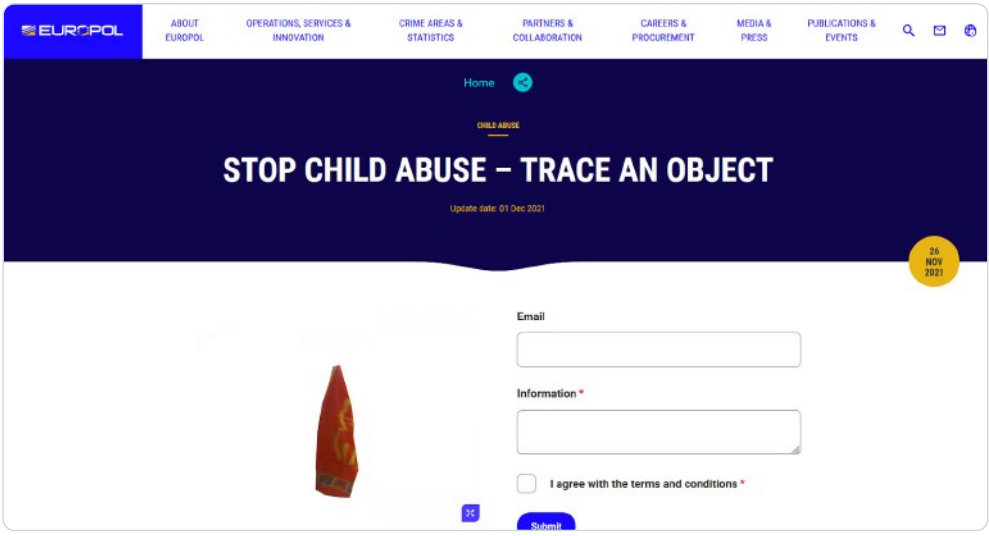
Każdy, kto chce zostać uczestnikiem takiego wydarzenia, musi nie tylko poznać je i przyswoić jego zasady, ale także zarejestrować się poprzez wykupienie płatnej wejściówki i dołączyć do zespołu. Zespoły są maksymalnie czteroosobowe, ale oczywiście mogą zawierać mniejszą liczbę uczestników, chociaż ze względu na ilość informacji, które trzeba wyszukać, zweryfikować, skategoryzować i zgłosić do sędziów (oraz ewentualnie konieczność dyskusji z nimi na tematy, w których mamy odmienne zdanie co do punktacji), najlepszym wyborem jest pełny zespół. Punkty są przyznawane według kategorii, np. za zidentyfikowanie informacji dotyczących znajomych poszukiwanej osoby, takich jak: nicki w portalach czy mediach społecznościowych, numer jej telefonu albo adres, dostaniemy jedynie 50 punktów, ale już za informacje dotyczące miejsca, w którym dana osoba była widziana po zaginięciu, będzie to 700 punktów, natomiast za informacje o aktualnym miejscu jej przebywania (lub informacje, dzięki którym można je ustalić) przyznawana jest maksymalna stawka – 5000 punktów. Należy mieć jednak na uwadze fakt, że śledztwa zazwyczaj dotyczą osób spoza Unii Europejskiej, np. z USA czy Australii, gdzie nie obowiązują zasady RODO, więc i sposób poszukiwania zaginionych odbywa się na nieco innych zasadach. Prowadząc śledztwo np. w USA, można skorzystać z ogromnej bazy źródeł publicznych, które rodzimych administratorów i inspektorów danych osobowych przyprawiłyby o zawrót głowy.

W The Search Party CTF uczestniczą entuzjaści OSINT-u z całego świata i każdy po przygotowaniu sobie środowiska do prowadzenia tego typu poszukiwań jest w stanie zarejestrować się i wziąć w nim udział. Ważne jest także przeszkolenie w zakresie technik poszukiwania osób, gdyż często za sukces odpowiada

znajomość narzędzi (dotyczących weryfikacji tego, co mogło się stać z zaginioną osobą i jakie powszechnie dostępne dane na to wskazują), które na co dzień nie są wykorzystywane w działaniach OSINT-owych.

Działania na rzecz dzieci

Jeśli ktoś chce się jednak zaangażować w przedsięwzięcia spod znaku #OSINTForGood, nie musi czekać na konkretne wydarzenia, a może to uczynić w każdej chwili, odwiedzając stronę Europolu i dołączając do poszukiwań w ramach inicjatywy Stop Child Abuse – Trace An Object (rysunek 57), która – jak sama nazwa wskazuje – ma na celu walkę z przemocą wobec dzieci i polega na dostarczeniu informacji o pochodzeniu, aktualnym rynku sprzedaży lub występowaniu ukazanych na zdjęciach fragmentów odzieży czy sprzętu.



Rysunek 57. Strona Stop Child Abuse – Trace An Object z wycinkiem zdjęcia przedstawiającym przedmiot do zidentyfikowania

Tak samo jak w przypadku CTF-a, wszystkie takie informacje są przekazywane do organów ścigania i mogą pomóc w przyspieszeniu śledztw. Zgodnie z danymi opublikowanymi na stronach Europolu dotychczas (a inicjatywa działa od 2017 roku), dzięki ponad 26 tysiącom wskazówek od internautów, w 105 przypadkach udało się określić bliższe dane obiektów, a podobny program został także uruchomiony przez australijską policję dla obszaru Azji i Pacyfiku (rysunek 58)[35].

Rysunek 58. Australijska wersja portalu wykorzystywanego do wspólnej identyfikacji przedmiotów przez użytkowników Internetu

Jeśli już jesteśmy przy działaniach na rzecz dzieci, to należy jeszcze wspomnieć o fundacji The Innocent Lives Foundation. Pomaga ona zwalczać przemoc wobec dzieci dzięki współpracy wielu osób angażujących się w poszukiwania z wykorzystaniem technik OSINT-owych prawdziwych tożsamości anonimowych internetowych oprawców. Wśród aktywnych w sieci organizacji jest też chociażby amerykańska NCPTF (National Child Protection Task Force), która dzięki współpracy wielu ekspertów w różnych dziedzinach wspiera, jak sama wskazuje, niedostatecznie dofinansowane służby porządkowe.

Bellingcat

W nieco innym zakresie, ale jakże ważnym, działa Bellingcat – niezależna grupa dziennikarzy, śledczych i badaczy z różnych krajów, która dzięki wykorzystaniu ogromu informacji, jakie codziennie trafiają do Internetu za sprawą jego użytkowników na całym świecie, wydobywa na światło dzienne szczegóły spraw dotyczących m.in. konfliktów zbrojnych czy łamania praw człowieka. Nazwa „Bellingcat" jest nawiązaniem do starej bajki, w której myszy debatują nad tym, co zrobić, żeby nie zagrażał im kot – i w końcu postanawiają przyczepić mu dzwonek, aby go w porę usłyszeć. Kiedy jednak szukają wśród siebie kogoś do wykonania tej misji, okazuje się, że chętnych nie ma już tak wielu, jak tych zgłaszających pomysły. Ideą Bellingcat jest pokazywanie, jak możliwości wynikające z analizowania informacji pojawiających się w Internecie przekuć w faktyczne rezultaty. Jednymi z najbardziej znanych śledztw Bellingcat, wykorzystujących dane zebrane w sieci, są przypadek zestrzelenia lotu MH17[36] nad Ukrainą i monitorowanie przestrzeni powietrznej Kazachstanu[37].

Każdy może pomóc

To oczywiście tylko wybrane przykłady możliwego wykorzystania OSINT-u do pomocy innym. Organizacji poszukujących wsparcia w tego typu inicjatywach, zarówno na poziomie globalnym, jak i lokalnym, jest więcej – i naprawdę trudno byłoby mi tutaj wszystkie wymienić. Każdy może włączyć się w pomoc, chociażby wyszukując ogłoszenia o potrzebnym wsparciu wolontariuszy lub śledząc aktualne informacje o poszukiwanych osobach (z użyciem frazy „policja prosi o pomoc" lub „zaginął"/„zaginęła" w Google). Użytkownicy serwisu Reddit mają nawet swoje podforum do spraw z tej kategorii: RBI: Reddit Bureau of Investigation.

Przeglądanie Google Maps (rysunek 59) także może okazać się przydatne, gdyż można tam natrafić na zdjęcie poszukiwanego od dawna bossa włoskiej mafii, który ukrywa się przed policją[38].

Rysunek 59. Google Street View także może być narzędziem OSINT-owym

Możemy też natknąć się na zatopiony samochód[39] (rysunek 60), w którym odnaleziono pozostałości ciała mężczyzny zaginionego bez śladu ponad 20 lat temu. Nawet oglądanie kanałów kulinarnych na YouTube okazuje się bardziej pożyteczne, niż można byłoby się spodziewać, skoro – pomimo braku widocznej twarzy – doprowadziło do zidentyfikowania poszukiwanego członka włoskiej mafii na podstawie dość oryginalnych tatuaży[40], które eksponował, pokazując na swoim kanale sposoby przyrządzania włoskich potraw.

Rysunek 60. Zatopiony samochód widoczny w Google Earth

W każdym przypadku należy jednak pamiętać o tym, że za poszukiwania odpowiedzialne są organy ścigania i nam nie wolno wyciągać żadnych wniosków, ani tym bardziej ich formułować w Internecie, gdyż zbyt pochopnie wysunięte oskarżenia mogą doprowadzić do samosądów. Są przypadki potwierdzające, że kosztowały one już zdrowie, a nawet życie niewinnych osób (przykłady zostały podane w rozdziale *O jeden OSINT za daleko, czyli przykre skutki złych analiz*, s. 132–137). Jeśli zauważymy niepokojące treści, to w ogromnej większości przypadków możemy je zgłosić właścicielom danego serwisu, gdyż coraz więcej z nich przy wyświetlanych filmach lub innych materiałach udostępnia taką możliwość.

Niestety, wiele tego typu „społecznych śledztw", z wytypowanym z góry sprawcą, jest bezrefleksyjnie udostępniane w Internecie, a newsy, które wyzwalają nagłe emocje, jak np.: „Zobacz, co stało się z tym dzieckiem w markecie", są bardzo często elementem phishingu i mogą nas pozbawić (w najlepszym przypadku) dostępu do konta na Facebooku, ale i – w skrajnym przypadku – oszczędności w banku.

Podsumowanie i rady

Wiele organizacji wykorzystuje OSINT jako narzędzie do niesienia pomocy – warto sprawdzić, czy nie potrzebują wolontariuszy, np. w dziedzinie OSINT-u. Każdy, kto ma chociażby podstawową wiedzę z zakresu korzystania z narzędzi i technik OSINT-owych, może się zaangażować, jednak poszukiwanie osób wymaga dodatkowego przygotowania pod kątem specyficznych technik.

Podczas poszukiwań osób jedną z najważniejszych zasad jest pozostanie anonimowym, niewykrytym i prowadzenie jedynie pasywnego rekonesansu. Weryfikacja informacji publikowanych codziennie w sieci może doprowadzić do rozwiązania wielu dotychczas niewyjaśnionych spraw – warto sprawdzać to, co się widzi.

UWAGA | Odpowiedzialne za prowadzenie śledztw i formułowanie oskarżeń są zawsze organy ścigania – samosądy i pochopnie wyciągane wnioski mogą doprowadzić do tragedii.

R10 #F12ISNOTACRIME, CZYLI OPOWIEŚĆ O ZAGLĄDANIU W KOD ŹRÓDŁOWY

Chociaż śledztwa OSINT-owe z wykorzystaniem metod wizualnych, takich jak badanie zawartości zdjęć czy map, są bardzo spektakularne, to analiza kodów źródłowych stron internetowych także może dawać ciekawe rezultaty. W tym rozdziale przyjrzymy się nieco bliżej temu, co możemy znaleźć w kodzie i jak to wykorzystać.

Rysunek 61 przedstawia prześmiewczą wersję okładki w stylu serii książek o tematyce IT. Ciekawe, ile z patrzących osób w ciągu pierwszych 5 sekund zorientuje się, że coś tu nie gra.

Rysunek 61. Prześmiewcza wersja okładki w stylu serii książek o tematyce IT

Ku przestrodze

Zacznę jednak od historii będącej dla niektórych źródłem wątpliwości, czyli od pytania, czy można zaglądać do „wnętrza" stron i portali w Internecie bez obawy o konsekwencje. Na początku października 2021 roku Josh Renaud, dziennikarz gazety „St. Louis Post-Dispatch" z Saint Louis w stanie Missouri, odkrył[41], że z kodu źródłowego strony stanowego Departamentu Edukacji Podstawowej i Ponadpodstawowej (DESE) można odczytać ponad 100 tysięcy numerów ubezpieczenia społecznego (SSN – Social Security Numbers) należących do nauczycieli. Dla uproszczenia można powiedzieć, że te dziewięciocyfrowe identyfikatory to amerykańskie odpowiedniki numerów PESEL.

Dziennikarz zgłosił ryzyko wycieku danych do DESE i opublikował artykuł informujący o tym incydencie, kiedy problem został usunięty. Niedługo po tym, zamiast podziękowań, spotkała go niemiła niespodzianka: gubernator Mike Parson wystąpił z oświadczeniem, że był to hacking – i domagał się wyciągnięcia

konsekwencji prawnych wobec dziennikarza (rysunek 62). W wypowiedzi komisarz ds. edukacji Margie Vandeven na ten temat pojawiła się nawet informacja, że dane nauczycieli zostały „odszyfrowane" z kodu strony. Trudno w tej chwili powiedzieć, czy chodziło tutaj o samo odczytanie informacji ze źródła strony i to nazwane zostało „odszyfrowaniem", czy też faktycznie do ich przechowywania zastosowano np. kodowanie Base64. Niemniej w żadnym z tych przypadków nie można *de facto* mówić o szyfrowaniu, a co najwyżej o zmianie formy zapisu danych. Base64 jest często wykorzystywany do kodowania informacji w Internecie ze względu na przedstawienie wszystkich bajtów za pomocą znaków ASCII, co ułatwia np. przekazywanie dowolnych wartości w adresach URL bez obawy o problemy związane z kodowaniem znaków.

Rysunek 62. Gubernator Mike Parson o „konwertowaniu i dekodowaniu kodu" strony internetowej (wpis na Twitterze)

Po kompromitujących wypowiedziach gubernatora Parsona na sile przybrała akcja z hasztagiem #F12IsNotACrime, czyli „F12 to nie przestępstwo". F12 to klawisz, którego naciśnięcie otwiera w ogromnej większości przeglądarek internetowych narzędzia deweloperskie, umożliwiające podejrzenie nie tylko kodu źródłowego strony, ale także informacji dotyczących błędów, przesyłanych mediów, ciasteczek i innych danych, również na temat wydajności strony.

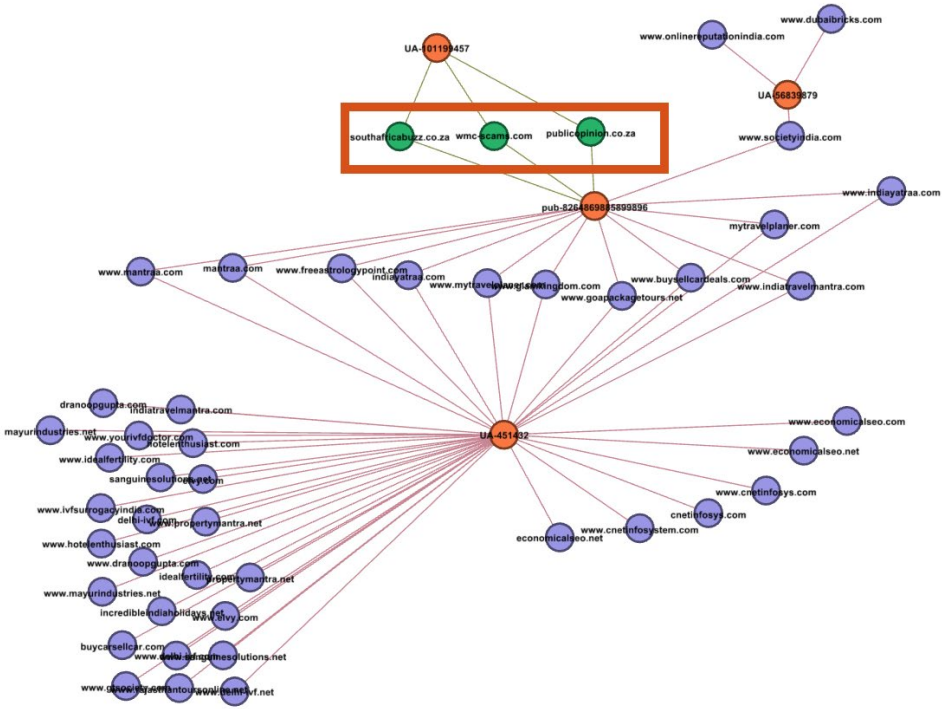
Innym przypadkiem, kiedy w kodzie strony umieszczono informacje, które nie powinny być ogólnodostępne, jest wydarzenie o pół roku wcześniejsze[42]. Wówczas to holenderskie Stowarzyszenie Gmin Niderlandów (VNG) musiało zdjąć stronę internetową *opeventuitslag.nl* ze względu na możliwość podglądu frekwencji i rezultatów wyborów parlamentarnych, właśnie dzięki przeglądaniu kodu źródłowego.

Kod strony może być kopalnią danych także podczas śledztwa OSINT-owego. Jedną z informacji, którą można w ten sposób uzyskać, jest identyfikator konta Google czy Microsoft, o czym pisałem w rozdziale *Pasywny rekonesans kont Google i Microsoft* (s. 35–40). W ramach sekurakowych szkoleń OSINT master, prowadzonych przez Securitum, także niejednokrotnie zaglądamy do źródeł witryn w Internecie.

Identyfikatory Google Analytics

Przykładem interesujących elementów zawartych w kodzie wielu stron są identyfikatory Google Universal Analytics. Usługa tego typu pozwala właścicielom witryn śledzić statystyki dla wybranych stron. Jeden identyfikator może być wykorzystywany na różnych stronach i w różnych domenach, dzięki czemu umożliwia powiązanie danej witryny z innymi, co z kolei może znacznie ułatwić ustalenie powiązań danego serwisu z konkretnymi osobami. Identyfikator konta w Google Analytics ma postać: `UA-XXXXXXXX`, a w formie z dodanym na końcu numerem usługi wygląda następująco: `UA-XXXXXXXX-Y` (X i Y oznaczają dowolną cyfrę). Warto wspomnieć, że od 1 lipca 2023 usługi Universal Analytics przestały przetwarzać dane oraz aktualizować raporty i są aktualnie zastępowane przez nowsze rozwiązanie – Google Analytics 4 (GA4) z identyfikatorami rozpoczynającymi się od `G-`.

W 2017 roku w RPA właśnie dzięki analizie Google Analytics ID dziennikarzowi Janowi Cronjé udało się wpaść na trop[43] prowadzący do właściciela stron związanych z teorią o powstrzymywaniu przemian w Afryce Południowej, znanych jako narracja *white monopoly capital*. W śledztwie, oprócz Google Analytics, ważne okazały się także identyfikatory Google Adsense (usługi reklam kontekstowych od Google; rysunek 63*).



Rysunek 63. Powiązania domen w ramach południowoafrykańskiego śledztwa

* Rys. Justin Seitz.

Aby sprawdzić, czy można prześledzić powiązania na podstawie powyższego identyfikatora, zajrzymy w kod strony serwisu „The Guardian”. Po naciśnięciu klawisza F12 lub wybraniu opcji pokazania źródła strony z menu kontekstowego (dostępnego po naciśnięciu prawego przycisku myszy na stronie, najlepiej poza elementami graficznymi) możemy w pole wyszukiwania wpisać ciąg znaków UA-, co wskaże miejsca, w których znajduje się poszukiwany identyfikator. Do dalszej analizy można wykorzystać serwisy SpyOnWeb lub DNSlytics, które na podstawie podanego identyfikatora zwrócą nam listę powiązanych serwisów internetowych. Zawsze warto jednak pamiętać, by nie ufać ślepo otrzymanym wynikom, chociażby dlatego, że taki ciąg znaków w kodzie swojej strony może umieścić każdy, kto ma władzę nad serwerem.

Na stronie „The Guardian” ciekawą zawartość ma jeszcze jeden element, na który także warto zwracać uwagę podczas poszukiwań OSINT-owych. Są to komentarze pozostawione przez twórców serwisu – czy to w celu ułatwienia sobie pracy, czy też przez roztargnienie. Mogą się w nich znaleźć wskazówki dotyczące wyłączonych lub jeszcze niedostępnych stron, informacje o technologii użytej do wykonania strony albo dane dostępowe lub osobowe. Oczywiście w kodzie strony będą widoczne tylko komentarze umieszczone w elementach HTML – jeśli kod strony pisany jest np. w PHP, to komentarze z kodu nie znajdą się w wynikowym kodzie strony (chyba że specjalnie je tam umieścimy). Na rysunku 64 widać, że w kodzie strony zawarte zostało ogłoszenie skierowane do osób, które wiedzą, jak ten kod wyświetlić – i wpadną na to, by to zrobić.

```

<!DOCTYPE html>
<html id="js-context" class="js-off is-not-modern id--signed-out" lang="en" data-page-path="/international">


    <head>



<!--
     __        __                  _     _      _
     \ \      / /__    __ _ _ __ ___  | |__ (_)_ __(_)_ __   __ _
      \ \ /\ / / _ \  / _` | '__/ _ \ | '_ \| | '__| | '_ \ / _` |
       \ V  V /  __/ | (_| | | |  __/ | | | | | |  | | | | | (_| |
        \_/\_/ \___|  \__,_|_|  \___| |_| |_|_|_|  |_|_| |_|\__, |
                                                            |___/
    Ever thought about joining us?
    https://workforus.theguardian.com/careers/product-engineering/
     --->



<title>News, sport and opinion from the Guardian's global edition | The Guardian</title>



<meta charset="utf-8">

    <meta name="description" content="Latest international news, sport and comment from the Guardian" />

```

Rysunek 64. Ogłoszenie w kodzie strony internetowej „The Guardian”

Nie wiadomo, jaka przyszłość czeka Google Analytics w Europie, gdyż w toczącej się od lat batalii europejskich organów ochrony danych nastąpił przełom i austriacki Urząd Ochrony Danych wydał decyzję dotyczącą łamania

postanowień RODO przez Google. Wynika to z faktu, że dane z Google Analytics są przesyłane poza obszar Unii Europejskiej. Czy zatem Google zmieni konfigurację tak, żeby dane trafiały na serwery europejskie, czy też odetnie Europejczyków od tej usługi – czas pokaże.

W kodach źródłowych stron można znaleźć jeszcze wiele innych ciekawych informacji. O nich jednak opowiem innym razem. I pamiętajcie: #F12IsNotACrime.

Podsumowanie i rady

- Każdy może zajrzeć w kod źródłowy strony internetowej, więc wszystkie informacje tam zawarte należy traktować tak, jak gdyby znajdowały się na stronie. Taka jest idea działania WWW.
- Często informacje dostępne w kodzie źródłowym, takie jak identyfikatory śledzenia lub komentarze, mogą wskazać faktycznego autora lub właściciela witryny.
- Nie wszystko jest zapisane tekstem jawnym, niezakodowanym, niekiedy trzeba odkodować dane z Base64.
- Dobrze jest też znać notację JSON (JavaScript Object Notation), czyli tekstowy format zapisu danych strukturalnych (np. tablic, obiektów itp.), ułatwiający ich wymianę. Jest stosunkowo prosty do wygenerowania i odczytania w dowolnym języku programowania, a także, przez swoją tekstową reprezentację, możliwy do analizy przez człowieka bez użycia dodatkowych narzędzi.
- Warto umieć modyfikować parametry przekazywane metodą `GET` w URL-ach.

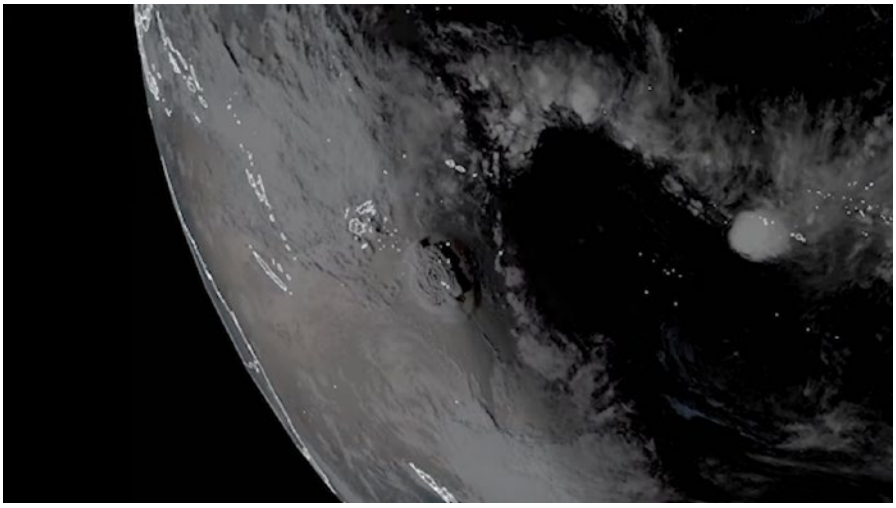
R11 WIELKI BRAT PATRZY, CZYLI OSINT Z WYKORZYSTANIEM ZDJĘĆ SATELITARNYCH

Dzięki rosnącej liczbie satelitów, udostępniających zdjęcia wykonane z orbity, mamy na co dzień możliwość sięgnięcia do ogromnej bazy ogólnodostępnych informacji na temat praktycznie każdego zakątka Ziemi. Tym samym możemy weryfikować i poddawać analizie to, co przekazują nam media, nie ruszając się nawet sprzed komputera. Znacząca część tych zdjęć dostępna jest w Internecie zupełnie za darmo, choć jeśli chcemy uzyskać większą szczegółowość obrazu, musimy liczyć się z większymi lub mniejszymi opłatami.

Tam sięgaj, gdzie wzrok nie sięga

22 stycznia 2022 roku w okolicy archipelagu wysp Tonga na Oceanie Spokojnym wybuchł podwodny wulkan Hunga Tonga Hunga Ha'apai. Erupcja ta, określana jako jedna z największych zarejestrowanych zdarzeń tego typu

w ciągu ostatnich kilkudziesięciu lat, była tak duża, że słyszano ją nawet na Alasce, a powietrzna fala uderzeniowa została zarejestrowana m.in. na Kasprowym Wierchu. Dzięki ogromnej ilości materiału przesłanego przez satelity mogliśmy dokładnie prześledzić[44] (rysunek 65), jak wyglądał ten wybuch i jakie były jego konsekwencje[45].



Rysunek 65. Widok wybuchu wulkanu Hunga Tonga Hunga Ha'apai przesłany przez satelity NOAA (National Oceanic & Atmospheric Administration)

Jednak nie tylko nagłe zdarzenia geologiczne czy pogodowe można zweryfikować z wykorzystaniem do tego zdjęć satelitarnych. Kolejnym procesem, który pozwalają prześledzić, jest długotrwała zmiana klimatu. Zmiany w typie roślinności i zalesieniu wybranych obszarów Ziemi czy zmniejszająca się ilość wody w zbiornikach wodnych i rzekach dostarczają wielu informacji o faktycznych zjawiskach zachodzących na planecie.

Najprościej jest to zaobserwować z wykorzystaniem aplikacji **Google Earth Pro** (w wersji desktopowej, nie przeglądarkowej, ponieważ udostępnia o wiele więcej funkcji i możliwości prezentacji danych). Posiada ona funkcjonalność tzw. suwaka czasu do wyboru danych satelitarnych/lotniczych z dostępnych punktów czasowych dla danej lokalizacji. Dzięki temu możemy zobaczyć, jak wyglądały niektóre miasta nawet przed II wojną światową (rysunek 66), i to z zadziwiająco dużą dokładnością. Powojenne zdjęcia są jednak bardzo niewyraźne i dopiero po roku 2000 ich szczegółowość znacząco się poprawiła. W rękach wielu dziennikarzy śledczych to narzędzie jest znakomitą bronią w walce o dotarcie do prawdy na temat wydarzeń z całego świata.

Rysunek 66. Widok w aplikacji Google Earth Pro: Warszawa, 1935 rok

Jednym z celów śledztw wykorzystujących „oczy Wielkiego Brata" jest weryfikacja zdarzeń związanych z konfliktami zbrojnymi (w tym migracjami uchodźców), nielegalnym handlem ludźmi i towarami, celowym lub przypadkowym niszczeniem przyrody, a także katastrofami o dużej skali oddziaływania.

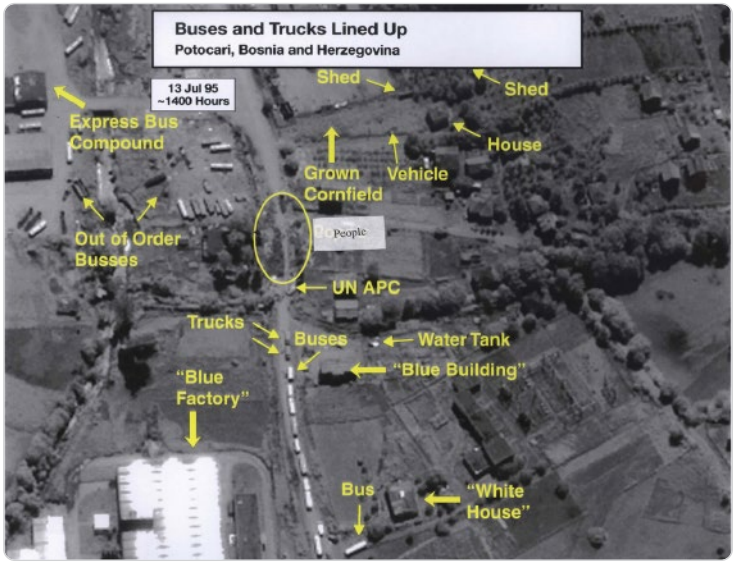
Na podstawie OSINT-owego śledztwa możliwe było zweryfikowanie, co się stało z członkami muzułmańskiej grupy etnicznej Rohingja, zamieszkującej północną część stanu Rakhine w Mjanmie (czyli we wcześniejszej Birmie). Dane satelitarne dostępne w publikacji Human Rights Watch[46] pokazują, że rząd Mjanmy dokonał zniszczenia wiosek Rohingja z użyciem ciężkiego sprzętu. Na zdjęciach wykonanych przed zdarzeniami mającymi miejsce w 2018 roku i po nich widać ich skutki: ślady wiosek, które praktycznie znikły z powierzchni ziemi.

Wizualizacja zmian

Aby zwizualizować skalę zmian w danym miejscu, posłużymy się narzędziem World Imagery Wayback. Pozwala ono zobaczyć zdjęcia satelitarne dla wybranego miejsca, ale jego siłą jest możliwość wyświetlenia zdjęć z dwóch punktów czasowych (w ramach dostępnych dat wykonania zdjęć satelitarnych) na osobnych warstwach i kontrolowania zakresu nakładania się jednego zdjęcia na drugie z wykorzystaniem suwaka (rysunek 67). Takie działanie w znacznie większym stopniu pozwala na uzmysłowienie sobie, co się zmieniło w danym miejscu, niż gdybyśmy oglądali te zdjęcia osobno.

Rysunek 67. Widok jednej ze zniszczonych wiosek w Mjanmie – z lewej strony zdjęcie z 2019 roku, z prawej – z 2017 roku. Całość pokazuje dokładnie to samo miejsce, a suwak pośrodku umożliwia nakładanie jednego zdjęcia na drugie (za: World Imagery Wayback)

Przed erą powszechnego dostępu do tego typu narzędzi weryfikacja zdarzeń możliwa była jedynie dla wojska, które dysponowało zdjęciami wykonanymi przez satelity. Upublicznione w ramach The National Security Archives[47] (rysunek 68[48]) dane pokazują np. działania w okolicach miasta Srebrenica w Bośni i Hercegowinie, gdzie w 1995 roku doszło do masowego ludobójstwa dokonanego przez Siły Zbrojne Republiki Serbskiej.



Rysunek 68. Zdjęcie z miejscowości Potočari (niedaleko Srebrenicy), gdzie stacjonowali holenderscy żołnierze

Wracając jeszcze do Mjanmy, techniki OSINT-owe są cały czas wykorzystywane do śledzenia działań rządowych na tym obszarze. 25 stycznia 2022 roku Benjamin Strick opublikował na Twitterze informację o raporcie[49], który ukazywał szczegóły transportu wozów opancerzonych BRDM-2M z Władywostoku w Rosji do Yangoon w Mjanmie, a dane do jego opracowania uzyskano przy wykorzystaniu tego typu technik. Informacje z serwisu Marine Traffic, pozwalającego śledzić trasy różnych jednostek pływających, potwierdziły, że frachtowiec CAPTAIN YAKUBOVICH znajduje się w porcie w Mjanmie. Informacje o tym, jak statek wygląda, pozyskane z tego serwisu, miały także odzwierciedlenie w zdjęciach, które udało się zrobić fotoreporterom w porcie w Yangoon. Dalsza analiza fotografii ujawniła obecność na jego pokładzie wozów BRDM. Z kolei informacje uzyskane z rejestrów handlu bronią sztokholmskiego instytutu SIPRI[50] potwierdziły kontrakt na dostawę tego typu pojazdów pomiędzy Rosją a Mjanmą.

Mnogość danych

Przedstawione powyżej sprawy to tylko mały wycinek informacji, jakie można uzyskać na podstawie zdjęć satelitarnych. Techniki wykorzystujące ten rodzaj otwartych źródeł danych opierają się nie tylko na analizie obrazów powierzchni Ziemi, ale także innych aspektów, jak analiza źródeł ciepła czy roślinności. Mnogość danych dostępnych na przeróżnych mapach jest ogromna, a jeśli Czytelników interesuje tematyka korzystania z danych geograficznych, to zagadnienia te poruszane są np. na szkoleniu Securitum OSINT/OPSEC.

Obecna sytuacja na świecie jest bardzo dynamiczna i często przedstawiana na tyle różnych sposobów, że trudno jednoznacznie stwierdzić, kto mówi prawdę, a kto się z nią mija. Pod koniec stycznia 2022 roku na portalu NBC News pojawił się artykuł[51], w którym relacjonowano, jak za pomocą nagrań publikowanych na TikToku ludzie na całym świecie, od amatorów śledztw internetowych po zawodowych analityków, mają wgląd w to, co dzieje się na Wschodzie.

Zdjęcia satelitarne w połączeniu z informacjami udostępnianymi przez użytkowników mediów społecznościowych dają obecnie każdemu możliwość weryfikacji tego, co naprawdę dzieje się w danym miejscu na świecie. Zachęcam do korzystania z tych możliwości, głębszej ich analizy i mówienia „Sprawdzam" w sytuacjach, kiedy podejrzewamy, że przedstawione materiały mogą być manipulacją.

Podsumowanie i rady

Wiele zdjęć satelitarnych powierzchni Ziemi jest dostępnych za darmo w Internecie – na stronach serwisów: Google Maps, Bing Maps czy Apple Maps, ale także przez portale związane bezpośrednio z obrazami udostępnionymi przez operatorów satelitów, jak np. Sentinel Hub Playground. Porównanie zdjęć

z dwóch lub więcej punktów czasowych pomaga zweryfikować informacje o przebiegu zdarzeń na danym terenie.

Obecnie dodatkowym sposobem weryfikacji zdarzeń jest porównanie zdjęć satelitarnych ze zdjęciami lub filmami wykonywanymi na Ziemi i zamieszczanymi w mediach społecznościowych. Pozwala to określić (mniej lub bardziej) dokładne położenie autora zdjęcia lub nagrania wideo, a co za tym idzie – miejsce zdarzenia.

R12 ANALIZA CZASOWA Z WYKORZYSTANIEM (NIECO) UKRYTYCH DANYCH

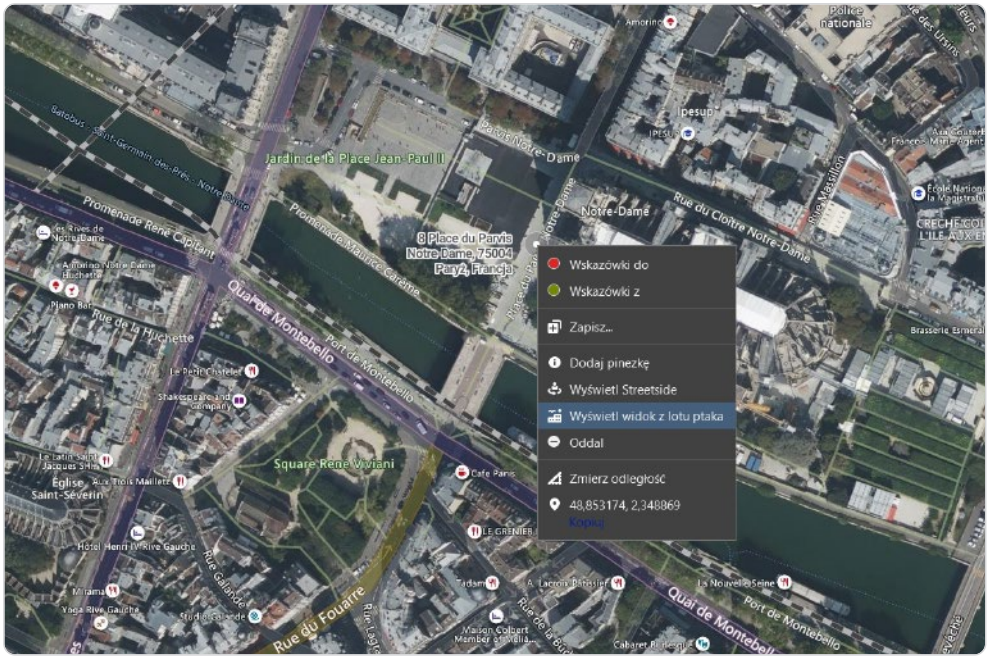
W rozdziale *Wielki Brat patrzy, czyli OSINT z wykorzystaniem zdjęć satelitarnych* (s. 79–84) pisałem o weryfikacji zdarzeń na podstawie zmian widocznych na zdjęciach satelitarnych. Bywa jednak, że serwisy mapowe nie podają informacji na temat czasu wykonania zdjęcia. Jak wtedy stwierdzić, kiedy je zrobiono?

Na szczęście jest na to sposób. Wymaga wprawdzie zagłębienia się nieco w zagadnienia techniczne (a konkretnie: w narzędzia programistyczne w przeglądarce), jednak kiedy już opanujemy tę technikę, będziemy mogli weryfikować nie tylko datę wykonania zdjęcia, ale także inne aspekty czasowe w mediach społecznościowych, jak chociażby moment opublikowania multimediów.

Analiza w Bing Maps

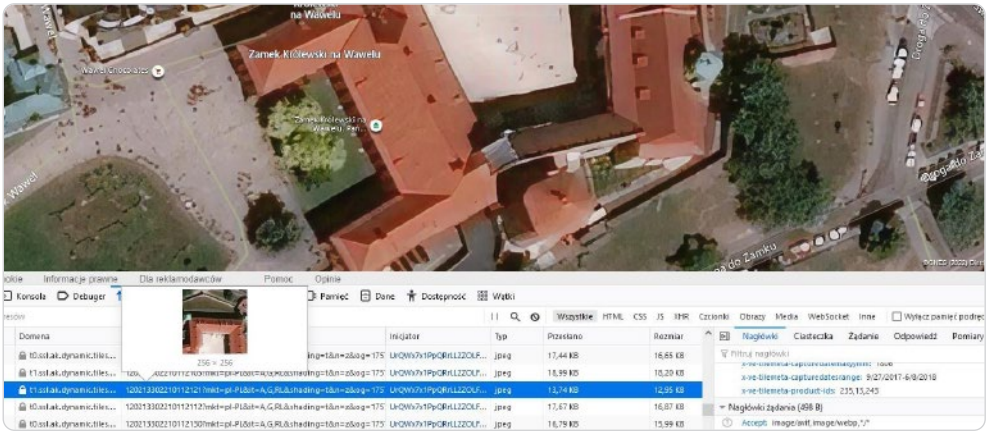
Jednym z serwisów, które nie udostępniają wprost informacji o czasie wykonania zdjęcia, jest Bing Maps. To bliźniacza wersja map Google prezentująca mapy drogowe i satelitarne (zwane tutaj lotniczymi). Dla wybranych miejsc na Ziemi udostępnia także widok z lotu ptaka (rysunek 69), jednak nie są to zdjęcia w pełnym 3D, tak jak w Google, gdzie mamy możliwość zmieniania kąta nachylenia widoku i kierunku, w którym jest on zorientowany.

Dają one za to pewne złudzenie widoku trójwymiarowego poprzez prezentację zdjęć wykonanych pod mniejszym kątem niż zdjęcia lotnicze i możliwość wyboru jednego z czterech ujęć – po jednym dla każdego kierunku geograficznego. Tryb ten włącza się z menu w prawym górnym rogu, jak pozostałe opcje tej mapy, lub z menu kontekstowego, dostępnego po naciśnięciu prawego przycisku myszy na mapie. Jak wspomniałem, nie dla każdego miejsca dostępny jest widok z lotu ptaka – w Europie ta usługa ogranicza się jedynie do większych miast.



Rysunek 69. Sposób włączania widoku z lotu ptaka z menu kontekstowego w Bing Maps

Weryfikacji, z jakiego okresu pochodzą zdjęcia lotnicze i te z lotu ptaka, można dokonać poprzez analizę nagłówków odpowiedzi dla pojedynczego kafelka mapy. W celu ich odczytania należy otworzyć stronę Bing Maps i przejść do jednego ze wspomnianych widoków, a następnie otworzyć narzędzia deweloperskie (DevTools) przez naciśnięcie klawisza F12. Zwiększając przybliżenie widoku mapowego lub przesuwając go, można zauważyć w zakładce SIEĆ (lub NETWORK, w wersji anglojęzycznej) odpowiedzi pochodzące z adresów kończących się na *dynamic.tiles.virtualearth.net* i posiadające w polu TYP rozszerzenie JPEG (Joint Photographic Experts Group). Jeśli ustawimy kursor myszy nad takim żądaniem, powinniśmy zobaczyć podgląd kafelka mapy, który został przesłany w odpowiedzi na nie. Po zaznaczeniu wpisu na liście żądań w oknie poniżej lub po prawej stronie (w zależności od tego, czy panel DevTools mamy ustawiony pionowo czy poziomo) wyświetlają się dodatkowe związane z nim informacje (np. nagłówki). Interesującym nas nagłówkiem będzie `x-ve-tilemeta-capturedatesrange`, pokazujący, jak sama nazwa wskazuje, zakres dat, z których pochodzi dany wycinek. Dodatkowo potwierdza to nagłówek `x-ve-tilemeta-capturedatemaxyymm` – tutaj data sformatowania jest zgodna z opisem zawartym w nazwie: `yymm`, czyli dwie cyfry roku i dwie cyfry miesiąca. Na rysunku 70 będzie to sierpień 2019 roku.

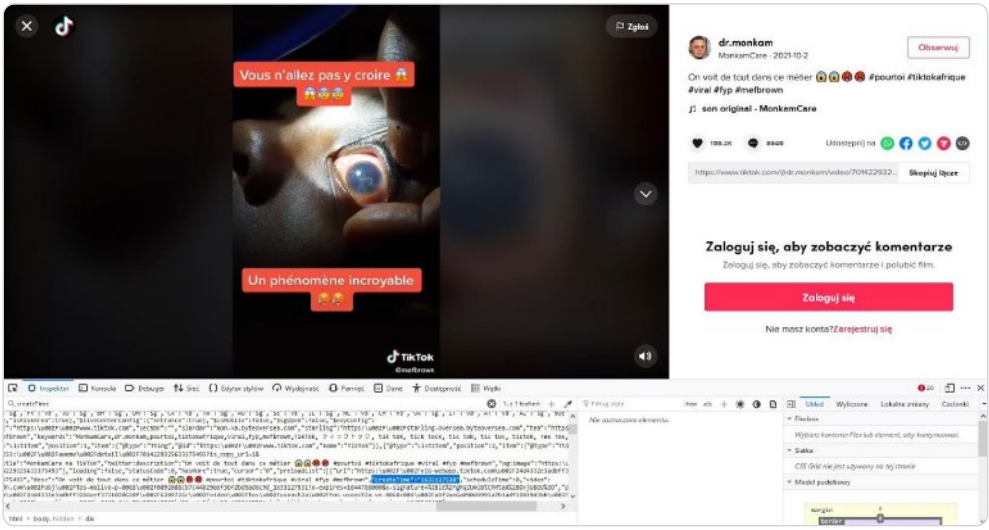


Rysunek 70. Widok narzędzi deweloperskich Bing Maps z zaznaczonym żądaniem dla pojedynczego kafelka mapy i nagłówkami zawierającymi zakres dat wykonania zdjęcia

Analiza kodu strony

Podobną technikę, jednak w zupełnie innym serwisie, zastosował belgijski dziennikarz Brecht Castel podczas weryfikacji fake newsa dotyczącego domniemanych skutków szczepionki Pfizer[52]. Widoczny na rozpowszechnianym w mediach społecznościowych filmie wijący się w ludzkim oku robak miał być dowodem na istnienie grupy, która za cel stawia sobie przejęcie kontroli nad światem za pomocą szczepionek. Po nitce do kłębka, poprzez analizę poszczególnych klatek filmu, dziennikarz dotarł do kolejnych, wcześniejszych tweetów, a także filmików na TikToku zawierających tego newsa. W końcu trafił na ten sam materiał wideo, ale w zupełnie innym kontekście.

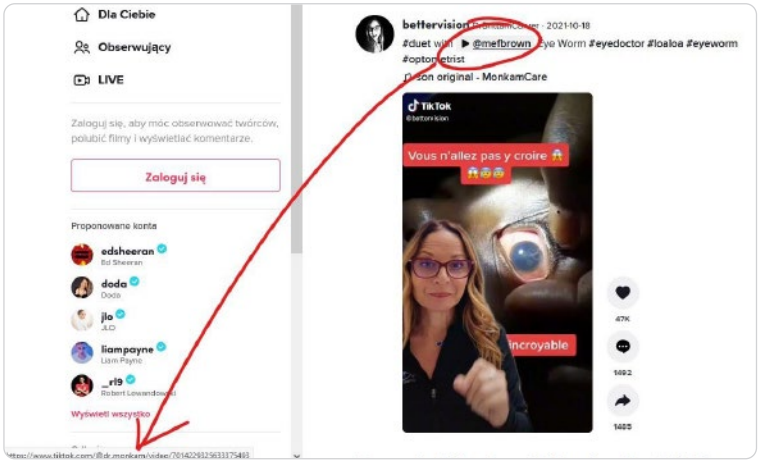
Jak jednak stwierdzić, kto pierwszy umieścił go w Internecie? W tym celu pomocna okazuje się właśnie analiza kodu strony z wyświetlonym filmem na TikToku. By mieć pewność, że znajdujemy się na stronie wyłącznie z materiałem wideo do analizy, najlepiej kliknąć w wyświetlany film. Za pomocą klawisza F12 (lub przez opcje przeglądarki) otwieramy DevTools i tym razem w zakładce INSPEKTOR (lub ELEMENTY w przeglądarkach Chrome i Edge), czyli *de facto* w kodzie źródłowym strony, szukamy ciągu `createTime`. Będzie on wskazywał bardzo precyzyjnie datę utworzenia wpisu i będzie miał format tzw. uniksowego timestampa (rysunek 71), o którym wspominałem już w rozdziale *OSINT w pandemii, czyli co wynikało z wyników testów* (s. 60–68). Jeśli wyfiltrowanie tego ciągu znaków będzie kłopotliwe w realizacji, można wyświetlić kod strony w osobnej zakładce przy użyciu opcji POKAŻ ŹRÓDŁO STRONY – i tam go wyszukać.



Rysunek 71. Miejsce, w którym znajduje się *timestamp* pokazujący moment umieszczenia filmu w serwisie TikTok

Po jego zamianie na datę bardziej przyjazną człowiekowi (np. przy użyciu serwisu EpochConverter) możemy jednoznaczne stwierdzić, kiedy wpis został utworzony. To ustalenie umożliwiło Castelowi weryfikację, kto pierwszy opublikował film, a więc kto tak naprawdę jest jego autorem. Link do konta na TikToku, na którym po raz pierwszy opublikowano film z robakiem w oku, widoczny na zrzutach ekranu w śledztwie Castela, już nie działa, gdyż konto ma aktualnie przypisaną inną nazwę użytkownika. Możemy jednak potwierdzić, że jest to to samo konto, które analizował Brecht Castel, przez wyszukanie widocznej na jego screenach nazwy użytkownika w wyszukiwarce Google. W jednym z wyników, odnoszącym się do innego filmu na TikToku, bazującego na poszukiwanym materiale, widać link do profilu autora oryginalnego materiału. Po kliknięciu w link jesteśmy jednak przenoszeni do profilu o nowej nazwie. Wygląda na to, że po zmianie nazwy użytkownika na TikToku linki do profilu utworzone wcześniej nadal mają w opisie pierwotną nazwę konta, ale adres URL jest podmieniony na nowy, co daje nam możliwość znalezienia konta o nowej nazwie.

Przy okazji analizy tego tematu natknąłem się na jeszcze jedną ciekawą właściwość TikToka. Nie jest ważne, jaką nazwę użytkownika wpiszemy w adresie konkretnego filmu, ważny jest jedynie identyfikator klipu wideo. Jest to zatem druga metoda na dotarcie do nowego profilu danej osoby: po wpisaniu adresu konkretnego filmu TikTok przekierowuje na adres wskazujący aktualną nazwę konta (rysunek 72). Można to sprawdzić, wyświetlając dowolny film na TikToku i zmieniając nazwę występującą po znaku @, ale przed znakiem /. Pomimo zmian w nazwie użytkownika zawsze jesteśmy przenoszeni do właściwego filmu.



Rysunek 72. Opis linku do profilu (zaznaczony na czerwono) zawiera starą nazwę użytkownika, ale prowadzi już do nowego konta, ze zmienioną nazwą

Po analizie źródłowego materiału filmowego i konsultacji z ekspertem od pasożytów okazało się, że obecność takiego dziwnego organizmu w ludzkim oku nie jest związana ze szczepionką, a z najzwyklejszym pasożytem, naturalnie występującym w Afryce. Dodatkowym elementem weryfikacji było znalezienie map obrazujących występowanie owego pasożyta na świecie i potwierdzenie związku pomiędzy wskazanymi tam obszarami a miejscem zamieszkania autora filmu. Zainteresowanych szczegółami tego tematu zachęcam do obejrzenia filmiku belgijskiego badacza na YouTube, w którym przedstawia poszczególne etapy weryfikacji tego fake newsa.

Po raz kolejny, dzięki analizie kodu źródłowego stron serwisów w Internecie, możliwe było wskazanie czasu, z jakiego pochodzą publikowane tam media. Taka umiejętność w epoce dezinformacji i zalewających nas zewsząd fake newsów jest niezmiernie przydatna. Wskazane tutaj przykłady to tylko mały wycinek serwisów, które można analizować pod tym kątem. Zachęcam również do samodzielnych prób wyszukiwania podobnych danych na innych stronach internetowych.

Podsumowanie i rady

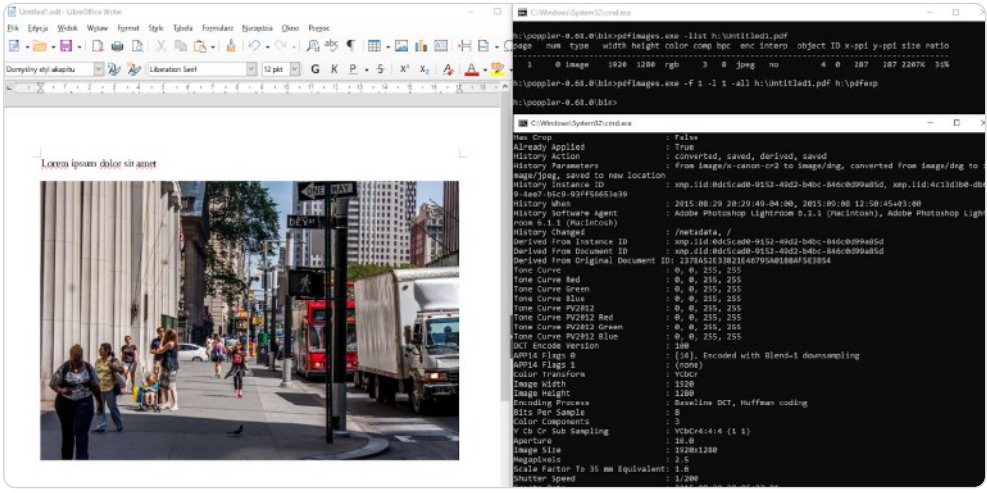
- Wiele serwisów internetowych zamieszcza informacje o dacie utworzenia obrazu lub filmu, jednak nie publikuje ich wprost. Niekiedy konieczne jest samodzielne wyszukanie takich informacji w kodzie lub w nagłówkach przesyłanych przez strony.
- Każdą znalezioną informację należy dodatkowo zweryfikować z innymi dostępnymi źródłami lub – w przypadku bardzo konkretnych i nieznanych nam dziedzin – skonsultować z ekspertem w danym temacie.
- Przeglądarki dają coraz większe możliwości analizy przesyłanych danych: od kodu źródłowego strony, przez rodzaje odbieranych danych i ich źródło, aż po nagłówki zapytań oraz odpowiedzi.

R13 METADANE – ŚWIĘTY GRAAL CZY ŚLEPY ZAUŁEK?

Metadane stanowią ciekawy element śledztw OSINT-owych. Są bardzo konkretną wskazówką przy ustalaniu źródła pochodzenia zdjęć, filmów lub dokumentów i przyczyniają się do lepszego zrozumienia kolejności zdarzeń. Ten rozdział poświęcony jest analizie metadanych zawartych bezpośrednio w plikach publikowanych w Internecie.

Eksportowanie zdjęć z metadanymi z plików PDF

Na początku lutego 2022 roku w serwisie Twitter opublikowana została informacja[53], że z plików PDF można wyeksportować zdjęcia w pełnej rozdzielczości i z całym zestawem metadanych (rysunek 73). W tym celu wystarczy skorzystać z narzędzia pdfimages. O ile faktycznie okazuje się, że podczas tworzenia pliku PDF możliwe jest zawarcie w nim obrazka z pełnymi metadanymi, to jednak z przeprowadzonej przeze mnie na szybko analizy wynika, że większość programów generujących dokumenty w takim formacie usuwa je. Programem, który tego nie robi, jest Writer z LibreOffice, ale tylko wtedy, gdy przy eksporcie do formatu PDF ustawimy opcję „brak kompresji" dla plików graficznych. Niemniej jednak spostrzeżenie to jest bardzo ciekawe dla poszukiwania dodatkowych metadanych w dokumentach.



Rysunek 73. Metadane (po prawej) w obrazku (po lewej) wyeksportowanym z PDF-a programem LibreOffice Writer

Weryfikacji tego, jakie metadane pozostawiają przeróżne organizacje w dokumentach otwartych (z rozszerzeniem .docx) lub eksportowanych do PDF-a, można dokonać, wyszukując dowolne pliki o tym rozszerzeniu w Google lub innej wyszukiwarce. Tutaj posłużę się zapytaniem do Google o brzmieniu:

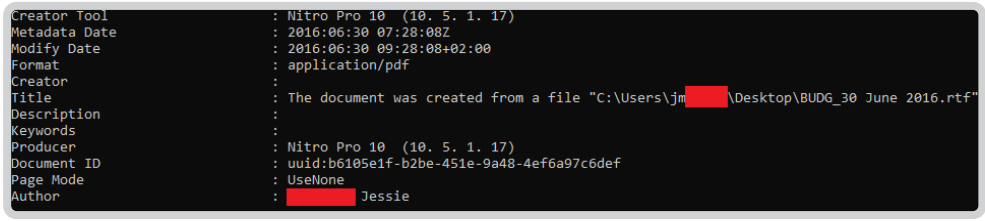
`"audit report" ext:docx`, które wskaże mi wszystkie dokumenty zawierające słowa „audit report" i posiadające rozszerzenie .docx, a więc stworzone w Wordzie (w przypadku pakietu MS Office) lub we Writerze (w przypadku Libre/OpenOffice).

Jeden z pierwszych wyników wyszukiwania przyniósł efekt w postaci pliku z bardzo dużą ilością metadanych, co pozwala zobaczyć, jak szeroki może być wachlarz informacji w nich zawartych: od wersji oprogramowania, w jakiej dokument powstawał, przez dane autora i firmy, aż po ścieżkę jego przechowywania. Ciekawym zestawem metadanych są etykiety MSIP, które dotyczą zabezpieczeń w ramach chmury Microsoft Azure (rysunek 74).

```
Words                           : 2613
Characters                      : 15561
Application                     : Microsoft Office Word
Doc Security                    : None
Lines                           : 129
Paragraphs                      : 36
Scale Crop                      : No
Heading Pairs                   : Title, 1, Titre, 1
Titles Of Parts                 : JAP audit-report - distant assessment changes January 2022, JAP Audit report template_
revision 1_draft 2018 08 10
Company                         : European Medicines Agency
Links Up To Date                : No
Characters With Spaces          : 18138
Shared Doc                      : No
Hyperlinks Changed              : No
App Version                     : 16.0000
Classification                  : Internal All EMA Staff and Contractors
DM_Author                       :
DM_Category                     : General
DM_Creation_Date                : 24/01/2022 09:58:34
DM_Creator_Name                 : R[redacted]
DM_DocRefId                     : EMA/45273/2022
DM_emea_doc_ref_id              : EMA/45273/2022
DM_emea_filing_code             :
DM_Keywords                     :
DM_Language                     :
DM_Modifer_Name                 : R[redacted]
DM_Modified_Date                : 24/01/2022 10:00:07
DM_Modifier_Name                : R[redacted]
DM_Modify_Date                  : 24/01/2022 10:00:07
DM_Name                         : JAP audit-report - template revision 3_ January 2022_final
DM_Path                         : /04. Inspections/4. GMP/GMP IWG/4.Other activities/01.Compliance Group/04.Joint Audit
Programme/Audit documents/JAP 2022 revision (audit template + checklist)
DM_Status                       :
DM_Subject                      :
DM_Title                        :
DM_Type                         : emea_document
DM_Version                      : 1.0,CURRENT
MSIP_Label_afe1b31d-cec0-4074-b4bd-f07689e43d84_ActionId: 5886ea32-5a2f-40bb-aa2f-f333b8e3305f
MSIP_Label_afe1b31d-cec0-4074-b4bd-f07689e43d84_Application: Microsoft Azure Information Protection
MSIP_Label_afe1b31d-cec0-4074-b4bd-f07689e43d84_Enabled: True
MSIP_Label_afe1b31d-cec0-4074-b4bd-f07689e43d84_Extended_MSFT_Method: Automatic
MSIP_Label_afe1b31d-cec0-4074-b4bd-f07689e43d84_Name: Internal
MSIP_Label_afe1b31d-cec0-4074-b4bd-f07689e43d84_Owner: [redacted]@ema.europa.eu
MSIP_Label_afe1b31d-cec0-4074-b4bd-f07689e43d84_SetDate: 2020-05-20T13:36:17.1438910Z
MSIP_Label_afe1b31d-cec0-4074-b4bd-f07689e43d84_SiteId: bc9dc15c-61bc-4f03-b60b-e5b6d8922839
MSIP_Label_39b352ef-c49b-4068-987f-9b664711be4a_Enabled: true
MSIP_Label_39b352ef-c49b-4068-987f-9b664711be4a_SetDate: 2022-01-24T10:28:13Z
MSIP_Label_39b352ef-c49b-4068-987f-9b664711be4a_Method: Privileged
MSIP_Label_39b352ef-c49b-4068-987f-9b664711be4a_Name: 39b352ef-c49b-4068-987f-9b664711be4a
MSIP_Label_39b352ef-c49b-4068-987f-9b664711be4a_SiteId: bc9dc15c-61bc-4f03-b60b-e5b6d8922839
MSIP_Label_39b352ef-c49b-4068-987f-9b664711be4a_ActionId: 2a66d91a-2187-4b7e-8e41-08990f3633c5
MSIP_Label_39b352ef-c49b-4068-987f-9b664711be4a_ContentBits: 2
```

Rysunek 74. Fragment metadanych z pliku w formacie DOCX z Microsoft Azure, wyświetlonych przy użyciu narzędzia ExifTool. Zasłonięte elementy dotyczą danych osobowych autora lub innych osób zaangażowanych w obieg dokumentu

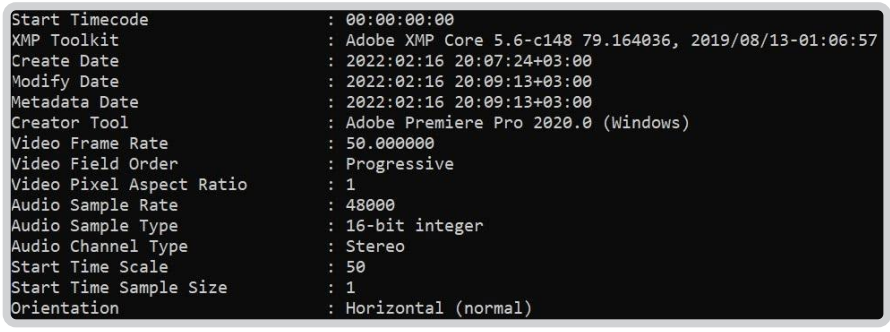
W niektórych plikach można znaleźć bardzo dokładne dane o maszynie, na której tworzony był plik, łącznie z systemem operacyjnym, ścieżką pliku i nazwą użytkownika (rysunek 75).



Rysunek 75. Ścieżka do pliku źródłowego dla PDF-a wraz z nazwą użytkownika komputera i oprogramowaniem używanym do generowania PDF-ów

Metadane z filmów publikowanych w serwisach internetowych

Jednak nie tylko dokumenty tekstowe mogą zawierać istotne metadane. 18 lutego 2022 roku w filmach opublikowanych na Telegramie (*Zayavleniye glavy LNR Leonida Pasechnika*[54] oraz w filmie zamieszczonym na profilu Denisa Pushilina[55]) przez prorosyjskich separatystów pojawiła się informacja o ewakuacji ludności na wschodzie Ukrainy. Tematem szybko zainteresowali się m.in. dziennikarze śledczy z grupy Bellingcat. Zarówno Aric Toler[56], jak i Eliot Higgins[57] opublikowali na Twitterze zrzuty ekranu pokazujące metadane plików, które dowodziły, że filmy zostały nagrane dwa dni wcześniej (czyli 16 lutego 2022 roku; rysunek 76), a opublikowano je dopiero wtedy, gdy sytuacja się zaogniła. Pomimo doniesień z wielu stron o zdemaskowaniu tej manipulacji, autorzy postu nie przejęli się wpadką i nie usunęli filmów, co umożliwiło każdej osobie posiadającej konto na Telegramie pobranie plików i samodzielne zweryfikowanie tych metadanych.



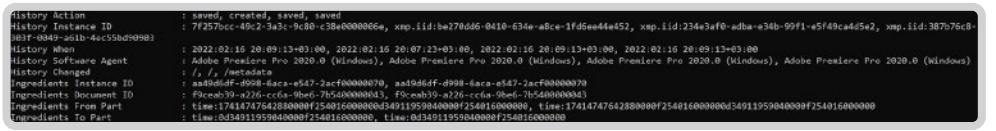
Rysunek 76. Fragment metadanych z jednego z filmów zamieszczonych w serwisie Telegram, w którym widać datę jego utworzenia i modyfikacji: 16 lutego 2022 roku

Minusem jest tu konieczność posiadania konta na Telegramie (aby można było pobrać wspomniane filmy) i zainstalowania aplikacji, gdyż, w odróżnieniu np. od Twittera/X czy Facebooka, Telegram nie ma w pełni funkcjonalnej wersji przeglądarkowej. Plusem – oczywiście z punktu widzenia OSINT-u, a nie prywatności użytkowników – jest natomiast polityka Telegrama polegająca na nieusuwaniu metadanych z wgrywanych mediów. Dodatkowe ułatwienie stanowi fakt, że Telegram umożliwia pobranie pliku na dysk bezpośrednio z opcji aplikacji i nie trzeba w tym przypadku znać żadnych trików, jak to ma miejsce chociażby w przypadku pobierania filmów z TikToka.

Oczywiście do metadanych w pliku należy zawsze podchodzić z dużą ostrożnością, gdyż modyfikowanie ich jest bardzo proste i za pomocą kilku komend lub kliknięć można zarówno je usunąć, jak i wprowadzić lub modyfikować. Metadane zależą także od czasu ustawionego na urządzeniu, np. aparacie fotograficznym. Telefony komórkowe zazwyczaj podają aktualną datę i godzinę, jednak w przypadku aparatów, które są urządzeniami działającymi *offline*, data i godzina są określane przez użytkownika, który wprowadza je ręcznie.

Metadane pozyskane za pomocą narzędzia ExifTool

Nie mniej ciekawie przedstawiają się pozostałe metadane, do których dostęp można uzyskać, posługując się np. wszechstronnym narzędziem ExifTool. W pierwszej kolejności, po wpisach dotyczących dat, o których wspominałem powyżej, znajdują się informacje dotyczące oprogramowania wykorzystanego do stworzenia klipu (rysunek 77).



Rysunek 77. Informacje o oprogramowaniu i datach modyfikacji klipu uzyskane z wykorzystaniem ExifTool

Widoczne na zrzucie ekranu wpisy wskazują na Adobe Premiere Pro 2020.0 dla Windows, czyli są to dokładne informacje o środowisku, w którym powstawał docelowy klip. Aplikacja ta to rozbudowana wersja oprogramowania do tworzenia klipów filmowych od Adobe, jednak nie w najnowszej wersji. Także przebieg samego tworzenia pliku jest dość dokładnie udokumentowany, ponieważ widoczne są cztery wpisy (`saved`, `created`, `saved`, `saved`) oraz daty im odpowiadające. Wszystkie one wskazują na 16 lutego 2022 roku.

To jednak nie koniec metadanych. Kolejne wpisy wskazują, jakich plików źródłowych użyto do produkcji docelowego filmu. Były to dwa nagrania, zarejestrowane godzinę wcześniej (ale nadal 16 lutego) aparatem Panasonic

DC-GH5 (rysunek 78). Szybki rekonesans pokazuje, że jest to model flagowego, bezlusterkowego aparatu marki Panasonic z serii Lumix. Takie drobne szczegóły są ważne, gdyż mogą się przydać w późniejszej korelacji kolejnych badanych filmów z tym samym źródłem.

```
Ingredients File Path           : P1066476.MOV, P1066476.MOV
Ingredients Mask Markers        : None, None
Pantry Create Date              : 2022:02:16 18:50:20Z
Pantry Modify Date              : 2022:02:16 19:09:42+03:00
Pantry Metadata Date            : 2022:02:16 19:09:42+03:00
Pantry Start Time Scale         : 90000
Pantry Start Time Sample Size   : 3600
Pantry Video Compressor         : H264_420_LongGOP 150
Pantry Gamma Curve              : CINELIKE_D
Pantry Video Color Space        : Unknown (BT.709)
Pantry Make                     : Panasonic
Pantry Model                    : DC-GH5
Pantry Orientation              : Horizontal (normal)
```

Rysunek 78. Informacje o aparacie, za pomocą którego utworzono pierwotne ujęcia, uzyskane za pomocą narzędzia ExifTool

Każdy trop warto zweryfikować, więc dodatkowo można porównać sposób nazywania plików (zdjęć i filmów) ze wzorcem nazewnictwa plików dla aparatów danej marki. Tego typu zestawienia można wyszukać w kilku miejscach w Internecie, jednak dla własnej wygody, a także dla innych osób potrzebujących takich informacji, zebrałem je w jedną listę, która jest dostępna na moim koncie w serwisie GitHub[58]. Wszystko się zgadza – pliki o nazwach rozpoczynających się od `P10` pochodzą z aparatów Panasonic lub Olympus.

Kolejne wpisy w zestawie metadanych pozwalają stwierdzić, w jakiej ścieżce na dysku Adobe Premiere zapisywał film. Z pola `Windows Atom Unc Project Path` (rysunek 79) można wyczytać zbiór dalszych informacji: potwierdzenie, że oprogramowanie działało na systemie Windows, użytkownik najprawdopodobniej pracował na koncie administratora, a plik był tworzony dość krótko. Ten ostatni wniosek pozwoliłem sobie wysnuć na podstawie nazwy pliku `Untitled.prproj` w katalogu automatycznego zapisywania stanu projektu – skoro plik nie miał nawet nadanego tytułu, to prawdopodobnie nie był elementem jakiegoś większego projektu. Daty zapisu i edycji pliku zdają się to potwierdzać.

```
Windows Atom Extension          : .prproj
Windows Atom Invocation Flags   : /L
Windows Atom Unc Project Path   : \\?\C:\Users\Admin\Documents\Adobe\Premiere Pro\8.0\Adobe Premiere Pro Auto-Save\Untitled.prproj
Mac Atom Application Code       : 1347449455
Mac Atom Invocation Apple Event : 1129468018
Media Data Size                 : 280807057
Media Data Offset               : 117808
Image Size                      : 1920x1080
Megapixels                      : 2.1
Avg Bitrate                     : 16.3 Mbps
Rotation                        : 0
```

Rysunek 79. Zestaw metadanych ze ścieżką, w której zapisany był klip podczas tworzenia (ExifTool)

Na podstawie analizy zaledwie jednego pliku możliwe było zdobycie wielu informacji: ustalenie czasu stworzenia klipu, określenie systemu operacyjnego twórcy, oprogramowania wykorzystywanego do edycji filmu, modelu aparatu fotograficznego użytego do nagrania, a nawet nazwy użytkownika systemu operacyjnego i prawdopodobnie też poziomu jego uprawnień. Oczywiście każda z tych informacji (a nawet wszystkie naraz) może być fałszywym tropem, jednak zdają się one zazębiać ze sobą i tworzyć spójny obraz procesu produkcji nagrania.

Podsumowanie i rady

- Metadane, jeśli są obecne, mogą stanowić źródło różnorodnych informacji o procesie powstawania pliku: zdjęcia, filmu czy dokumentu.
- Manipulacja metadanymi jest procesem niewymagającym szerokiej wiedzy lub specjalistycznego oprogramowania.
- Im więcej możliwości połączenia faktów w spójną całość lub potwierdzenia ich za pomocą innych technik, tym lepiej.
- Chociaż wiele serwisów internetowych czyści pliki multimedialne z metadanych, niektóre tego nie robią, a co za tym idzie, narażają twórców na zdradzenie większej ilości informacji, niż ci prawdopodobnie chcieliby opublikować.

R14 CO POWIE MAPA, CZYLI O OTWARTYCH DANYCH W SERWISACH MAPOWYCH

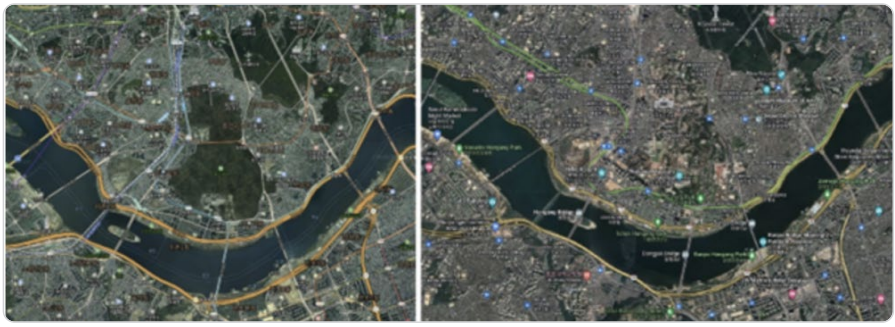
Serwisy mapowe, takie jak chociażby Google Maps, stały się częścią codziennego życia wielu osób. Coraz rzadziej można już usłyszeć spektakularne historie o tym, jak poprowadzony przez nawigację kierowca wjechał do jeziora, bo takie wskazówki otrzymał od swojej aplikacji. Dzisiejsze mapy są na bieżąco aktualizowane, zarówno jeśli chodzi o topografię miast, jak i zobrazowanie satelitarne. Czy jednak można im w pełni zaufać?

Nie wszystko, co widzisz, jest prawdziwe

Serwisy mapowe udostępniające zdjęcia satelitarne mogą zostać uznane za najbardziej wiarygodne, bo przecież dużo trudniej jest zmienić coś na zdjęciu niż „dorysować" ulicę tam, gdzie jej nie ma. Jak pokazał jednak swego czasu Benjamin Strick[59], można odnaleźć miejsca, w wypadku których zdecydowano się na modyfikację zdjęć satelitarnych, aby ukryć przed oczyma ciekawskich obszary wojskowe (rysunki 80 i 81).

Temat dotyczy obiektów zlokalizowanych w Korei Południowej, więc na mapach koreańskiego serwisu Naver w miejscu bazy wojskowej znajduje się las.

Jeśli jednak będziemy chcieli obejrzeć ten sam obszar w Google Maps, okaże się, że został on doklejony. Samego procesu sztucznego „zalesiania" terenu nie wykonano ze zbytnią starannością, gdyż tu i ówdzie drzewa wyrastają nagle w połowie ulicy (rysunki 82 i 83).



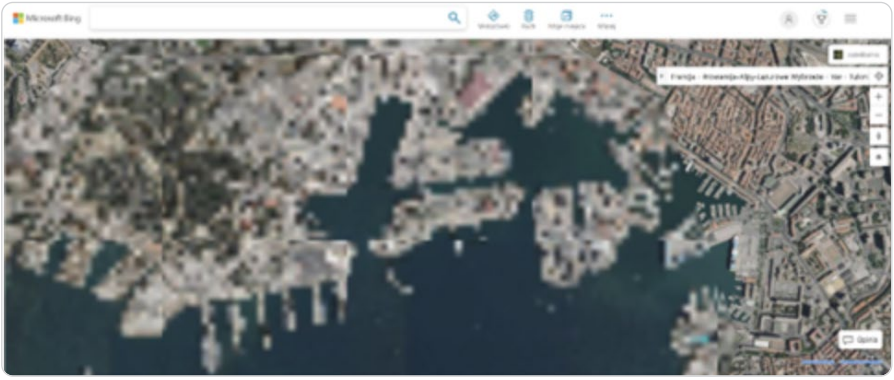
Rysunki 80 i 81. Widok jednej z baz w Korei Południowej (po lewej: Naver Maps, po prawej: Google Maps)

Rysunki 82 i 83. Na mapie koreańskiej ulice zastąpił las (po lewej: Naver Maps, po prawej: Google Maps)

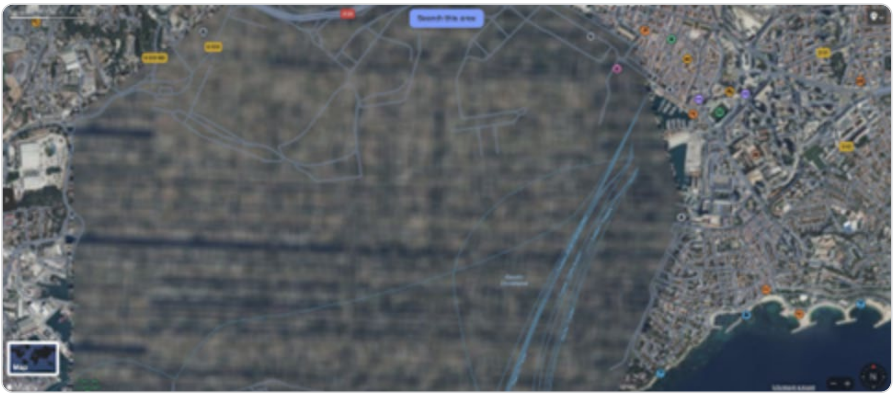
Przedstawiony powyżej sposób zaciemniania informacji dotyczących obiektów militarnych jest dość unikatowy. Z reguły tego typu miejsca są widoczne w dużo niższej rozdzielczości niż reszta zdjęcia z danego obszaru lub fragmenty zobrazowania są nieostre. Takich przykładów na całym świecie jest wiele i są one w większości związane z terenami jednostek wojskowych lub innymi obiektami albo obszarami ważnymi ze względu na bezpieczeństwo państwa. Można tutaj przywołać chociażby przykład pewnej francuskiej bazy marynarki wojennej. Na mapach Google obraz satelitarny w jej lokalizacji został „zapikselowany" i nie da się obejrzeć, co dokładnie znajduje się na nabrzeżu. Podobnie sprawa wygląda w serwisach Bing Maps i Apple Maps, gdzie obraz jest rozmazany. W Internecie istnieją jednak źródła map satelitarnych, które umożliwiają

obejrzenie zabudowań w dość wysokiej rozdzielczości, bez żadnego zamazania czy zapikselowania (rysunki 84–86).

Rysunek 84. Widok francuskiej bazy marynarki wojennej w serwisie Google Maps



Rysunek 85. Widok francuskiej bazy marynarki wojennej w serwisie Bing Maps



Rysunek 86. Widok francuskiej bazy marynarki wojennej w serwisie Apple Maps

Niestety (dla instytucji chcących zachować prywatność), mnogość serwisów oferujących tego typu zdjęcia sprawia, iż zawsze istnieje niebezpieczeństwo, że nie na wszystkich z nich możliwe będzie zaciemnienie informacji. Celowo nie pokazuję tutaj widoku opisywanego miejsca w takim serwisie mapowym, chociaż jestem świadomy, że zdobycie tych informacji nie należy do szczególnie trudnych. Taki już jednak jest urok OSINT-u i odpowiedzialności za pozyskiwane jego technikami dane.

W powyższym przykładzie posłużyłem się m.in. mapami Apple, które domyślnie są dostępne tylko na urządzeniach tego producenta. Istnieje jednak kilka sposobów na wyświetlenie map autorstwa tej firmy w przeglądarce niezależnie od systemu operacyjnego, jakim dysponujemy. Pierwszym z nich jest skorzystanie z wyszukiwarki DuckDuckGo. Po wyszukaniu interesującego miejsca wystarczy kliknąć w link MAPY u góry ekranu. Dostępne tam warstwy zdjęć satelitarnych pochodzą właśnie z Apple Maps. Drugim sposobem jest skorzystanie z serwisu *satellites.pro*, w którym możliwe jest wybranie m.in. tego źródła zobrazowania.

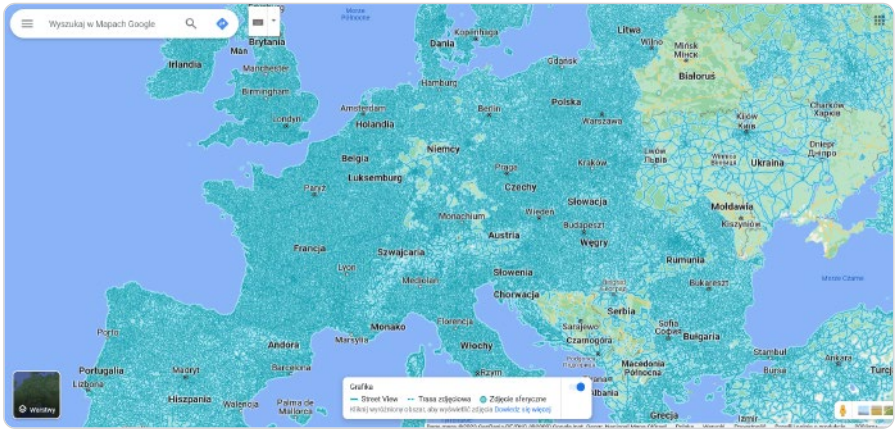
Wracając jeszcze do map południowokoreańskich, można zauważyć, że zachodnie serwisy mapowe nie umożliwiają planowania tras dojazdu w tym kraju ze względu na obowiązujące tam przepisy prawa dotyczące prywatności. Pozostaje więc wykorzystanie lokalnych serwisów, które, jak zostało to wcześniej pokazane, także nie oferują prawdziwego i pełnego zestawu informacji. Żeby było jeszcze trudniej: jeśli Czytelnicy wybierają się do tego kraju i planują zabrać ze sobą lokalizatory typu AirTag lub Tile, warto wiedzieć, że najprawdopodobniej nie zadziałają one tam z powodu tych samych przepisów.

Ograniczenia w Google Street View

Nie tylko Korea mocno ogranicza informacje zawarte na mapach. Bardzo zdecydowane podejście Niemców i Austriaków do swojej prywatności długo powstrzymywało Google przed dalszym zobrazowaniem w Street View większej części tych krajów, rozpoczętym jeszcze zanim ogromna liczba obywateli tych państw zaczęła protestować przeciw upublicznianiu widoków ich ulic i prosić o zamazanie zdjęć posesji. Niemcy pozostawali wiele lat „białą plamą" na mapie Google Street View, co mogło być pewnym utrudnieniem np. podczas poszukiwań miejsca wykonania zdjęcia lub filmu (rysunki 87 i 88).

Rysunek 87. Pokrycie terytorium Niemiec zdjęciami Google Street View jest znacznie mniejsze niż w innych krajach Europy

W 2023 roku ta sytuacja się zmieniła i liczba widoków Google Street View w Niemczech znacznie się zwiększyła.



Rysunek 88. Pokrycie terytorium Niemiec zdjęciami Google Street View w listopadzie 2023 roku

Chiński pomysł na zabezpieczenie przed dokładną lokalizacją

Chiny z kolei podeszły dość kreatywnie do zobrazowania swojego kraju na mapach satelitarnych: w serwisie Google Maps linie ulic przesunięte są o losowe odległości, o 100–700 metrów od ich faktycznego położenia (rysunek 89). Chińskie prawo nie pozwala na zbieranie i publikowanie dokładnych danych geograficznych przez osoby i firmy nieposiadające stosownego zezwolenia Chińskiej Republiki Ludowej. W Wikipedii, w tekście dotyczącym projektu OpenStreetMap[60], można nawet przeczytać, że zgodnie z chińskim

prawem wszyscy cudzoziemcy zbierający dane geograficzne bez pozwolenia zostaną dotkliwie ukarani. Ma to mieć związek z potrzebą utrzymania odpowiedniego poziomu bezpieczeństwa kraju i jego obywateli.

Rysunek 89. Widoczne przesunięcie dróg na mapach w serwisie Google Maps w stosunku do zdjęć satelitarnych na terytorium Chin

Technicznie rzecz biorąc, można stwierdzić, że przesunięcie na mapach związane jest z wykorzystaniem innych geograficznych systemów odniesienia. Mapy satelitarne są pozycjonowane z zastosowaniem systemu WGS-84[61], który używany jest także przez urządzenia GPS, natomiast rozkład ulic pozycjonowany jest przy użyciu chińskiego systemu GCJ-02*, który nie pokrywa się z WGS-84 i wprowadza przesunięcia. Rozkład ulic wyświetlany w OpenStreetMap jest poprawny jedynie dlatego, że teren został spozycjonowany przy wykorzystaniu nielegalnych odbiorników GPS.

Podsumowanie i rady

- Dostępne w Internecie mapy satelitarne umożliwiają rozpoznanie i śledzenie zmian na danym terenie oraz weryfikację informacji pochodzących z innych źródeł.
- Możliwość uzyskania zdjęć analizowanego obszaru jest pożądana z punktu widzenia osoby wykonującej rozpoznanie, ale jednocześnie niewskazana z punktu widzenia osób odpowiadających za bezpieczeństwo. Dlatego zapewne wyścig pomiędzy tymi, którzy próbują te dane ukryć lub chociażby nieco utrudnić ich szczegółową analizę, a tymi, którzy będą tych danych poszukiwali, będzie trwał nadal.

* Zob. np.: E. Fuentes, *Why GPS Coordinates Look Wrong on Maps of China*, Service Objects, September 19, 2019, lub T. Whitehead, *Chinese street maps out of alignment in Google Earth and Google Maps*, Google Earth Blog, August 17, 2015.

- Jak przy każdej analizie pozyskanych informacji, warto jest konfrontować te same dane pochodzące z różnych źródeł, aby uniknąć pomyłki wynikającej z niekompletności lub celowego zafałszowania obrazu.

CIEKAWOSTKA NA KONIEC

Czy wiedzieliście, że gdy upuścimy Pegmana (ludzika Google Street View) nad jeziorem Loch Ness, stanie się on zielonym stworkiem, a nad Strefą 51 zmieni się w UFO?

R15 OSINT^2, CZYLI KILKA SŁÓW O WERYFIKACJI DANYCH

OSINT zyskał dużą sławę szczególnie dzięki publicznemu zaprezentowaniu możliwości, jakie daje, ale także ze względu na fakt, że coraz większa część światowej społeczności jest obecna i aktywna w Internecie. Nie bez znaczenia jest też rozwój platform społecznościowych oraz narzędzi, które umożliwiają dostęp do różnych typów danych umieszczanych w sieci. Należy jednak pamiętać, że OSINT nie jest magicznym kapeluszem, z którego można zawsze wyciągnąć oczekiwanego królika. Po bliższym przyjrzeniu się otrzymanym informacjom może okazać się (jak w znanym dowcipie z Radia Erewań), że to jednak nie w Moskwie, tylko w Petersburgu, nie samochody, tylko rowery i nie rozdają, tylko kradną.

Poszukiwania Andrew Tate'a

Pod koniec 2022 roku w Internecie dość głośno zrobiło się o sprawie Andrew Tate'a (rysunek 90), byłego kickboksera i zarazem kontrowersyjnej osobowości internetowej, który został zatrzymany przez rumuńskie władze, a niedługo później aresztowany w związku z zarzutami o gwałt oraz handel ludźmi. Fakt ten pewnie przeszedłby bez większego echa, gdyby Tate nie wdał się kilka dni wcześniej w internetową przepychankę słowną z Gretą Thunberg. 27 grudnia Tate pochwalił się swoimi samochodami, oznaczając Thunberg we wpisie na Twitterze[62]. Ta następnego dnia odpowiedziała zaczepką na zaczepkę[63] i tak sprawa się rozkręciła. Użytkownicy Internetu sięgnęli po popcorn i patrzyli, co będzie dalej. Chwilę później Tate opublikował niespełna dwuminutowy filmik[64], który odnosił się do całej sytuacji i ostatniego tweeta Thunberg. Co jednak najbardziej przykuło uwagę widzów, to fakt, że w trakcie filmiku Tate prosił, by podać mu pizzę, a na pierwszym planie pojawiły się dwa opakowania, na których znajdowały się logo i nazwa pizzerii oraz jej adres internetowy, jasno wskazujący, że cała sytuacja nagrywana jest gdzieś w Rumunii.

Kiedy 30 grudnia Andrew Tate został zatrzymany przez rumuńską policję, natychmiast pojawiła się teoria[65], że do odnalezienia go przyczynił się dowód jego obecności w Rumunii i że to właśnie pudełko na pizzę było tym dowodem.

Rysunek 90. Kadr z filmu opublikowanego na Twitterze, który rzekomo przyczynił się do zlokalizowania Andrew Tate'a

Tego typu chwytliwe tematy szybko rozprzestrzeniają się w portalach internetowych (także tych oficjalnych serwisach informacyjnych); tak stało się i tym razem. Temat zrelacjonowała również telewizja TVN, informując o zdarzeniu w „Faktach". Dopiero później zaczęto publikować informacje, pochodzące od przedstawicieli rumuńskiej policji, mówiące o tym, że akcja operacyjna w sprawie karnej, w której prowadzone są śledztwa dotyczące przestępstw tworzenia zorganizowanej grupy przestępczej, handlu ludźmi i gwałtu, była zorganizowana przez Bukareszteńską Brygadę ds. Przestępczości Zorganizowanej wraz z prokuratorami DIICOT (Dyrekcji ds. Badania Przestępczości Zorganizowanej i Terroryzmu w Rumunii) już 29 grudnia. Rzeczniczka tej ostatniej jednostki w wywiadzie dla Associated Press, w którym pytano ją, czy to pudełka na pizzę przyczyniły się do znalezienia i zatrzymania Tate'a, odpowiedziała, że „to zabawne, ale nie". Cały proces weryfikacji tej chwytliwej teorii został dokładnie opisany na fakenews.pl[66].

W czasie gdy na Twitterze podawano dalej filmik z pizzą jako „OPSEC fail", wystarczyło tylko nie dać się ponieść emocjom szybkiego i łatwego zwycięstwa OSINT-u nad pracą operacyjną i przewinąć wpisy Andrew Tate'a trochę dalej, aby zauważyć, że 25 grudnia, czyli na dwa dni przed akcją z Gretą Thunberg, wrzucił na Twittera inny filmik[67] z krajobrazem górskim opatrzonym tylko jednym słowem: Romania (rysunek 91). W nim bardziej jednoznacznie pokazywał, gdzie aktualnie przebywa. Gdyby ktoś pokusił się o pójście krok dalej w poszukiwaniach aktualnego miejsca zamieszkania byłego kickboksera, miałby szansę odnaleźć też m.in. informację, że w Rumunii mieszka on już od 2017 roku, zatem policja raczej nie miała problemu z ustaleniem adresu jego mieszkania w Bukareszcie. Czasami jednak pozorny szybki i trafny wynik zniechęca do zweryfikowania go i zastanowienia się, czy na pewno to, co uzyskaliśmy, jest prawidłową informacją.

Rysunek 91. Tweet z 25 grudnia 2022 roku opisany „Romania"

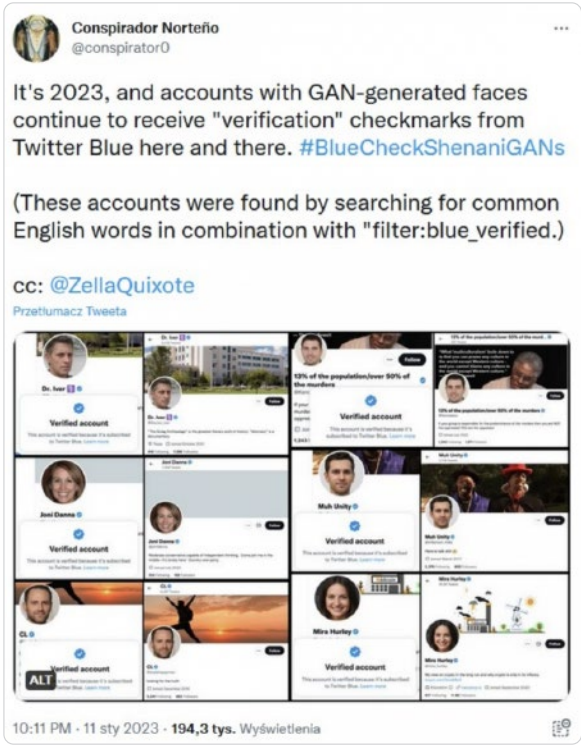
Nawiązując do tytułu tego rozdziału, warto zauważyć, że czasami na pierwotne proste działania poszukiwawcze (których nie można tak naprawdę nazwać pełnym OSINT-em, gdyż nie mają fazy analizy danych) trzeba nałożyć jeszcze jedną warstwę OSINT-u, uzupełniającą braki w pierwotnym cyklu. Próbując prawidłowo nazwać działania na otwartych danych, pierwotnie uzyskane wyniki można co najwyżej sklasyfikować jako **OSD (Open Source Data)**, czyli po prostu surowe dane, pozyskane z otwartych źródeł, lub **OSINF (Open Source Information)**, czyli dane pozyskane ze źródeł, które już częściowo je przefiltrowały, np. media. Dopiero zweryfikowane i przekazane odpowiednim odbiorcom, mogą zostać określone jako OSINT. Dla porządku można jeszcze wyróżnić OSINT-V, czyli OSINT, który przeszedł weryfikację lub pochodzi ze źródła, które można uznać za godne zaufania. Tego typu dodatkowa weryfikacja pozwala wychwytywać nieprawdziwe informacje, które są celowo rozpowszechniane i wpadają w tryby analiz OSINT-owych.

Nowe oznaczenia kont na Twitterze/X

Nie tylko podsunięte przez kogoś wyniki „szybkiego OSINT-u" mogą wprowadzić w błąd. Sam X, zarządzany przez Elona Muska, wprowadził oznaczenia zweryfikowanych kont za jedyne osiem dolarów (lub 11 dolarów, jeśli subskrypcja dokonywana jest poprzez aplikację na iOS bądź Androida). Problem w tym,

że dla przeciętnego czytelnika newsów na X oznaczenia prawdziwie zweryfikowanych kont (tzw. starych) i tych wykupionych za garść dolarów oznaczeń (tzw. nowych) są identyczne. Dlatego też kupowanie oznaczeń zweryfikowanego konta stało się popularne wśród operatorów fałszywych kont, mających szerzyć dezinformację lub być elementem ataków na użytkowników platformy.

Przykład tego typu działań został zaprezentowany m.in. w styczniu 2023 roku na profilu Conspirador Norteño (rysunek 92)[68].



Rysunek 92. Zestawienie znalezionych fałszywych kont, zweryfikowanych za opłatą

Zdjęcia profilowe dla kont botów są często generowane przy wykorzystaniu mechanizmów GAN w serwisach *thispersondoesnotexist.com* lub *generated.photos*, więc wprawne oko od razu je rozpozna. Jednak dla zwykłego użytkownika social mediów nie jest to takie oczywiste. Konta takie były wykorzystywane do siania dezinformacji i propagandowych treści już wiele razy, a ich zdemaskowanie możliwe było dzięki wyszukiwaniu za pomocą filtrów na X. Wpisując w pole wyszukiwania frazę: `filter:blue_verified -filter:verified`, można uzyskać listę kont mających wykupiony znaczek zweryfikowanego konta („blue verified"), które nie są „starymi" kontami, zweryfikowanymi na podstawie obowiązujących od dawna zasad, czyli m.in. konieczności posiadania zdjęcia profilowego, odpowiedniej nazwy konta, zweryfikowanego numeru

telefonu i braku oznak, że konto było ostatnio modyfikowane lub może służyć do dezinformacji. Sposób, w jaki dany profil uzyskał swoją weryfikację, można także sprawdzić, klikając na niebieski znaczek obok nazwy użytkownika na stronie profilu (rysunek 93).

Rysunek 93. Sposób na sprawdzenie, czy konto w portalu X ma znaczek weryfikacji kupiony czy otrzymany po faktycznej weryfikacji (tu przykład faktycznie zweryfikowanego konta Miasta Gdańsk)

Serwis X wprowadził dwa dodatkowe kolory[69] znaczków weryfikacji konta – złote dla biznesu i szare dla kont rządowych. Być może za rogiem czają się już kolejne kolory i kształty. I jak tu się w tym odnaleźć?

OSINT, jako sposób wyszukiwania danych, daje ogrom możliwości, jednak nie należy przeceniać jego uniwersalności i łatwości znajdowania prawdziwych informacji. Za każdym razem należy zadać sobie pytania: „Czy na pewno to, co widzę, jest prawdziwe?" i: „Jakie argumenty za tym przemawiają?". Dzięki temu możliwe będzie uniknięcie w przyszłości wpadania w pułapki „łatwych rozwiązań".

Podsumowanie i rady

- Jeśli coś jest zbyt piękne, aby było prawdziwe, to najprawdopodobniej prawdziwe nie jest – zasada ta dotyczy także przykładów genialnych śledztw OSINT-owych.

- Weryfikacja informacji jest kluczowa, jeśli przygotowujemy analizę OSINT-ową i chcemy uniknąć zupełnego lub częściowego zaburzenia jej wniosków i wyników.
- Jeśli wszyscy użytkownicy portalu X będą mogli być zweryfikowani, to tak naprawdę nikt nie będzie zweryfikowany. Tę zasadę można odnieść do wielu aspektów, ale akurat w opisywanym przypadku dotyczy ona możliwości dowolnego oznaczania przez portal kont jako „zweryfikowane".

R16 OSINT KONTRA DEZINFORMACJA, CZYLI JAK ZDEMASKOWAĆ TROLLA

Wydarzenia o dużym ładunku emocjonalnym, takie jak wojna w Ukrainie czy silne trzęsienie ziemi, które miało miejsce w lutym 2023 roku na terenie Turcji i Syrii, stanowią bazę do działań dezinformacyjnych, gdyż przez mocne oddziaływanie na ludzkie emocje łatwiej jest spowodować szybką reakcję dużej liczby osób. Możliwe jest jednak wykorzystanie OSINT-u do przeciwdziałania takim praktykom i ujawnienia „sztuczek", które mogą także wpływać na wnioski wyciągane ze śledztw prowadzonych w Internecie.

Na początek: dlaczego w tytule nie znalazł się znak zapytania

Jednym z często spotykanych sposobów na przyciągnięcie uwagi czytelników gazet i portali informacyjnych jest wykorzystywanie w tytule artykułu pytania, które stanowić będzie *clickbait* (czyli poprzez swój ładunek emocjonalny będzie nakłaniało do kliknięcia w link do artykułu). Co jednak zrobić, jeśli w opisywanym temacie nie ma nic nadzwyczajnego? W tym przypadku można posłużyć się pytaniem, które będzie na tyle kontrowersyjne, aby zainteresowało potencjalnego czytelnika, np. „Wprowadzą ograniczenie liczby aplikacji instalowanych na smartfonie?". Zgodnie z tzw. prawem nagłówków Betteridge'a, na każdy nagłówek prasowy zakończony znakiem zapytania można odpowiedzieć „nie". Prawo to sprawdza się w naprawdę dużej części newsów, publikowanych zarówno w mediach mainstreamowych, jak i w mniejszych serwisach, które potrzebują klikalności. Warto o nim pamiętać przy czytaniu nagłówków, chociaż należy mieć na uwadze fakt, że nie jest to regułą.

Co jednak w sytuacji, kiedy nawet po przeczytaniu całego artykułu prasowego nie jest możliwe ustalenie, czy informacje w nim zawarte są prawdziwe, czy też stanowią narzędzie manipulacji? Poza weryfikacją, czy dany tekst próbuje wzbudzić skrajne emocje, co może być oznaką próby manipulacji, można posłużyć się kilkoma prostymi technikami OSINT-owymi, które ułatwią ustalenie, z czym mamy do czynienia. Do takich podstawowych technik można zaliczyć m.in. te opisane poniżej.

Źródło

Pierwszym krokiem przy weryfikacji prawdziwości informacji może być sprawdzenie źródła, z którego ona pochodzi. Jeśli jest to serwis internetowy, warto zwrócić uwagę, jakie inne informacje się w nim znajdują, tzn. czy np. nie jest to strona publikująca same sensacyjne informacje bez odpowiedniej weryfikacji lub czy nie jest to strona o określonym, wąskim zakresie publikacji silnie nacechowanych emocjonalnie. Warto też sprawdzić, kiedy zarejestrowana została domena dla danego serwisu, korzystając z jednego z ogólnodostępnych w Internecie narzędzi do analizy domen, takich jak np. DomainTools lub Whois. Świeżo zarejestrowana domena oznacza większe prawdopodobieństwo, że dany serwis może nie być godny zaufania, chociaż nie musi być to regułą.

W przypadku większych serwisów także istnieje znaczne prawdopodobieństwo, że informacja jest prawdziwa, chociaż i dużym graczom zdarzają się wpadki polegające na powtarzaniu niepotwierdzonych informacji, czego przykładem jest wspomniany w poprzednim rozdziale słynny filmik, w którym Andrew Tate reaguje na zarzuty Grety Thunberg. Dlatego zawsze należy mieć na uwadze fakt, że świeża informacja, szczególnie sensacyjna, mogła nie zostać odpowiednio zweryfikowana, ponieważ w świecie newsów czas odgrywa istotną rolę w wyścigu o pierwszeństwo opublikowania konkretnej wiadomości.

Możliwe jest także sprawdzenie serwisu informacyjnego, którego nie znamy, a który wydaje się podejrzany, w archiwum Internetu, czyli np. w serwisie Internet Archive – The Wayback Machine. Jeśli jeszcze niedawno strona wyglądała zupełnie inaczej lub publikowała zupełnie inne treści, może się okazać, że domena została przejęta w wyniku ataku[70] na serwery hostujące lub DNS albo przez wykupienie nazwy domenowej, której ktoś zapomniał[71] przedłużyć lub też celowo tego nie zrobił. Dla bardziej zaawansowanych użytkowników interesującym źródłem będzie także weryfikacja historycznych wpisów DNS, które mogą świadczyć o przejęciu domeny.

Autor

W celu sprawdzenia wiarygodności analizowanej informacji należy zweryfikować, kto jest jej autorem. Oznakami, że informacja jest nieprawdziwa, mogą być (chociaż nie muszą!) następujące wskazówki:

- brak autora informacji,
- fakt, że autor zajmuje się wyłącznie publikowaniem informacji o dużym ładunku emocjonalnym, ale z różnych dziedzin,
- autor poza analizowanym przypadkiem zajmuje się zupełnie inną tematyką (może to oznaczać zarówno próbę manipulacji przez przekupionego autora, jak i przejęcie konta lub próbę podszycia się pod tę osobę),
- konto, które publikuje informacje, powstało niedawno lub niedawno zmieniło nazwę użytkownika albo opis,

- brak zdjęcia profilowego konta, jest ono domyślne, skopiowane z innego konta lub innego miejsca w Internecie albo przedstawia osobę, która ewidentnie nie istnieje (np. widać, że zdjęcie zostało wygenerowane przez stronę *ThisPersonDoesNotExist*).

Autorzy dezinformacji często nie zadają sobie zbyt dużo trudu, aby przygotować naprawdę dobre i trudne do wychwycenia zdjęcia dla kont publikujących zmanipulowane informacje, dlatego proste wyszukanie w Internecie danych autora lub wyszukiwanie obrazem zdjęcia profilowego konta może szybko przynieść efekt w postaci potwierdzenia fałszywości danego konta (rysunek 94[72]).

Rysunek 94. Zestawienie kont botów, które publikują dokładnie ten sam tekst

Często kopiowane są także całe fragmenty tekstu, który stanowi treść zmanipulowanej informacji, co pozwala zidentyfikować wiele kont używanych do ich rozsiewania, dzięki wyszukaniu dłuższego ciągu słów, który może być dezinformacją.

Jeśli dokładnie ten sam tekst będzie widniał na wielu pozornie niepowiązanych kontach, można mieć niemal całkowitą pewność, że trafiliśmy na farmę trolli.

Te same zasady dotyczą komentarzy pod artykułami, w których trolle rozsiewają dezinformacje i podgrzewają atmosferę dyskusji, aby wywołać kłótnie pomiędzy użytkownikami i (*nomen omen*) „zaszczepić" w nich swoje teorie. Autorów komentarzy można również w wielu przypadkach prześwietlić za pomocą ich zdjęć profilowych, nazw użytkownika lub powiązanych profili, np. kont Google.

Osobom, które chcą spróbować swoich sił w rozpoznawaniu fałszywych profili w Internecie, polecam serwis Spot The Troll.

Czas i miejsce

Jednym ze sposobów na dodanie wiarygodności zmanipulowanej informacji jest poparcie jej zdjęciami lub filmami z tego samego miejsca, ale innego momentu czasowego, lub z innego miejsca, które tylko z pozoru przypomina to, o którym jest mowa. Tego typu sytuacje zdarzały się już w trakcie wojny w Ukrainie, ale także m.in. po tragicznym w skutkach trzęsieniu ziemi na terenie Turcji i Syrii w lutym 2023 roku. Weryfikacją i demaskowaniem krótkich filmów zamieszczanych w mediach społecznościowych i szerzących nieprawdziwe informacje zajmuje się wielu dziennikarzy, m.in. wspomniany już wcześniej Brecht Castel. Na jego koncie na Twitterze/X można znaleźć wiele przykładów tego typu analiz, w tym także analizę filmu walącego się budynku[73], rzekomo w Turcji (rysunek 95).

Rysunek 95. Tweet Brechta Castela z serii dotyczącej analizy filmu walącego się budynku, który miał mieć związek z trzęsieniem ziemi w Turcji

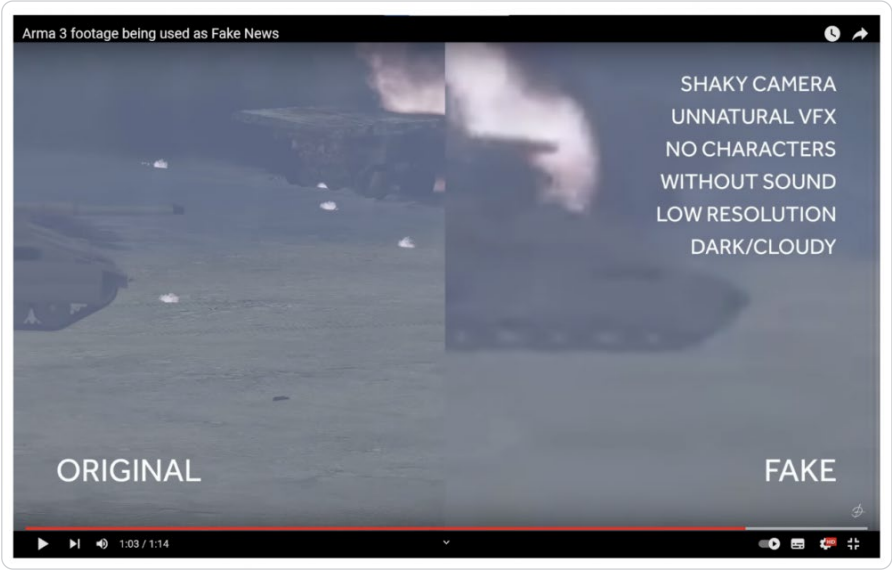
W analizie belgijski dziennikarz skupił się na kilku aspektach. Po pierwsze, krajobraz był raczej letni, podczas gdy zdjęcia i filmy wykonane po trzęsieniu ziemi w Turcji pokazywały zimową scenerię. Zwrócił także uwagę na ludzi, którzy nie wydawali się przejęci zapadającym się budynkiem. Zauważył też, że napisy (w tym na tablicach rejestracyjnych) zawierają znaki alfabetu arabskiego, a nie przypominają napisów tureckich lub syryjskich. W końcu odnalazł źródło filmu, które okazało się przedstawiać miasto Jeddah w Arabii Saudyjskiej, gdzie przeprowadzono kontrolowane wyburzenie jednego z budynków. Okazało się także, że te filmy udało się odnaleźć m.in. na TikToku, gdzie pojawiły się już w połowie stycznia 2023 roku, czyli jeszcze przed trzęsieniem ziemi w Turcji. Dalsza analiza konta na Twitterze, które publikowało fałszywie opisany film, ujawniła, że zostało ono utworzone niedawno, ma bardzo małą liczbę śledzących je osób oraz nazwę użytkownika (*Twitter handle*) niepasującą do nazwy konta, która wraz z linkiem wskazywała na sklep internetowy, a nie na źródło informacyjne.

Grafika komputerowa

W dobie ogólnodostępnych narzędzi wykorzystujących techniki *deepfake* nie dziwi już manipulacja obrazem lub materiałem wideo polegająca na umieszczaniu w nim nieprawdziwych elementów. Kiedy twórcom manipulacji nie chce się samodzielnie tworzyć sfałszowanych materiałów, korzystają z grafik, filmów z gier lub filmów. Mój osobisty faworyt to wpis na Twitterze, w którym rosyjska ambasada w Wielkiej Brytanii użyła grafiki z gry *Command & Conquer: Generals* do ilustracji wpisu mówiącego o otrzymaniu kilkunastu ciężarówek z bronią chemiczną przez ekstremistów niedaleko Aleppo. Gra ma już swoje lata, więc od razu rzuca się w oczy fakt, że nie może to być wizualizacja faktycznych ciężarówek, a dodatkowo na zdjęciu dodany jest napis informujący o tym, że jest to tylko wizualizacja wiadomości, jednak pokazuje to ekstremalny przypadek nieprawdziwej ilustracji (rysunek 96).

Rysunek 96. Ciężarówki z gry *Command & Conquer: Generals* jako ilustracja wpisu na Twitterze dotyczącego działań ekstremistów w Syrii

Filmy z innej gry, *Arma 3*, były wykorzystywane do uwiarygodnienia przekazywanych informacji, zarówno o zniszczeniu dużych zapasów sprzętu nieprzyjaciela przez Armię Ukrainy[74], jak i do zaatakowania rakietami NATO-wskiego konwoju[75]. W obu przypadkach udało się ustalić, że nagrania nie są prawdziwe, jednak zdążyły one już dotrzeć do ogromnej liczby odbiorców. W przypadku drugiego materiału zdążyło go obejrzeć ponad 700 tysięcy osób. Twórcy gry – Bohemia Interactive – opublikowali nawet film na YouTube[76], w którym pokazują, jakie sztuczki zostały wykorzystane, aby z materiału wideo z ich gry zrobić prawdopodobne nagranie z frontu. Zazwyczaj w takich wypadkach jakość materiału jest obniżana, obraz jest rozmyty i niestabilny pod względem kadru, co miałoby sugerować nagranie wykonane np. kamerą w smartfonie, jednak tak naprawdę są to zabiegi mające ukryć widoczne cechy grafiki komputerowej (rysunek 97).



Rysunek 97. Kadr z materiału producenta gry *Arma 3*, przedstawiający sposoby manipulacji materiałem wideo z gry w celu stworzenia z niego filmu wyglądającego jak nagranie z frontu (opublikowany na YouTube)

Innym przykładem analizy zmanipulowanych nagrań wideo jest weryfikacja reklam[77], z których jedna pokazywała warszawskie metro i plakaty namawiające Polaków do zostania kierowcami czołgów w Ukrainie. Miało to być dowodem na „terytorialne ambicje Polski wobec Ukrainy". Po analizie materiału wideo przez badaczy z Belgii okazało się, że widoczne są w nim cechy nieudolnego nałożenia reklamy na oryginalne nagranie (rysunek 98).

Rysunek 98. Wpis demaskujący fałszywe reklamy, publikowane oryginalnie na kanale Telegramu

Aby zweryfikować, czy dane nagranie nie jest jedynie grafiką wygenerowaną komputerowo lub pochodzącą z filmu, można pokusić się o jego analizę pod kątem niespójności pomiędzy klatkami lub wyszukiwanie za pomocą wybranych klatek (np. klatek kluczowych) w wyszukiwarkach grafiki. Istnieje szansa, że uda się odnaleźć tę samą scenę, ale w zupełnie innym kontekście.

Wyjście z bańki

UWAGA

Należy pamiętać, że każdy, czy tego chce, czy nie, żyje obecnie w bańce informacyjnej (zwanej też bańką filtracyjną, ang. ***filter bubble***), którą tworzą serwisy internetowe, a wśród nich głównie media społecznościowe.

Serwowane tam informacje są dopasowywane do osobistego profilu ich użytkownika tak, aby jak najbardziej przypadły mu do gustu, co ma się z kolei przełożyć na zyski dla takich gigantów jak Google czy Meta (właściciel m.in. Facebooka

i Instagrama). Dlatego wiele osób dziwi się, przykładowo: „Jak partia X mogła zdobyć tyle głosów? Przecież wszyscy pisali, że będą głosować na partię Y!". Winna jest temu właśnie owa bańka filtracyjna, w której znajduje się konto danej osoby w mediach społecznościowych, chociaż można ją rozciągnąć także na życie poza Internetem. Obracamy się na ogół w kręgach osób o podobnych poglądach i upodobaniach, co często przekłada się na mylne pojęcie o ogóle społeczeństwa. Aby ujrzeć świat poza bańką, warto wyszukiwać informacje bez logowania się na swoje konta, a także korzystając z wyszukiwarek i serwisów nieprofilujących (przynajmniej teoretycznie) swoich użytkowników, jak np. DuckDuckGo lub Startpage. W przypadku tego pierwszego serwisu profilowanie miało niestety pewne wyłączenia[78], jeśli chodzi o trackery Microsoftu.

Podsumowanie i rady

Dezinformacja towarzyszy nam od dawna, jednak w wyniku coraz większego dostępu do mediów społecznościowych i portali internetowych, a także ze względu na coraz łatwiejsze publikowanie w nich treści o dowolnej tematyce, bez jakiejkolwiek weryfikacji ich prawdziwości, ekspozycja na zmanipulowane informacje jest coraz większa. Na szczęście rosną także możliwości weryfikacji źródeł, autorów i materiałów multimedialnych przez techniki OSINT-owe. Warto więc za każdym razem dokonać weryfikacji informacji na poziomie psychologicznym („czy ta informacja wywołuje u mnie emocje i czy skłania mnie do natychmiastowego działania?"), gdyż jest wiele sposobów na wykorzystanie błędów poznawczych w ludzkim rozumowaniu w celu przekonania odbiorcy do swoich teorii. Warto sprawdzić także inne, bardziej techniczne jej aspekty, aby nie dać się oszukać.

Przedstawione tutaj techniki oczywiście nie są zamkniętym zbiorem sposobów weryfikacji treści, a jedynie nakreślają temat. Osoby, które chciałyby zgłębić tematykę błędów poznawczych w ocenie informacji oraz sposobów weryfikacji treści w ramach śledztw OSINT-owych, odsyłam do mojej książki *Bezpieczeństwo osób i systemów IT z wykorzystaniem białego wywiadu. OSINT*.

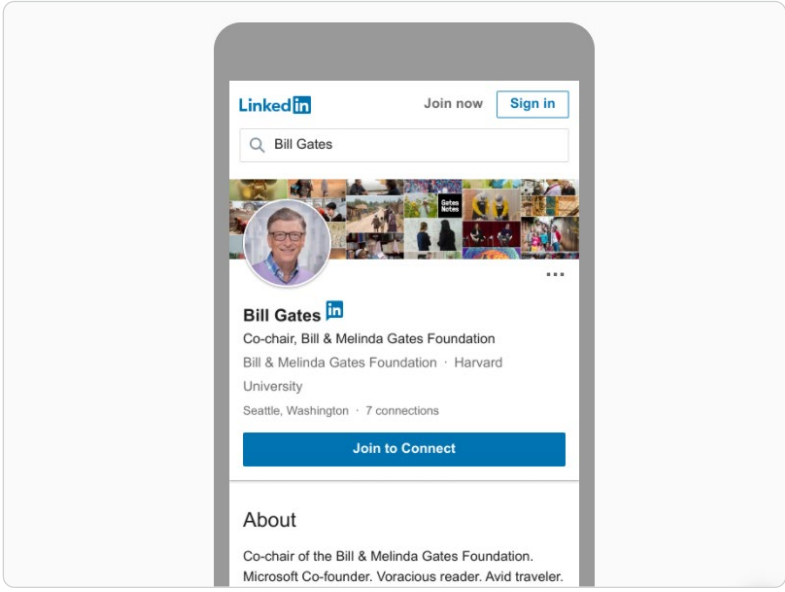
Dodatkowo, dla osób, które nie miały jeszcze zbyt wiele (lub wcale) do czynienia ze zdjęciami wygenerowanymi przez mechanizmy GAN na stronie *thispersondoesnotexist.com*, przygotowałem proste narzędzie Am I Real?, dzięki któremu można zidentyfikować zdjęcia poprzez analizę umiejscowienia na nich oczu i ust. Oczywiście narzędzie przeznaczone jest tylko do nauki i nie można traktować jego wyników jako wyroczni, ale pozwala ono szybko zweryfikować, czy zdjęcie może być sztucznie wygenerowane, czy nie.

R17 JAK ANONIMOWO POZYSKAĆ INFORMACJE O PRACOWNIKACH FIRMY – PRZYPADEK LINKEDIN I WZORCE ADRESÓW E-MAILOWYCH

Jakiś czas temu natrafiłem na bardzo ciekawą technikę przeglądania LinkedIn bez logowania się do tego portalu. Taki sposób przeglądania profili pracowników firm może być przydatny, jeśli np. zamierzamy szybko sprawdzić dane jakiegoś przedstawiciela firmy, a nie chcemy logować się na swoje konto z danego miejsca lub pragniemy pozostać w 100% niewykrywalni, tzn. żeby żadna informacja o tym, że odwiedzaliśmy czyjś profil, nie dotarła do jego właściciela (można oczywiście ukryć swoje imię i nazwisko dla osób, których profile przeglądamy, ale sam fakt przeglądania zostanie zarejestrowany).

Pasywne przeglądanie prywatnych profili na LinkedIn

Technika przeglądania LinkedIn bez logowania została pokazana[79] przez Nico Dekensa, lepiej znanego jako Dutch Osint Guy Nico (@dutch_osintguy). Opierała się ona na trzech prostych krokach. Pierwszym było wyszukanie danej osoby w Google, z dodaniem do frazy wyszukiwania informacji, że interesuje nas jej profil na LinkedIn. Wyszukiwana fraza w przypadku profilu sympatycznego Niderlandczyka może brzmieć: „Dutch Osint Guy Nico LinkedIn" (bez cudzysłowu). Jako pierwszy wynik, który nie jest sponsorowany, powinien wyświetlić się link do jego profilu. W tym przykładzie używam pseudonimu, bo ten został użyty w profilu, ale w większości przypadków wyszukiwane będzie imię i nazwisko, np. „Bill Gates LinkedIn" (rysunek 99).



Rysunek 99. Przeglądanie profilu na LinkedIn bez logowania się do tego portalu

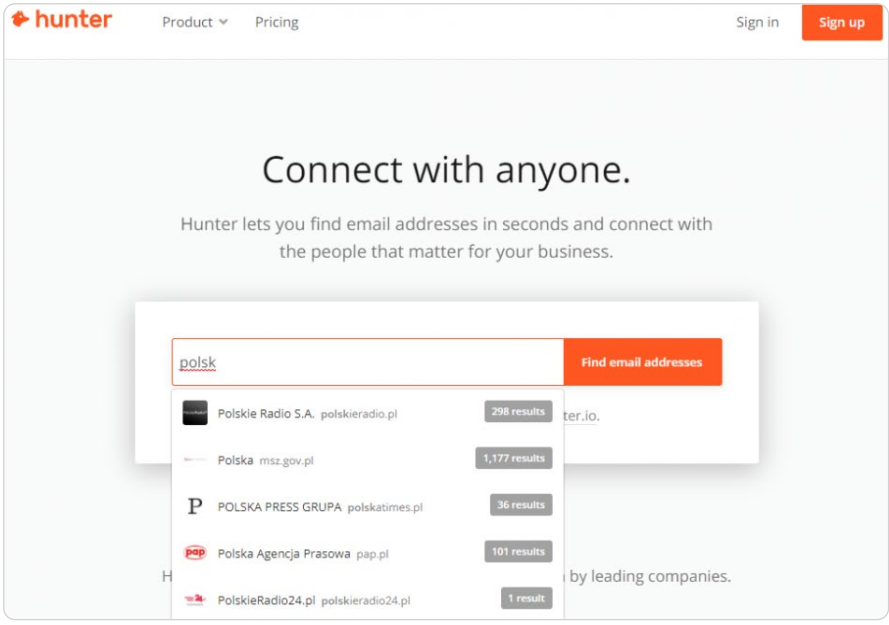
Warto zwrócić uwagę, że po kliknięciu w link jesteśmy przenoszeni do portalu LinkedIn, ale finalnie widoczna jest tylko możliwość zalogowania się.

Przy wykorzystaniu strony Google Mobile Friendly Test można było zbadać, czy strona profilu z LinkedIn jest przystosowana do pracy na urządzeniach mobilnych. Otóż okazuje się, że jest – i nawet do pewnego czasu był nam wyświetlony podgląd. Niestety, z czasem ta opcja przestała działać, jednak postanowiłem o niej napisać, bo może okazać się użyteczna w przypadku innych, podobnych stron.

W widoku strony mobilnej w Google Mobile Friendly Test widać tylko podgląd początku analizowanej strony. Przydałoby się jednak poznać i dalsze informacje. I tu z pomocą przychodzi zakładka HTML, pokazujca cały kod pobranej strony. Z użyciem ulubionego narzędzia do renderowania kodu HTML (może to być np. Tryit Editor czy Real-time HTML Editor) można już zobaczyć wszystkie informacje wyświetlane na profilu danej osoby na LinkedIn. Kurtyna.

Od imienia i nazwiska do adresu e-mail

Na koniec jeszcze kilka słów o serwisie *Hunter.io* (rysunek 100), wykorzystywanym przez niektóre narzędzia do automatycznego przeszukiwania LinkedIn.

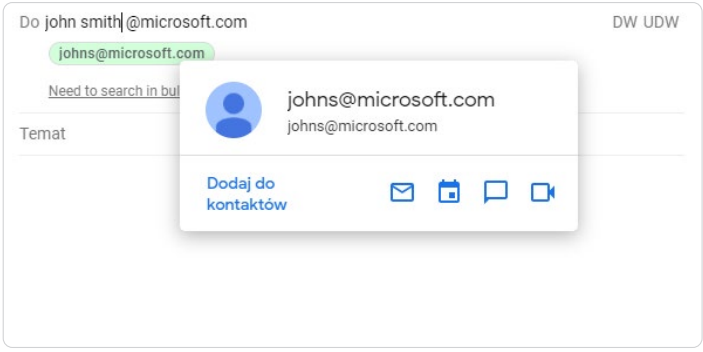


Rysunek 100. Serwis *hunter.io* jest wykorzystywany przez niektóre narzędzia do automatycznego przeszukiwania LinkedIn

Sam w sobie może on okazać się przydatny podczas rekonesansu, bo już w ramach darmowego konta oferowana jest co miesiąc możliwość wyszukiwania

50 adresów e-mail przedstawicieli analizowanej firmy zebranych z sieci, uzupełnionych o informację o prawdopodobnym wzorze używanym podczas generowania tychże adresów (czyli np. czy login tworzony jest z pełnego imienia i nazwiska, z pierwszych liter lub innych kombinacji). Może to ułatwić np. wysłanie wiadomości do osób, których adresu e-mail nie znamy, natomiast wiadomo, jak się nazywają i gdzie pracują.

Podobną funkcjonalność daje także wtyczka Name2Email do przeglądarki Chrome (rysunek 101). W polu adresata wiadomości Gmail wtyczka automatycznie wyszukuje adresy e-mail i profile Google na podstawie wpisanych danych w formacie „imię nazwisko @domena". Jej minusem jest to, że należy podać wszystkie te trzy wartości, aby wtyczka spróbowała znaleźć adresy według różnych typowych wzorców.



Rysunek 101. Efekt pracy wtyczki Name2email

Podsumowanie

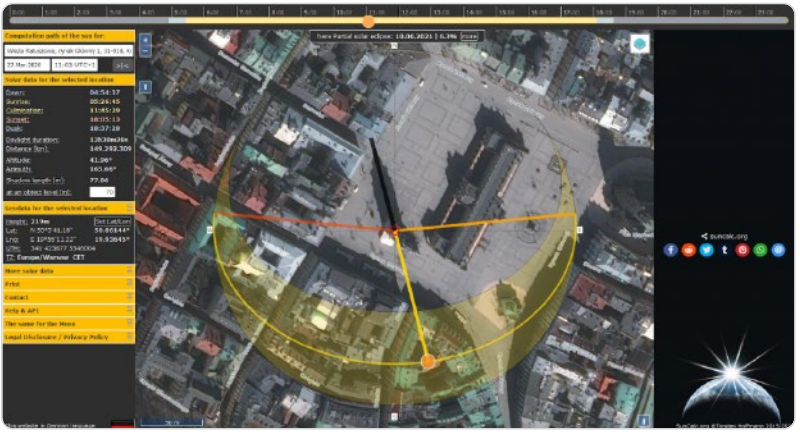
Pasywne przeglądanie serwisów społecznościowych staje się w moim odczuciu coraz trudniejsze z powodu wymuszania przez nie konieczności zalogowania się, aby w ogóle obejrzeć czyjś profil. Dlatego takie metody jak opisana na początku tego rozdziału są bardzo przydatne w zachowaniu odpowiedniego poziomu anonimowości prowadzenia rozpoznania w Internecie. Ze względu na zmieniające się zasady działania serwisów może okazać się, że wiele technik tego typu przestanie działać, jednak cały czas znajdowane są kolejne sposoby na dotarcie do informacji bez konieczności logowania się.

R18 PO SŁONECZNEJ STRONIE OSINT-U – WYKORZYSTANIE CIENI DO WERYFIKACJI ZDJĘĆ

Szukając informacji o czasie lub lokalizacji wykonania zdjęcia, można posłużyć się danymi EXIF* zawartymi w samym pliku, ale jeśli je usunięto lub mamy podejrzenie, że zostały zmodyfikowane, jest jeszcze coś, co może nam pomóc – Słońce.

Analiza cieni

Na stronie dziennikarzy śledczych Bellingcat oraz na blogu Somedeva Sangwana ukazały się kilka lat temu opisy podstaw używania pozycji Słońca do określania daty i godziny wykonania danego zdjęcia (niestety, drugi wpis został usunięty, chociaż nadal pamięta o nim archiwum Internetu[80]). Przedstawione tam możliwości analizy zdjęć (rysunek 102) wynikają z tego, że Słońce, jak zapewne wszyscy doskonale wiedzą, w ciągu dnia pojawia się na wschodnim widnokręgu i, poprzez ruch obrotowy Ziemi, pozornie „wędruje" po niebie, żeby na koniec dnia „zniknąć" za zachodnim widnokręgiem. Dodatkowo, w związku z nachyleniem osi Ziemi w stosunku do prostej prostopadłej do jej orbity, każdego dnia w roku światło słoneczne pada na powierzchnię Ziemi pod nieco innym kątem, co daje możliwość wyznaczenia w miarę dokładnego momentu czasowego, w którym cień jakiegoś przedmiotu, drzewa lub budynku miał określony stosunek długości do wysokości rzucającego go przedmiotu i padał pod danym kątem (a konkretnie chodzi o wyznaczenie azymutu, czyli kąta pomiędzy położeniem Słońca a kierunkiem północnym).



Rysunek 102. Przeprowadzona symulacja zdaje się potwierdzać datę wykonania zdjęcia satelitarnego – 27 marca. Dodatkowo wiadomo, która wtedy była godzina (materiały własne)

* EXIF to skrót od Exchangeable Image File Format – formatu metadanych obecnych w plikach fotografii cyfrowych. Metadane obecne są w wielu rodzajach plików, nie tylko w fotografiach i klipach wideo, ale także w dokumentach Word, plikach PDF, i mają za zadanie przechowywać dodatkowe informacje o pliku, np. daty utworzenia i zapisu, autora, a także w przypadku zdjęć np. lokalizację ich wykonania i model aparatu.

Jeśli uda nam się znaleźć odpowiednio dobrze widoczne cienie na zdjęciu, pozostaje już tylko skorzystać z niezwykle użytecznego narzędzia, jakim jest SunCalc. Pokazuje ono m.in. kąty wysokości i azymutu Słońca, a także długość cienia obiektu o określonej wysokości dla danego wybranego miejsca na Ziemi i wybranego czasu. Manipulując datami, można określić moment wykonania zdjęcia, porównując wyliczone dane z tymi „odczytanymi" z obrazu. Oczywiście, im mniej dokładne zdjęcie i wyliczenia długości oraz kątów cienia, tym mniejsza pewność co do określenia momentu czasowego.

Prowadząc działania OSINT-owe na półkuli południowej, warto pamiętać o tym, że cienie padają tam w kierunku południowym, a zegary słoneczne „chodzą" (jakkolwiek bez sensu by to brzmiało) niezgodnie z ruchem wskazówek zegara.

Podsumowanie i rady

- Korzystanie z cieni jest bardzo przydatną umiejętnością, lecz także trudną w przypadku typowych zdjęć „turystycznych".
- Analizując zdjęcie wykonane pod pewnym kątem, należy wziąć też poprawkę na perspektywę, która może zaburzyć pomiary. Idealne będzie ujęcie, na którym obiekt rzucający cień umiejscowiony jest przed obiektywem, a cień pada prostopadle do linii łączącej fotografa z obiektem, jednak takie ujęcia zdarzają się niezwykle rzadko. W innych przypadkach długość cienia należy odnosić do innych znanych odległości, widocznych pod tym samym kątem w podobnym oddaleniu.
- Opisy rozwiązywania zagadek OSINT-owych z wykorzystaniem analizy cieni można znaleźć m.in. we wpisie OSINT challenge[81] na blogu walnut oraz *Using Flight Tracking For Geolocation – Quiztime 30th October 2019*[82] na blogu Nixintela.

R19 JEDNO ZDJĘCIE, BY ZNALEŹĆ ICH WSZYSTKICH – OSINT NA PODSTAWIE MATERIAŁÓW WIZUALNYCH

11 lutego 2023 roku odbyła się kolejna edycja ogólnoświatowego wydarzenia spod znaku #OSINT4Good – Trace Labs OSINT Search Party CTF. W tej odsłonie wzięło udział ponad 200 drużyn liczących od jednej do czterech osób, z różnych zakątków świata. Celem spotkania było, jak zwykle, OSINT-owe znalezienie jak największej liczby wskazówek, które mogłyby pomóc policji i innym służbom zaangażowanym w poszukiwanie zaginionych osób. Często w takim przypadku dostępne jest tylko zdjęcie i kilka podstawowych informacji. Także w innych śledztwach, które dotyczą poszukiwania osób przez służby lub dziennikarzy śledczych, ich podstawą może być zaledwie jedno lub kilka zdjęć.

Jak więc wykorzystać tak niewielki zasób danych do zlokalizowania miejsca wykonania fotografii?

Zdjęcie, które doprowadziło do zespołu odpowiedzialnego za programowanie rosyjskich pocisków

W trakcie śledztwa prowadzonego przez członków zespołu Bellingcat[83] zidentyfikowany został zespół osób odpowiedzialnych za konfigurację pocisków manewrujących, które uderzyły nie tylko w ukraińskie obiekty wojskowe, ale także w tamtejsze budynki mieszkalne, przedszkola czy place zabaw. Odpowiednia konfiguracja pocisków manewrujących, tak aby trafiły dokładnie tam, gdzie mają uderzyć, jest procesem wymagającym wykonania wielu obliczeń wspomaganych komputerowo. Stąd wśród śledczych pojawiło się przeświadczenie, że zespół odpowiedzialny za obliczenia wiedział, w jakie cele uderza, a zniszczenie obiektów cywilnych nie było dziełem przypadku.

Bellingcat skontaktował się z członkami zidentyfikowanego zespołu Głównego Centrum Obliczeniowego Sztabu Generalnego (określanego także skrótem ГВЦ, GWC) i poprosił ich o potwierdzenie lub zaprzeczenie ustaleniom. Wszystko oczywiście przygotowane zostało tak, aby przekazanie informacji dziennikarzom możliwe było w sposób anonimowy, m.in. przez zapewnienie przez Bellingcat i gazetę „The Insider" kont pocztowych wykorzystywanych jedynie do tej komunikacji. Jedna z osób przesłała dziennikarzom zdjęcie wykonane w 2013 roku, na którym widać cały zespół wraz z dowódcą, stojący na schodach przed budynkiem określonym jako siedziba GWC (rysunek 103). Dziennikarze jednak, chcąc zweryfikować tę informację, musieli zlokalizować ten budynek[84]. Miejscem wykonania zdjęcia miała być siedziba GWC znajdująca się przy ulicy Znamenka 19 w Moskwie, gdzie mieści się rosyjskie Ministerstwo Obrony, jednak należało to potwierdzić.

Rysunek 103. Zdjęcie zespołu GWC, przesłane przez jednego z jego członków do zespołu Bellingcat

W ramach analizy zdjęcia dziennikarze wyodrębnili kilka szczegółów, kluczowych w identyfikacji budynku. Pierwszym z nich były ściany z czerwonej cegły oraz wzór namalowany na daszku nad wejściem, utrzymany w podobnym stylu. Dodatkowo w tym przypadku dopatrzono się wzorów cegieł i kostki brukowej przy ścianie, co mogło pomóc w potwierdzeniu lokalizacji, jeśli udałoby się dotrzeć do zdjęć satelitarnych tego miejsca w wysokiej rozdzielczości. Białe kolumny, które były częścią zadaszenia nad wejściem, zostały również zidentyfikowane w budynku naprzeciwko, widoczne w odbiciu w szybach drzwi wejściowych. Odbicie w jednej z szyb ukazało zakratowane okna z podłączoną na zewnątrz jednostką klimatyzatora. Kształt schodów oraz ich szczegóły zostały także dodane do listy elementów, które mogły potwierdzić lokalizację wykonania zdjęcia.

Dziennikarze skupili się nie tylko na podanym adresie, ale badali też inne prawdopodobne lokalizacje, jednak to przy ulicy Znamenka 19 udało się znaleźć poszukiwane wejście. Dokonano tego przy wykorzystaniu map Yandex (czyli rosyjskiego odpowiednika Google Maps, który jest znacznie lepszym źródłem map i zdjęć z ulic w przypadku terytorium Rosji). Na zdjęciu satelitarnym widoczny był kształt wejścia bardzo podobny do tego, które przedstawiała nadesłana fotografia. W tym przypadku dziennikarze mieli odrobinę szczęścia, bo wśród zdjęć opublikowanych na portalu VKontakte (czyli rosyjskim odpowiedniku Facebooka), oznaczonych jako wykonane w tej lokalizacji, było jedno zdjęcie w wysokiej rozdzielczości, zrobione przez miłośnika „turystyki dachowej" (rysunek 104). Przedstawiało ono dokładnie to poszukiwane wejście do budynku. Pomimo niemal ośmioletniej różnicy czasu wykonania obu zdjęć wszystkie rozpoznane wcześniej szczegóły się zgadzały, co pozwoliło dziennikarzom potwierdzić, że zdjęcie zespołu GWC zostało zrobione pod adresem Znamenka 19 w Moskwie.

Rysunek 104. Zdjęcie siedziby GWC znalezione na portalu VKontakte (za: Bellingcat)

Przybliż... przybliż... przybliż...

Geolokalizacja na podstawie odbitego obrazu nie jest łatwym zadaniem, ponieważ zdjęcie musi być wykonane w wysokiej rozdzielczości, odbijany fragment dość duży, a odbicie – czyste, aby możliwe było w ogóle rozpoznanie, co jest przedstawione. Sceny w stylu tych pochodzących z serialu *CSI: Kryminalne zagadki...*, gdzie obraz z kamery jest wielokrotnie powiększany i za każdym razem jego jakość utrzymuje się na wysokim poziomie, można włożyć między bajki. Jeśli jakiś element jest jedynie kropką na zdjęciu, to po jego powiększeniu najprawdopodobniej będzie zaledwie większą plamą, a nie stanie się nagle wyraźnym kształtem. Tym bardziej że większość udostępnianych obrazów z kamer, które mają pomóc w identyfikacji poszukiwanej osoby, np. przez policję, jest już na starcie słabej jakości.

Niekiedy jednak można zidentyfikować w odbitym obrazie miejsce, które jest na tyle charakterystyczne, że da się określić, gdzie wykonano daną fotografię. Tak było m.in. w przypadku zdjęcia rosyjskiego żołnierza[85], dla którego Benjamin Strick potwierdził, właśnie dzięki odbiciu w okularach (rysunek 105), że miejscem jego wykonania był Mariupol. Oczywiście było to jedynie potwierdzenie lokalizacji, a nie jej odnalezienie, ale daje to pewien pogląd na to, że odbicia są także ważną częścią OSINT-owej układanki[86].

Rysunek 105. Tweet Benjamina Stricka ze wskazaniem elementów zdjęcia, które ułatwiły jego geolokalizację

Kategorie poszukiwanych wskazówek

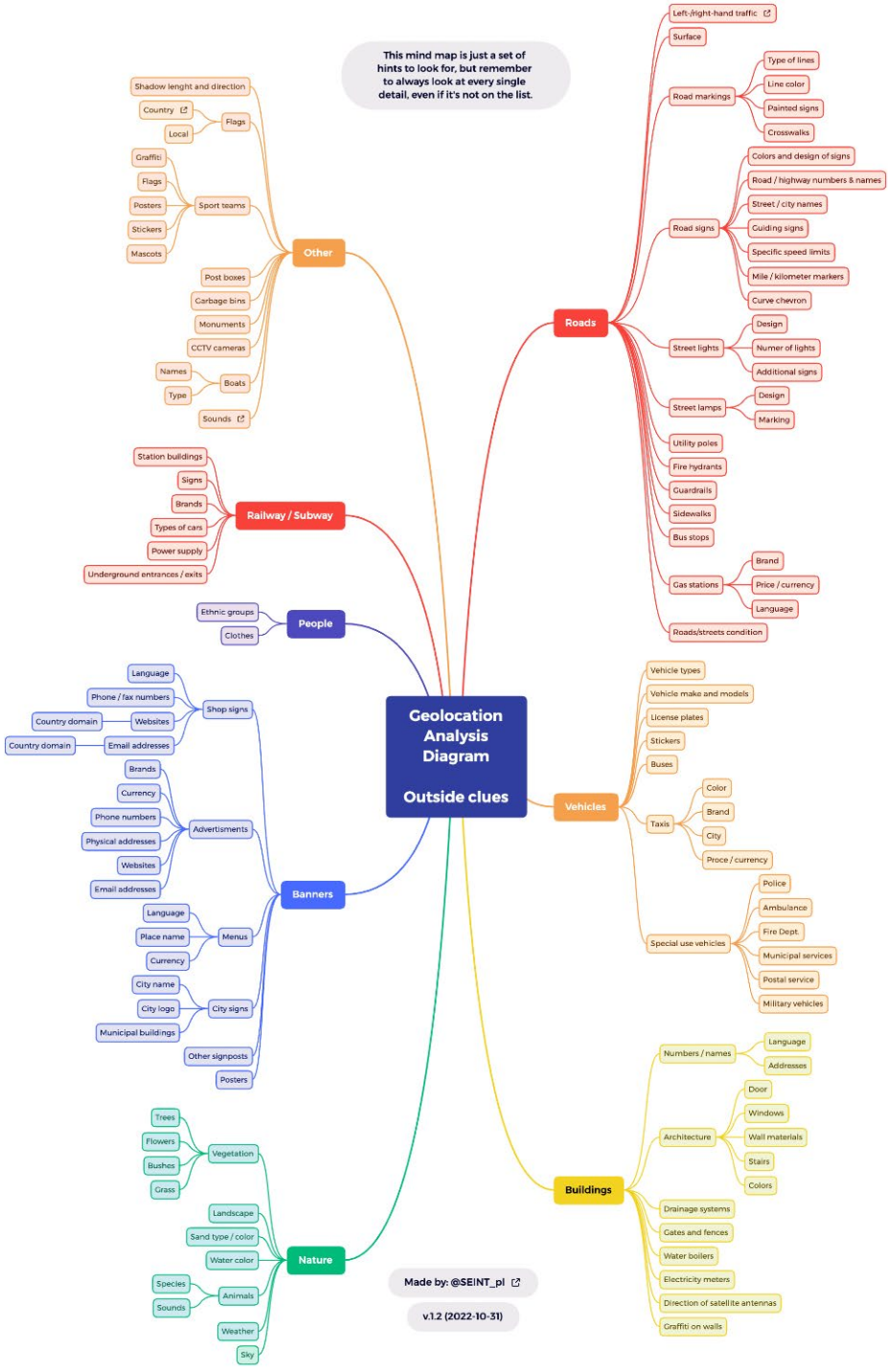
Aby przystąpić do analizy informacji dostępnych na zdjęciu lub w materiale wideo, warto wiedzieć, na jakie elementy należy zwrócić szczególną uwagę. Jako pomoc przy analizie zdjęć można także wykorzystać diagram, który opublikowałem pod koniec 2022 roku na swoim koncie na GitHubie (w formie PDF-a[87], obrazka lub możliwego do modyfikacji pliku XMind*). Starałem się na nim uwidocznić główne rodzaje przydatnych wskazówek, takie jak: drogi, pojazdy, budynki, elementy przyrody, wszelkiego rodzaju napisy oraz inne pomocne informacje.

Analiza obrazu powinna uwzględniać wiele elementów, ponieważ:

- **oznakowanie i konstrukcja dróg** mogą wskazywać na państwo lub grupę państw, w których zostało wykonane dane ujęcie;
- tak samo **pojazdy**, a w szczególności ich **tablice rejestracyjne**, są cenną wskazówką, gdyż zarówno marki samochodów, ich stan techniczny, jak i wszelkie umieszczane na nich oznaczenia są dość unikalne dla danych regionów;
- **konstrukcja budynków**, szczególnie poza centrami dużych miast, a także **ich oznaczenia**, takie jak np. **szyldy** czy **reklamy**, mogą wskazywać na konkretne państwo dzięki zamieszczonym na nich numerom telefonów, adresom e-mail lub domenom stron internetowych;
- **analiza przyrody**, czyli **gatunków drzew i roślin**, a także **zwierząt**, to kolejna cenna wskazówka, kiedy konieczne jest ustalenie kontynentu lub jego części w celu określenia miejsca wykonania analizowanego zdjęcia.

Rysunek 106[88] przedstawia jedynie podstawowy zestaw informacji, których należy poszukiwać – i nie jest to zbiór zamknięty. Zawsze należy mieć otwarty umysł i starać się znaleźć wszelkie szczegóły, które mogą pomóc zlokalizować miejsce wykonania zdjęcia lub osobę. Często takie informacje dostępne są także poza obrazem, jeśli pochodzi on np. z mediów społecznościowych. Mogą to być sąsiednie wpisy danego autora, oznaczone przez niego miejsca i dodatkowe informacje związane z daną sytuacją.

* XMind jest aplikacją służącą do tworzenia map myśli, czyli zapisywania informacji wraz z ich powiązaniami między sobą. Jest to bardzo przydatne np. przy zapisywaniu wyników rozpoznania OSINT-owego.



Rysunek 106. Diagram wskazówek ułatwiających poszukiwanie miejsca wykonania analizowanego zdjęcia

Podsumowanie i rady

Wyszukiwanie informacji wizualnych na zdjęciach i w klatkach materiałów wideo to dla mnie jeden z najciekawszych aspektów działań OSINT-owych. Przy wykorzystaniu stosunkowo niewielkiej liczby narzędzi, a głównie dzięki metodom interpretacji i kojarzenia faktów, możliwa jest poprawna geolokalizacja. Należy jednak poznać techniki analizy zawartości obrazów, sposoby wykorzystywania map satelitarnych i innych serwisów udostępniających informacje o danym miejscu, a także mieć doświadczenie w kojarzeniu drobnych szczegółów z konkretnymi lokalizacjami, aby za pomocą niewielkiego skrawka informacji wizualnej odnaleźć dane miejsce, a niekiedy nawet ustalić je co do metra.

Na koniec, pół żartem, pół serio, wzmianka o filmiku z bardzo zaawansowanym graczem w grę *GeoGuessr*[89], który lokalizowanie miejsc na Ziemi w tej grze opanował niemal do perfekcji i może je odgadywać nawet z zasłoniętymi oczami (rysunek 107). Oczywiście gra w *GeoGuessr* na tym poziomie staje się już grą pamięciową, ale i tak jest to nie lada wyczyn.

Rysunek 107. Dowód na to, że nie trzeba widzieć obrazu, aby odgadnąć miejsce, które on przedstawia (za: YouTube)

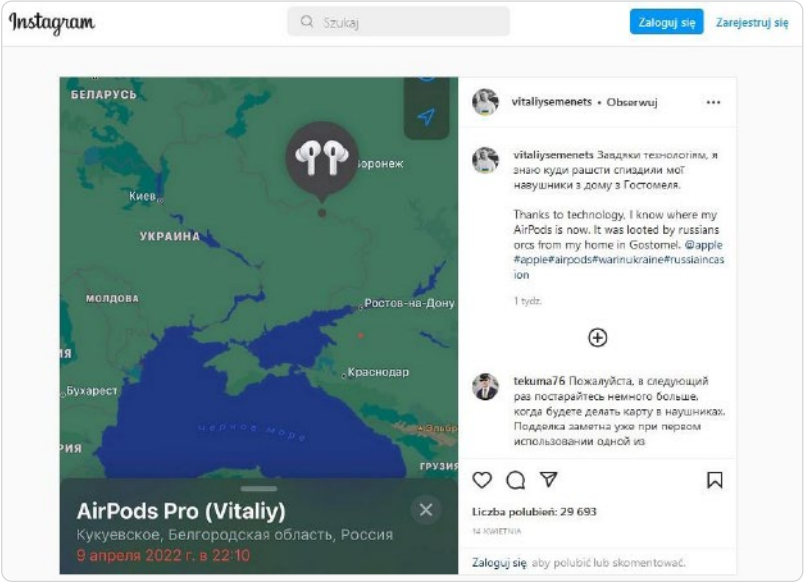
R20 APKI, SŁUCHAWKI I INNE WYCIEKAJĄCE INFORMACJE

Nieprawidłowe ustawienia bezpieczeństwa w aplikacjach i urządzeniach używanych podczas wykonywania codziennych czynności, takich jak np. bieganie, sprawiają, że stają się one źródłem cennych danych dla osób śledzących ruchy nieostrożnych użytkowników.

Jeszcze gorzej wygląda sytuacja w przypadku żołnierzy, którzy powinni zachować szczególną ostrożność w zakresie udostępnianych przez siebie informacji i są w tej kwestii szkoleni – przynajmniej ci z NATO, bo co do reszty, to pomimo świadomości istnienia materiałów szkoleniowych mam pewną wątpliwość dotyczącą skuteczności ich wykorzystywania.

Przyjrzymy się przykładom tego, jak teoretycznie niedostępne dane stają się bazą dla śledczych posługujących się metodami OSINT-owymi.

W połowie kwietnia 2022 roku popularnym tematem stał się przypadek mieszkańca Gostomla na Ukrainie, który poprzez funkcję odnajdowania położenia swoich słuchawek AirPods dowiedział się, że najpierw wskazywały one swoją lokalizację na Białorusi, a następnie znalazły się w okolicy rosyjskiego miasta Biełgorod, gdzie wojska rosyjskie przygotowywały się do ofensywy na Donbas. To jednocześnie oznaczało, że tam właśnie w chwili lokalizowania słuchawek byli ci żołnierze, którzy wcześniej „wyzwalali" jego miejscowość (i przy okazji „wyzwolili" jego sprzęt). Oznaczył on w swoim poście na Instagramie[90] firmę Apple i poprosił o nowe słuchawki, jednocześnie ciesząc się z faktu, że dzięki nowoczesnej technologii jest w stanie znaleźć swój sprzęт (rysunek 108). Jednak sprawa ta pokazuje szerszy problem (lub szansę – w zależności od perspektywy), a mianowicie ilość danych wywiadowczych, jakie mogą być pozyskane przy użyciu tego typu informacji. W momencie kiedy użytkownicy Internetu dzielą się losem swoich AirPodsów czy innych urządzeń, które można śledzić, zasilają otwarte źródła informacji o ruchach wojsk.



Rysunek 108. Post Vitalija na Instagramie, w którym pokazuje on aktualną lokalizację swoich słuchawek

Temat śledzenia produktów Apple opisałem w artykule dotyczącym przesłania pocztą AirTaga[91] i monitorowania trasy, jaką przemierzy przesyłka. Jak widać, technologia ta cały czas działa i niezawodnie pozwala na lokalizowanie zagubionych lub skradzionych rzeczy.

Sprawa ta jednak nie kończy się na jednych słuchawkach. Białoruski Projekt Hajun upublicznił[92] dane rosyjskich żołnierzy, którzy za pośrednictwem firmy kurierskiej CDEK nadawali na Białorusi paczki do Rosji. Udostępnione dane zawierają imiona, nazwiska, numery telefonów, a także zawartość paczek, które ważyły pomiędzy 50 a 450 kilogramów, i ich lokalizacje docelowe. Taka dodatkowa baza danych, wiążąca imiona i nazwiska z numerami telefonów oraz prawdopodobnymi miejscami zamieszkania, to jedno z wielu źródeł, które mogą w przyszłości ułatwić wszelkie śledztwa związane z tymi osobami, chociaż w tym przypadku wydaje się, iż mimo że dane te są publicznie dostępne w Internecie, nie można ich do końca traktować jako typowo OSINT-owego źródła.

Podobnie jest w przypadku informacji pochodzących z wycieków lub wykradzionych, choć często pomagają one w istotny sposób odnaleźć powiązania pomiędzy rozpracowywanymi osobami lub firmami. **Należy tutaj mieć na uwadze fakt, że mogą istnieć prawne przeciwwskazania w zakresie przetwarzania danych pozyskanych w nielegalny sposób lub może paść oskarżenie o czerpanie zysków z kradzieży** (jeśli np. w płatnym śledztwie skorzystamy z tego typu baz). Korzystając z tak pozyskanych danych, należy najpierw się upewnić, co i w jakim zakresie można zrobić, nie narażając się na niepotrzebne kłopoty.

Jeśli chodzi o rekonesans urządzeń IoT, to bardzo duże możliwości w tym zakresie daje serwis Shodan, który pozwala na wyszukiwanie wszelkich podpiętych do Internetu urządzeń. Dzięki użyciu odpowiednich filtrów możliwe jest np. wyszukiwanie dostępnych w sieci kamer, serwerów czy nawet czytników tablic rejestracyjnych. Sam serwis był już jakiś czas temu opisywany na sekuraku[93], skupię się więc tutaj jedynie na kilku aspektach, które mogą być pomocne z OSINT-owego punktu widzenia. Do wykorzystania niektórych narzędzi lub filtrów konieczne jest założenie płatnego konta, jednak warto śledzić informacje o promocjach, ponieważ co jakiś czas można trafić na bardzo dobre warunki (swego czasu można było np. wykupić dożywotni dostęp za dolara[94]).

Pierwszą z bardzo przydatnych możliwości serwisu jest Shodan Maps. Dzięki zastosowaniu filtrów można zobaczyć na mapie, które z interesujących nas urządzeń są dostępne w danym rejonie (rysunek 109).

Rysunek 109. Widok kamer na planie jednego z polskich miast

Możliwość znalezienia dokładnie tego, czego szukamy, dają filtry:

- jeśli chcemy np. wyszukać **wszystkie urządzenia, które wystawiają na świat swój interfejs graficzny** (a więc także kamery, które często od razu pokazują swój obraz bez konieczności logowania), możemy użyć dodatkowego filtru: `has_screenshot:yes`
- w celu zawężenia poszukiwań do **określonego kraju** wystarczy wpisać jego kod po filtrze: `country:PL`
- można także wyszukać wyniki dla **danego miasta**: `city:Warsaw`
- dla chcących zawęzić poszukiwania do okolicy o **konkretnych współrzędnych geograficznych** przydatny będzie poniższy filtr (podane współrzędne wskazują na Warszawę): `geo:52.2688,21.0153`
- możliwe jest także poszukiwanie **danych fraz w odpowiedziach serwerów**, np. poprawnych komunikatów o kodzie 200, z nagłówkiem wskazującym na serwer kamery IP: `"Server: IP Webcam Server" "200 OK"`
- jeśli zagłębimy się trochę bardziej w techniczne parametry, możemy naprawdę **dokładnie określić, jakie urządzenia są dostępne w sieci**, np. konkretne modele telewizorów smart: `product:"Samsung Smart TV UN50H6400"`

W Internecie można znaleźć naprawdę wiele przykładów, które pokazują, jak wyszukiwać konkretne systemy, urządzenia i systemy sterowania. Wystarczy wyszukać frazy `"Shodan dorks"`, a zostaniemy zasypani różnego rodzaju przykładowymi filtrami.

Wracając jednak jeszcze na chwilę do tematu śledzenia samych żołnierzy przez ich urządzenia *smart*, warto, dla utrwalenia poprawnych wzorców bezpieczeństwa operacji, przypomnieć jeden z najjaskrawszych przykładów zdradzania lokalizacji wojska, którym była sprawa aplikacji fitnessowej Strava, służącej do zapisywania tras i wyników podczas biegania lub jazdy na rowerze.

I gdyby na tym się kończyło, nie byłby to temat wart poruszania w zakresie tematyki OSINT-owej. Aplikacja jednak dawała także możliwość dzielenia się swoimi osiągnięciami ze społecznością, co sprawiło, że wiele osób z personelu baz wojskowych, które chętnie biegają w celu utrzymania formy, przy okazji tworzyło bardzo dokładne mapy tychże miejsc. Nie trzeba było wiele wysiłku, by odkryć, że lokalizacje, dookoła których tworzą się nakładające się trasy biegów, są bazami wojskowymi, a wspomniane trasy stanowią najprawdopodobniej ich granice. Udostępnienie mapy na stronie internetowej przez portal Strava dodatkowo ułatwiło analizowanie tych informacji (rysunek 110).

Rysunek 110. Widok tras biegów z portalu Strava wokół bazy Bagram w Afganistanie

Co więcej, mając konto w takiej aplikacji i śledząc poszczególne osoby, można nie tylko znaleźć położenie obiektów wojskowych, ale także poznać tryb codziennego funkcjonowania takiego użytkownika, a co za tym idzie, jednostki wojskowej, w której aktualnie przebywa obserwowana osoba, w tym znaczenie konkretnych miejsc w bazach wojskowych, jeśli użytkownik dodał do swoich tras odpowiednio dużo mówiący komentarz. Dodatkowo, jeśli dana osoba używała aplikacji przez dłuższy czas, mogło się okazać, że zdradziła także położenie innych baz, do których podróżowała. Przed upublicznieniem mapy wojsko amerykańskie miało co prawda procedury mówiące o konieczności wyłączania funkcji geolokalizacyjnych w urządzeniach IoT, ale dopiero skandal związany z trasami biegów spowodował zmianę i ograniczenie możliwości używania smartfonów przez personel baz. Rzecz jasna, nie tylko Amerykanie korzystali

z aplikacji do biegania – także pracownicy rosyjskiej ambasady w Damaszku[95] chętnie pokazywali całemu światu swoje trasy. Aplikacji fitnessowych jest oczywiście więcej i każda z nich może posłużyć do zdobycia informacji o badanym miejscu lub osobach.

Zdarza się, że sami użytkownicy tworzą bardzo dokładne i niekiedy dosadne opisy, co dzieje się w danej okolicy. Wiele miejscowości ma wdrożone mapy służące do zgłaszania zauważonych wykroczeń i spraw, którymi powinny zająć się policja, straż miejska lub inne służby miejskie. Bardzo jaskrawym przykładem takiego serwisu, w którym użytkownicy pozostawiają swoje subiektywne uwagi dotyczące danej okolicy, jest serwis *hoodmaps.com*. Pozwala spojrzeć w nieco inny sposób na miejsca, które chcemy odwiedzić, a nawet takie, co do których zdawało nam się, że je dobrze znamy (rysunek 111).

Rysunek 111. Widok fragmentu Warszawy i opisów na *hoodmaps.com*

Podsumowanie i rady

- Rozpoznanie przemieszczania się osób, w tym także żołnierzy na misjach, staje się, niestety, coraz prostsze ze względu na częste używanie aplikacji i urządzeń typu *smart*, które zdradzają wiele, teoretycznie poufnych, danych wszystkim zainteresowanym użytkownikom Internetu.
- Często powiązanie informacji z map i zdjęć w aplikacjach z danymi uzyskanymi z analizy OSINT-owej pozwala zbudować bardzo dokładny obraz stylu życia osoby lub trybu pracy organizacji.
- Nie tylko Google posiada operatory wyszukiwania, które pozwalają na szybsze znalezienie interesujących informacji – wiele innych serwisów także ma swoje zestawy filtrów.

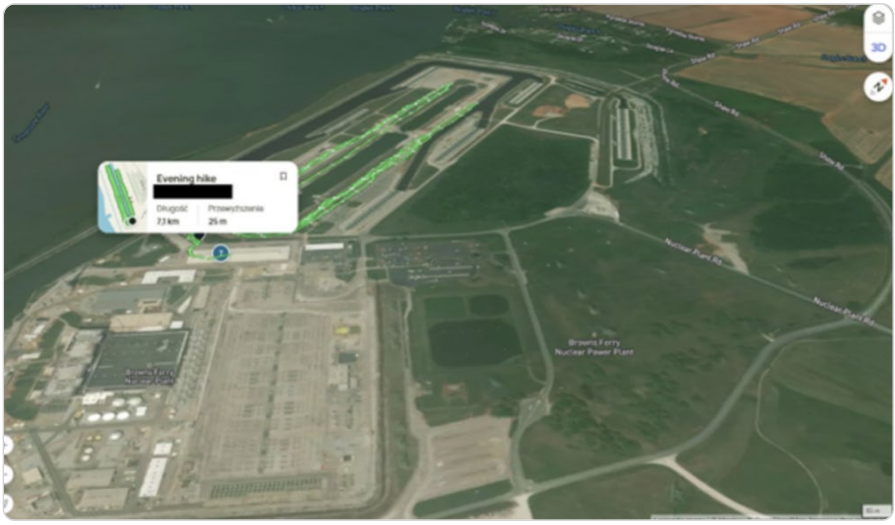
R21 ŚLEDZENIE OSÓB – JAK CZYTANIE Z OTWARTEJ KSIĄŻKI

Od czasu upublicznienia konsekwencji nierozważnego używania aplikacji Strava, kiedy na publicznie dostępnej mapie można było zobaczyć np. trasy przemieszczania się żołnierzy i pracowników ochrony wielu lokalizacji ważnych z punktu widzenia bezpieczeństwa (baz wojskowych czy ambasad), sytuacja wydawała się jasna. Tego typu działania mogą stanowić zagrożenie i publiczne udostępnianie takich informacji nie powinno mieć miejsca. Okazuje się jednak, że temat wkrótce się powtórzył.

Powrót problemów aplikacji do śledzenia tras biegów/wycieczek

8 marca 2023 roku na portalu Vice opublikowano artykuł[96] opisujący znaleziska rodzimego OSINT-owego badacza Wojciecha. Wskazał on, że dane dostępne w aplikacji AllTrails, służącej – podobnie jak Strava – do zapisywania tras biegów i wycieczek pieszych (rysunek 112[97]), ukazują dokładne miejsca pobytu wielu wysoko postawionych osób, w tym byłego przedstawiciela administracji amerykańskiego prezydenta Joe Bidena (ze względów bezpieczeństwa nie podano do wiadomości, o kogo chodzi). Pokazują one jego lokalizację w Białym Domu, a także mogą wskazywać na miejsce, w którym mieszka.

Sama aplikacja AllTrails chwali się posiadaniem ponad 45 milionów użytkowników, którzy wygenerowali ponad 1200 milionów kilometrów tras. Wojciech wskazuje także, że uzyskał interesujące rezultaty poprzez wyszukiwanie tras w okolicach Pentagonu, siedzib NSA, CIA oraz Białego Domu i analizę dalszego przemieszczania się wybranych użytkowników.



Rysunek 112. Trasa wokół elektrowni jądrowej Browns Ferry

Wspomniany wcześniej były wysoko postawiony przedstawiciel administracji Joe Bidena przebył właśnie m.in. drogę od Białego Domu do pobliskiego budynku mieszkalnego, mając włączoną aplikację, która zapisywała jego lokalizację. Zarejestrowane zostały także inne miejsca jego pobytu w Waszyngtonie, kiedy jeszcze pracował w otoczeniu prezydenta. Dziennikarze byli w stanie potwierdzić, że posiada aktywne konto w aplikacji, próbując zarejestrować się przy wykorzystaniu jego publicznie dostępnego adresu e-mail.

Gdzie leży przyczyna?

Gromadzenie wskazanych lokalizacji było możliwe poprzez niebezpieczne z punktu widzenia prywatności użytkowników **domyślne ustawienia, które powodują, że wszystkie zapisane miejsca pobytu stają się dostępne publicznie**. Taka konfiguracja sprzyja zbieraniu wielu interesujących informacji, co jest podstawą działania sieci społecznościowych, jednak aplikacja nie informowała użytkowników o tym fakcie w odpowiedni sposób, przez co wielu z nich mogło nie wiedzieć o takiej formie jej działania.

Nie jest to jednak problem tylko tej jednej aplikacji. Przeglądanie ustawień we wszystkich swoich kontach w serwisach społecznościowych, aplikacjach i systemach operacyjnych to ważny element **cyberhigieny***. Dzięki temu korzystające z nich osoby mogą znacznie zwiększyć prawdopodobieństwo, że **udostępniają za ich pośrednictwem jedynie wybrane przez siebie dane**. Niestety – niekiedy właściciele platform i aplikacji starają się za nas decydować o zasięgu udostępnianych informacji, a czasem także samowolnie zmieniają zakres ustawień prywatności, co powoduje, że niektóre z nich wracają do konfiguracji domyślnej. Taka sytuacja może mieć miejsce, kiedy np. z jednego ustawienia producent stworzy dwa nowe, które trzeba następnie samodzielnie odnaleźć i ustawić zgodnie z oczekiwaniami. To niestety oznacza konieczność cyklicznego przeglądania ustawień, co jest czasochłonne – nic więc dziwnego, że użytkownicy serwisów i aplikacji nie chcą tego robić. W końcu zamierzają korzystać z narzędzi, a nie ciągle na nowo je dostosowywać do swoich oczekiwań.

Co ciekawe, Wojciech w swoich badaniach wykorzystał autorskie narzędzie – Open Source Surveillance – które pozwala korzystać z bardzo obszernego zakresu danych udostępnianych przez różne serwisy społecznościowe i narzędzia, a następnie wizualizować je na mapie, co znacznie ułatwia korelację informacji (rysunek 113). W ramach swojego rozpoznania wskazał także inne interesujące lokalizacje, z których swoje pozycje do aplikacji przesyłali jej użytkownicy. Były to m.in.: bazy na pustyni Nevada, elektrownie jądrowe Browns Ferry w stanie Alabama i Palo Verde Generating Station w Arizonie, a także

* Więcej wskazówek, jak dbać o cyberhigienę, można uzyskać podczas szkoleń, m.in. OSINT/OPSEC.

bazy wojskowe w Nigrze i Kenii. Jak widać, zestaw danych nie ograniczał się jedynie do terenu Stanów Zjednoczonych.

Rysunek 113. Przykładowy widok mapy w narzędziu OS Surveillance wraz z informacjami i multimediami powiązanymi z danym obszarem

Anonimowe dane także można przypisać

W przypadku aplikacji AllTrails dane o przemieszczaniu się poszczególnych osób były powiązane z ich imieniem i nazwiskiem, co umożliwiało wskazanie, kto gdzie się porusza. Co jednak w przypadku, gdy możliwy jest dostęp jedynie do anonimowych danych o lokalizacji osób, bez przypisania ich do konkretnych imion i nazwisk? Okazuje się, że poprzez analizę miejsc, w których przebywa określona, teoretycznie anonimowa osoba, a także analizę czasową jej przemieszczania się, w wielu przypadkach można określić, z kim mamy do czynienia.

W ten sposób w 2019 roku dziennikarze „New York Timesa", którzy uzyskali dostęp do losowej próbki z ponad 50 miliardami lokalizacji zalogowanych przez telefony ponad 12 milionów Amerykanów, byli w stanie wyśledzić trasę przemieszczania się Donalda Trumpa[98]. Zaczęło się od jednej lokalizacji telefonu, wskazującej na pobyt w kurorcie Mar-a-Lago w Palm Beach, należącym właśnie do Trumpa (rysunek 114).

Rysunek 114. Trasa przemieszczania się Donalda Trumpa wskazana w śledztwie dziennikarzy „New York Timesa"

Telefon wraz z właścicielem przemieszczał się po terenie kurortu przez około godzinę od 7.10 rano, a następnie można go było zlokalizować w klubie golfowym, gdzie akurat ówczesny prezydent USA spotkał się na grę w golfa z ówczesnym premierem Japonii. Po południu właściciel telefonu udał się do kolejnego klubu golfowego, gdzie odbywało się przyjęcie dla światowych przywódców, po czym zakończył dzień z powrotem w Mar-a-Lago na kolacji z Shinzō Abe.

Na podstawie innych miejsc logowania się telefonu, w tym w okolicach siedziby United States Secret Service, dziennikarze założyli, że urządzenie musiało należeć do jednego z agentów. Z dostępnych danych możliwe było także określenie miejsca zamieszkania tej osoby, a więc dotarcie do jej danych osobowych. Instytucja nie odniosła się do znalezisk dziennikarzy. Temat wydaje się jednak szerszy i umożliwiający uzyskanie szczegółowych informacji o ogromnej liczbie osób, których dane lokalizacyjne są anonimowe, ale możliwe do deanonimizacji poprzez powiązanie ich z trasą przemieszczania się danego właściciela telefonu i czasem pojawiania się w określonych miejscach.

Podsumowanie i rady

- Coraz więcej osób korzysta z aplikacji do dzielenia się swoimi trasami biegów i wycieczek, jednak, jak widać, także dostęp do teoretycznie anonimowych danych może stanowić zagrożenie dla bezpieczeństwa osób lub instytucji, w których pracują.
- Na szczęście wgląd w te dane jest jeszcze dość mocno ograniczony i nie każdy może je analizować. Czy jednak wraz z rosnącą liczbą przypadków wycieków danych także te informacje staną się wkrótce ogólnodostępne? Czas pokaże, jednak już dzisiaj warto przejrzeć ustawienia swoich aplikacji, aby upewnić się, że udostępniamy tylko taki zakres danych, z którego upublicznieniem czujemy się komfortowo.

R22 O JEDEN OSINT ZA DALEKO, CZYLI PRZYKRE SKUTKI ZŁYCH ANALIZ

Zainteresowanie tematyką OSINT-u w ostatnich latach gwałtownie rośnie. Wraz z coraz większą liczbą możliwości przeprowadzania śledztw z wykorzystaniem otwartych źródeł informacji rośnie też grono *Internet sleuths*, czyli internetowych detektywów.

Z jednej strony, taki kierunek jest bardzo dobry, gdyż większa liczba śledczych jest w stanie weryfikować prawdziwość podawanych informacji medialnych lub pomagać w poszukiwaniu osób zaginionych. Z drugiej strony, niekiedy jednak sprawy zachodzą za daleko i tropiciele informacji częściowo lub kompletnie pomijają aspekt ich odpowiedniej analizy i weryfikacji. Chęć

szybkiego zabłyśnięcia w sieci i natychmiastowego ukarania domniemanych sprawców przestępstw lub wykroczeń wygrywa ze zdrowym rozsądkiem. **Wynikiem takiej drogi na skróty są często tragedie osób niesłusznie oskarżonych lub wykonywane na nich samosądy**. Nie chcę absolutnie zniechęcać nikogo do tropienia sprawców różnej maści występków, ale pragnę zachęcić do chłodnej analizy lub przekazywania zdobytych informacji kompetentnym przedstawicielom służb odpowiedzialnych za działania mające na celu schwytanie i osadzenie właściwych osób. Przedstawiciele FBI coraz częściej proszą świadków wydarzeń, w ramach których prowadzą śledztwa, o przesyłanie zdjęć i filmów mogących przyczynić się do identyfikacji poszukiwanych osób, jednak wielu poszukiwaczy wykracza swoimi działaniami daleko poza „podesłanie materiałów".

Poszukiwania zamachowców

15 kwietnia 2013 roku podczas maratonu w Bostonie miał miejsce zamach bombowy z wykorzystaniem dwóch ładunków domowej roboty. Zginęły wtedy trzy osoby, a ponad 260 zostało rannych. Krótko po tych wydarzeniach pojawiła się prośba służb o podzielenie się przez świadków wszelkimi dostępnymi nagraniami i zdjęciami, a chwilę potem w Internecie rozpoczęło się „polowanie na czarownice". Na utworzonym tylko w tym celu podforum Reddita (Subreddit) ponad trzy tysiące osób dzieliło się posiadanymi informacjami[99] i na podstawie różnych tropów starało się znaleźć zamachowców (rysunek 115).

Rysunek 115. Fragment dyskusji zamieszczanych w serwisie Reddit dotyczących poszukiwania zamachowców z Bostonu; obecnie dyskusje dostępne są tylko w archiwum Internetu (*The Wayback Machine*)

Zdjęcia krążyły także po innych serwisach, takich jak: Facebook, Twitter czy 4chan. W wyniku prób dopasowania osób ze zdjęć do własnych teorii (ktoś nie patrzył na trasę biegu, ktoś inny miał zwisający plecak, a jeszcze ktoś miał po prostu inny kolor skóry) wskazywano jako sprawców niewinne osoby. Pierwszą z nich był 22-latek Sunil Tripathi, z którym rodzina nie miała kontaktu już

od połowy marca. Jak się później okazało, nie mógł on być w Bostonie w dniu zamachu, ponieważ w tym momencie już nie żył – najprawdopodobniej popełnił samobójstwo jeszcze przed maratonem. Forumowicze z serwisu Reddit przeprosili rodzinę, ale chyba nie trzeba nikomu tłumaczyć, jak taka sytuacja musiała dotknąć już i tak straumatyzowanych bliskich zmarłego.

W toku dalszego śledztwa na pierwszej stronie „New York Post" znalazły się kolejne dwie osoby (rysunek 116), omyłkowo zidentyfikowane jako poszukiwane przez FBI. Tutaj także okazało się, że sfotografowana dwójka nie miała nic wspólnego z atakiem, a sprawa zakończyła się wytoczonym gazecie procesem o zniesławienie. FBI w końcu namierzyło dwóch braci uznanych za faktycznych (według oficjalnych doniesień) sprawców, przy czym jeden z nich zginął podczas pościgu. Drugi, pomimo odniesionych ran, przeżył i został postawiony przed sądem.

Rysunek 116. Pierwsza strona „New York Post" ze zdjęciem dwóch osób posądzanych o związek z zamachem

Nie tylko błędnie zinterpretowane obrazy mogą być przyczyną bezpodstawnych oskarżeń.

W przypadku pewnego Sikha z Kanady, Veerendera Jubbala, przerobione w programie graficznym zdjęcie stało się podstawą oskarżenia go o spowodowanie zamachów w Paryżu i Nicei w 2015 i 2016 roku. Żeby było jeszcze ciekawiej, nigdy nie był on nawet we Francji. Nie przeszkodziło to jednak w uznaniu go za zamachowca przez hiszpańską gazetę „La Razón" i umieszczeniu jego zdjęcia na pierwszej stronie (rysunek 117). Gazeta po jakimś czasie wystosowała przeprosiny[100], ale idea, która raz trafi do Internetu, nie umiera zbyt szybko.

Rysunek 117. Wpis na Twitterze wskazujący na niesprawiedliwe oskarżenie Veerendera Jubbala o atak w Nicei

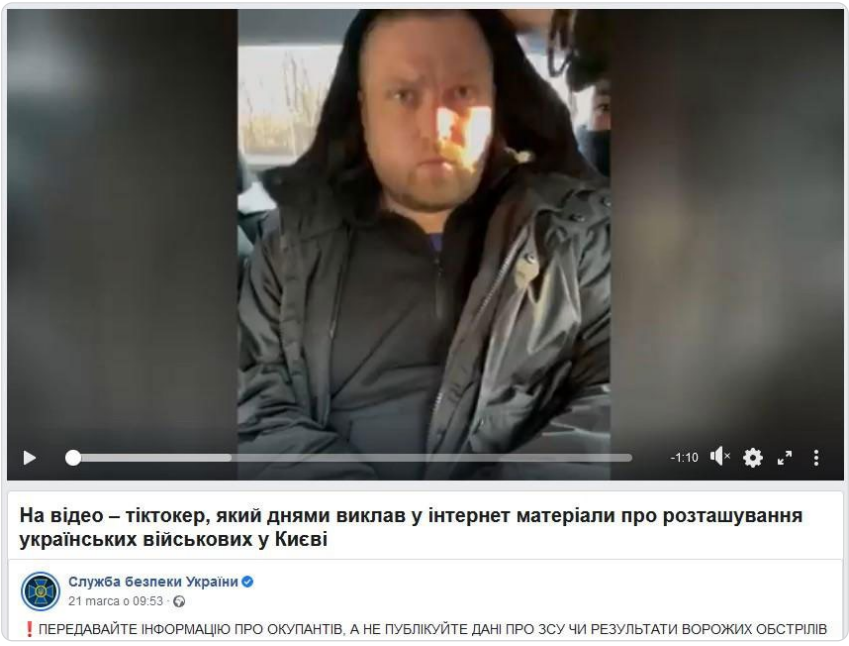
Zmodyfikowane zdjęcie Jubbala było podawane dalej, mimo że wprowadzone dodatki, mające zrobić z niego terrorystę, nie były zbyt dobrze wykonane, a wprawne oko byłoby w stanie zauważyć elementy wskazujące na fakt, że zdjęcie zostało wykonane w USA. Techniki analizy tak spreparowanych elementów nie są umiejętnościami szczególnie trudnymi do opanowania, istotniejsze jest tutaj nastawienie, by wszystko krytycznie oceniać, a już z pewnością to, co wydaje się oczywiste.

Udostępnianie zdjęć wojskowych

Wiele kontrowersji wzbudzało dzielenie się przez członków społeczności Internetu zdjęciami i filmami obrazującymi ruchy wojsk rosyjskich i ukraińskich w trakcie pierwszych dni wojny w Ukrainie. Przedstawiciele wojska (i nie tylko) wskazywali, że takie udostępnianie informacji może prowadzić do narażania zdrowia i życia żołnierzy, a także wpływać na powodzenie misji. Szczególnie po stronie Ukrainy i krajów zachodnich widoczne było prowadzenie wielu akcji informacyjnych w tym zakresie. Nie wszyscy jednak byli świadomi potencjalnych skutków swoich działań.

W początkowej fazie konfliktu pewien ukraiński tiktoker opublikował film pokazujący pojazdy wojskowe parkujące pod centrum handlowym na przedmieściach Kijowa. Niedługo później na to miejsce spadły rosyjskie pociski, zabijając osiem osób. Po tym wydarzeniu Służba Bezpieczeństwa Ukrainy

opublikowała na swoim profilu na Facebooku film, w którym tiktoker przeprasza (rysunek 118[101]) wszystkich i przestrzega, żeby nie powtarzać jego błędów. Zamiast publikowania zdjęć i filmów w Internecie obywatele Ukrainy byli zachęcani do wskazywania podejrzanych osób i zdarzeń poprzez aplikację Diia, która dotychczas służyła do przechowywania cyfrowej wersji dokumentów, certyfikatów COVID-owych czy korzystania z serwisów rządowych (w Polsce podobną funkcję pełni aplikacja mObywatel).



Rysunek 118. Opublikowane na Facebooku nagranie z przeprosinami ukraińskiego tiktokera

Także serwisy zajmujące się weryfikacją i dokumentacją konfliktu w Ukrainie zwróciły się do internautów o zasilanie ich baz informacjami zamiast publikowania ich bez wcześniejszej analizy. Przykładem takiego serwisu jest chociażby Centre for Information Resilence, które tworzy mapę Eyes on Russia Map, agregującą zweryfikowane i zlokalizowane wydarzenia dotyczące walk w Ukrainie. Tego typu inicjatywa zapewnia, że informacje przed publikacją zostaną gruntownie sprawdzone, a wszystkie wydarzenia odpowiednio udokumentowane w celu późniejszego wykorzystania ich przez dziennikarzy czy badaczy.

Poszukiwanie sprawców ataku na Kapitol

W USA po ataku na Kapitol 6 stycznia 2021 roku, którego koszty oszacowano na 1,5 miliona dolarów (nie licząc strat wizerunkowych i skutków dostępu do wrażliwych informacji przez osoby niepowołane), FBI rozpoczęło poszukiwania sprawców tego zajścia. Na podstawie ogromnej liczby zdjęć i filmów,

niejednokrotnie publikowanych przez samych demonstrantów, udało się dotychczas aresztować niemal 800 osób, a ponad 350 jest nadal poszukiwanych[102]. FBI zwróciło się z prośbą o pomoc w identyfikacji przedstawionych na zdjęciach i filmach osób, jednocześnie dziękując za wiele cennych wskazówek, które otrzymało z całego kraju. Dodatkowo FBI i ATF (agencja zajmująca się przepisami i przestępstwami dotyczącymi alkoholu, tytoniu, broni palnej oraz materiałów wybuchowych) wyznaczyły do 100 tysięcy dolarów nagrody[103] za przekazanie informacji, które doprowadzą do zlokalizowania, aresztowania i skazania osoby lub osób, które podłożyły bomby rurowe w przeddzień ataku na Kapitol. W przypadku tego śledztwa wskazówki przekazywane przez zwykłych obywateli okazały się bardzo cenne, chociaż nie zabrakło także przypadków omyłkowego wskazania przez użytkowników mediów społecznościowych emerytowanego strażaka[104] jako sprawcy śmiertelnego zranienia jednego z policjantów podczas opisywanego ataku. Jak się później okazało, ów mężczyzna w tym czasie był daleko od Waszyngtonu i świętował urodziny swojej żony. Dopiero później prawdziwy sprawca tego zajścia został złapany i postawiono mu zarzuty, ale do tego czasu ofiara błędnej identyfikacji musiała korzystać z ochrony policyjnej.

Internet zna wiele przypadków nieprawidłowo prowadzonych śledztw, które spowodowały jeszcze większe tragedie niż te będące ich podstawą. Sprawy przedstawione w tym rozdziale mają jedynie na celu wskazanie, jak daleko można się posunąć, prowadząc prywatne śledztwa. Nie oznacza to jednak, że nie należy wykonywać takich działań wcale. Ważne jest jedynie, aby nie dać się ponieść emocjom. **Osoba, która prowadzi tego typu śledztwo, musi znać zasady poprawnej analizy dowodów i faktów, a także zdystansować się emocjonalnie od przedmiotu swoich działań**. Jedynie wtedy możliwe będzie wyciągnięcie poprawnych wniosków i wskazanie tylko tych osób, które naprawdę mają związek z daną sprawą. Tego życzę wszystkim wykorzystującym swoje zdolności OSINT-owe w dobrym celu.

Podsumowanie i rady

- Coraz więcej osób poznaje techniki prowadzenia śledztw OSINT-owych w Internecie, co samo w sobie zwiększa świadomość społeczeństwa oraz możliwości weryfikacji informacji i pomocy organom ścigania.
- Brak odpowiedniego przygotowania i chęć „zabłyśnięcia” wśród współużytkowników mediów społecznościowych i innych portali często prowadzą do błędnych wniosków i oskarżenia niewinnych osób.
- Organy ścigania, a także wiele organizacji zwraca się do internautów o pomoc, jednak proces weryfikacji zgromadzonych danych leży już po stronie bardziej doświadczonych śledczych. Warto angażować się w tego typu akcje i pomagać, jednak w ramach ustalonych zasad.

CZĘŚĆ II: OSINT – NARZĘDZIA

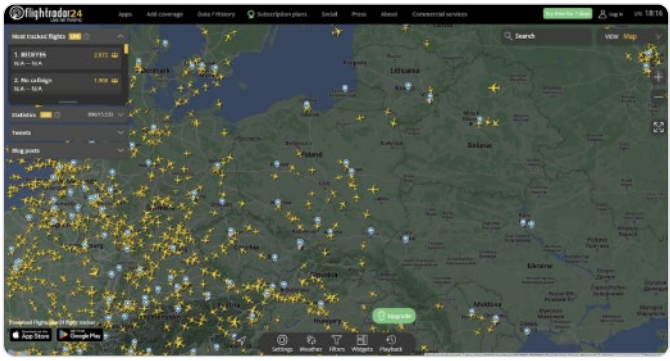
R23 JAK STWORZYĆ WŁASNY OSINT-OWY LAB DO ŚLEDZENIA SAMOLOTÓW I INNYCH OBIEKTÓW LATAJĄCYCH

Do tej pory poruszałem tematy związane z pozyskiwaniem danych z otwartych źródeł internetowych. Są jednak jeszcze inne źródła, z których można skorzystać, aby zdobyć interesujące dane do analiz OSINT-owych. Mam tu na myśli ogólnodostępną i otwartą komunikację radiową, którą wykorzystują obiekty latające, pływające, a także satelity. To dzięki temu, że jest to komunikacja nieszyfrowana, możliwe jest stworzenie własnego OSINT-owego laboratorium, przekazującego informacje o tym, co dzieje się wokół nas*. Przyjrzymy się teraz dokładniej komunikacji dotyczącej samolotów i innych statków powietrznych.

Źródła danych

Jednym z najpopularniejszych serwisów udostępniających informacje o ruchu lotniczym jest z pewnością Flightradar24 (rysunek 119). Jego historia rozpoczęła się w 2006 roku od inicjatywy dwóch miłośników lotnictwa, którzy stworzyli sieć odbiorników ADS-B w Europie. Dzisiaj serwis obejmuje niemal cały świat dzięki danym udostępnianym mu z wielu źródeł, należących zarówno do organów odpowiedzialnych za kontrolę lotów (np. amerykańska FAA, Federal Aviation Authority), jak i do zwykłych użytkowników, wyposażonych w odbiorniki radiowe, które można zbudować samemu lub otrzymać za darmo od Flightradar24 (szczególnie jeśli mieszka się w okolicy lotniska). Minusem tego serwisu jest ograniczona liczba informacji, które można uzyskać w wersji darmowej. Na przykład, aby dowiedzieć się, jaki kod transpondera (ang. *squawk*) aktualnie nadaje dany obiekt lub poznać historię lotów starszą niż siedem dni, należy wykupić płatny plan (lub zostać jedną z osób dostarczających do portalu dane z własnego odbiornika).

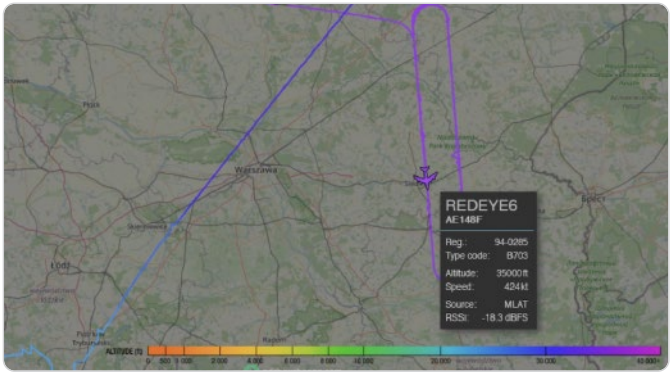
* Rozdział został napisany z punktu widzenia osoby zajmującej się pozyskiwaniem danych, stąd w tekście pojawiają się pewne uogólnienia lub uproszczenia w tematyce lotniczej i radiowej. Z pewnością można by te tematy opisać bardziej szczegółowo i precyzyjnie, jednak nie to było założeniem Autora.



Rysunek 119. Przykładowy widok nieba nad Polską w portalu Flightradar24

Podobnym serwisem jest FlightAware, który oferuje użytkownikom możliwość zakupu gotowych urządzeń do śledzenia ruchu lotniczego.

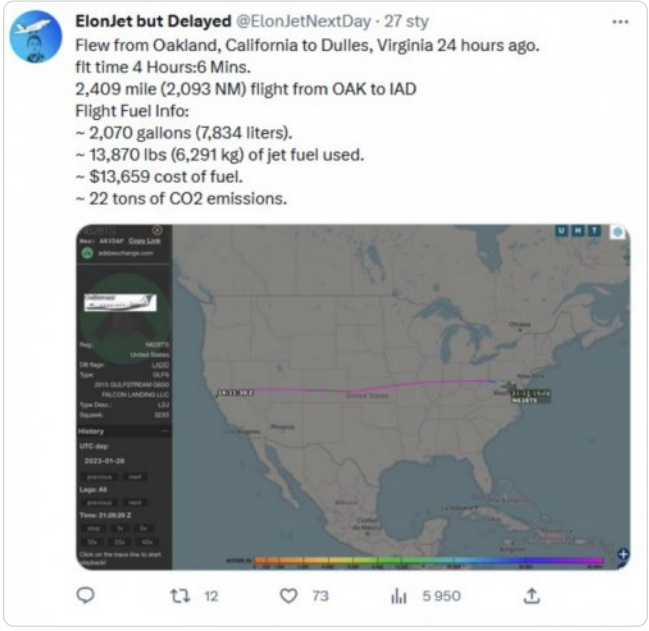
Wśród innych serwisów udostępniających informacje o ruchu lotniczym należy na pewno wskazać serwis ADS-B Exchange (rysunki 120 i 121), który sam siebie określa jako największe źródło niefiltrowanych danych lotniczych na świecie. W przeciwieństwie do innych, płatnych serwisów, korzysta jedynie z danych otrzymanych z odbiorników sieci swoich użytkowników, ale także nie usuwa żadnych danych, nie zmienia i nie estymuje ich. Jeśli uzyskuje jakieś informacje, wyświetla je na mapie i nie ma możliwości ich usunięcia lub zablokowania. Korzystając z łatwo dostępnych filtrów mapowych, można uzyskać np. widok jedynie wojskowych jednostek. I to bez żadnych opłat. To sprawia, że serwis ADS-B Exchange wielokrotnie pomógł śledczym z całego świata zdobyć informacje m.in. o przemytnikach i porywaczach. W związku z faktem, że dane przesyłane za pomocą technologii ADS-B są nieszyfrowane, wiele osób (w tym Elon Musk, a także saudyjska rodzina królewska czy rząd Chin) stara się walczyć z tego typu ogólnodostępnymi źródłami danych, które ujawniają trasy ich samolotów.



Rysunek 120. Trasa przelotu jednego z samolotów rozpoznawczych, które ostatnio dość często można zaobserwować na polskim niebie, dostępna w portalu ADS-B Exchange

Rysunek 121. Przykładowy widok nieba nad Polską w portalu ADS-B Exchange

Najpopularniejszym miejscem udostępniania aktualnych danych o flocie Elona Muska jest konto @ElonJet, prowadzone przez Jacka Sweeneya, które zostało już zablokowane w portalu X, jednak jest nadal dostępne na Facebooku, Instagramie czy Mastodonie. Sweeney korzysta właśnie z danych z ADS-B, aby automatycznie generować wpisy na portale społecznościowe z informacjami o lotach właściciela X, który swego czasu oferował mu 5000 dolarów za usunięcie konta. Kontroferta opiewała na 50 000 dolarów i nie została przyjęta. Aktualnie Sweeney utrzymuje na X konto ElonJet but Delayed (rysunek 122), które publikuje dane z 24-godzinnym opóźnieniem, co według zasad portalu nie stanowi już zagrożenia dla osoby, której te dane dotyczą.



Rysunek 122. Jeden z wpisów konta ElonJet but Delayed w portalu X

Żeby jednak nie było tak różowo, 25 stycznia 2023 roku portal ADS-B Exchange został zakupiony przez firmę Jetnet, co wzburzyło zarówno osoby zasilające go danymi, jak i zwykłych użytkowników, ponieważ może to oznaczać koniec darmowego dostępu do niefiltrowanych danych i zmianę ADS-B Exchange w kolejne z wielu niepełnych i płatnych źródeł informacji.

Trochę teorii

Zanim jednak przejdziemy do budowy własnego środowiska badawczego, przybliżę kilka terminów, których znajomość jest niezbędna do analizy ruchu lotniczego. Nie będę wchodził w szczegóły, gdyż są one potrzebne jedynie do zrozumienia kontekstu prowadzonych działań. Najpierw musimy się cofnąć nieco w czasie do momentu, kiedy zaczęto korzystać z radarów do monitorowania nieba.

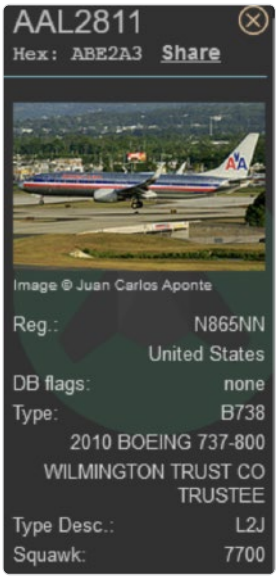
Pierwsze radary były urządzeniami wysyłającymi impulsy o wysokiej częstotliwości i nasłuchującymi impulsów odbitych. Dzięki temu były w stanie poinformować operatora o obecności w danym miejscu obiektów latających. Nie miały jednak możliwości zidentyfikowania statku, więc podczas drugiej wojny światowej w Anglii zaczęto używać radarów wtórnych, w celu odróżnienia, czy przypadkiem wraz z samolotami wracającymi z europejskiego frontu nie próbują się tam dostać samoloty Luftwaffe. Aby tego dokonać, opracowano system identyfikacji swój–obcy (ang. *Identification Friend or Foe*, IFF). Samoloty aliantów zostały wyposażone w transpondery (ang. *transmitter* + *responder*), dzięki czemu mogły odpowiadać na sygnały wysyłane przez radar SSR (Secondary Surveillance Radar) i były identyfikowane jako „swój". Nazwa IFF była stosowana przez Amerykanów, natomiast Brytyjczycy nadali systemowi nazwę Parrot (papuga), co zaowocowało późniejszym określeniem dla kodów transpondera, wysyłanych przez samoloty, jako ***squawk***, czyli ptasi skrzek. Określenie to jest stosowane do dzisiaj i oznacza **czterocyfrowe ciągi w zapisie ósemkowym**, tzn. na każdej pozycji mogą być cyfry od 0 do 7, co daje w sumie 4096 kombinacji.

Organizacja ICAO (International Civil Aviation Organization), odpowiedzialna m.in. za opracowywanie i wdrażanie międzynarodowych przepisów dotyczących bezpieczeństwa w cywilnym ruchu lotniczym, określiła także zestaw standardowych kodów transpondera, które mogą (choć nie zawsze muszą) oznaczać sytuacje awaryjne. Warto je znać, planując śledzenie ruchu lotniczego.

Trzy najważniejsze łatwo jest zapamiętać poprzez zrymowanie angielskiej wymowy ich pierwszych cyfr:

- 7500 – porwanie (*seven-five – man with knife*),
- 7600 – problemy z komunikacją/awaria radia (*seven-six – radio fix*),
- 7700 – sytuacja poważnego zagrożenia (*seven-seven – go to heaven*).

Niekiedy kod 7700 (rysunek 123) jest ustawiany także dla niekrytycznych przypadków, kiedy załoga rozpracowuje już problem, ale chce także dać znać kontroli lotów, że coś jest nie tak.

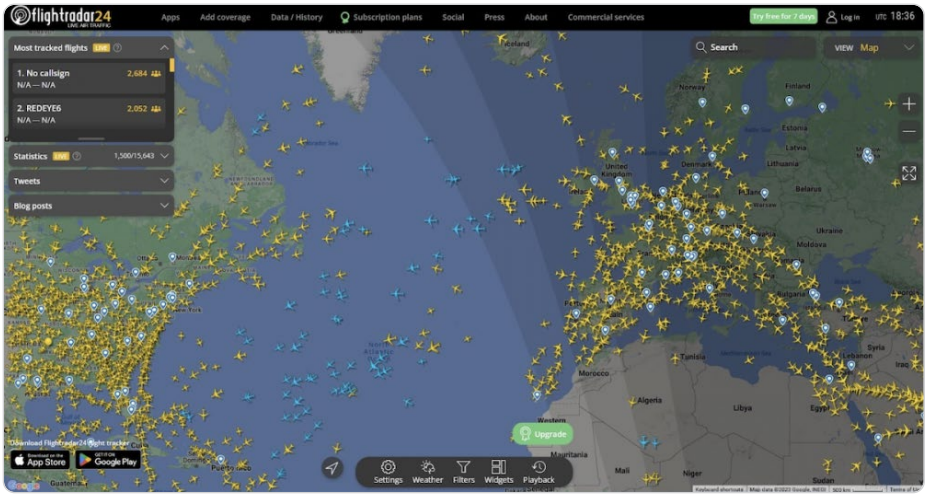


Rysunek 123. Samolot, który ustawił kod transpondera 7700, widoczny w portalu ADS-B Exchange

Do przekazywania większej ilości informacji niż tylko kod transpondera używana jest dzisiaj m.in. technologia ADS-B, czyli Automatic Dependent Surveillance – Broadcast. Umożliwia ona informowanie innych statków powietrznych oraz kontroli lotów m.in. o swojej pozycji, unikalnym 24-bitowym numerze samolotu, znaku wywoławczym lotu, jego kierunku oraz prędkości jednostki. System wysyłający te informacje określa się jako ADS-B out, a system odbioru danych z innych statków powietrznych – jako ADS-B in. Dane te są przesyłane w odstępach półsekundowych na częstotliwości 1090 MHz w formie otwartej i dostępne dla każdego, kto znajdzie się w wystarczającej odległości, aby je odebrać. Maksymalnie wynosi ona 450 kilometrów.

Portal Flightradar24 szczyci się posiadaniem ponad 20 tysięcy odbiorników niemal na całym świecie. Nie wszystkie statki powietrzne są jednak wyposażone w nadajniki ADS-B; niektóre z nich posiadają starsze urządzenia nadające w Mode-S – wtedy ich położenie może być określone za pomocą multilateracji (MLAT), czyli obliczania punktu w przestrzeni z wykorzystaniem różnic czasowych pomiędzy sygnałami otrzymanymi przez minimum cztery odbiorniki. Problemem są także obszary nad oceanami, gdzie komunikacja jest realizowana przy wykorzystaniu ADS-C (Automatic Dependent Surveillance – Contact). W tym przypadku transmisję bezpośrednią ze statkiem powietrznym

kontroluje stacja naziemna, a dane są przesyłane drogą satelitarną w dłuższych odstępach czasu (rysunek 124).



Rysunek 124. Niebieski kolor obiektu oznacza komunikację poprzez satelitę, żółty – poprzez stacje naziemne. W przypadku nadawania kodów o sytuacji wyjątkowej obiekt byłby zaznaczony na czerwono (Flightradar24)

Własne laboratorium

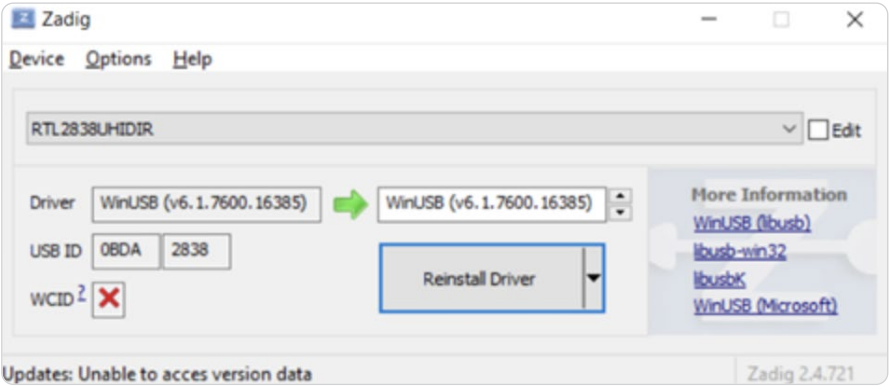
Sprzęt

Aby samemu odebrać transmisję z ADS-B, wystarczy zwykły, tani odbiornik SDR (Software Defined Radio) z interfejsem USB. Na komputerze należy zainstalować oprogramowanie dekodujące i wyświetlające przesyłane informacje, które później będzie można zwizualizować na mapie. Osobom zainteresowanym podstawami wykorzystania radia SDR polecam transmisję na ten temat na kanale SekurakTV[105].

Odbiornik RTL-SDR (rysunek 125), bazujący na zwykłym tunerze telewizyjnym, kosztuje aktualnie od kilkudziesięciu do kilkuset złotych, w zależności od zawartości zestawu. Można użyć także innego urządzenia odbiorczego, np. SDRplay, ale wiąże się to z większym wydatkiem i będzie wymagało wykorzystania innego oprogramowania do dekodowania sygnałów ADS-B. Dla naszych potrzeb wystarczy RTL-SDR, który ma możliwość obsługi częstotliwości 1090 MHz. Osobiście do testów korzystałem właśnie z tego rozwiązania. Należy jednak zwrócić szczególną uwagę, czy dana wersja na pewno jest oryginalna, ponieważ podrobiona może nie obsługiwać pożądanego zakresu częstotliwości. Szczegółową instrukcję, jak rozpoznać takie wersje tego urządzenia, można znaleźć na stronie *rtl-sdr.com*.

Rysunek 125. Odbiornik RTL-SDR

Do poprawnego działania RTL-SDR może być konieczne nadpisanie jego sterownika z wykorzystaniem programu Zadig. Procedura ta została opisana na stronie RTL-SDR Quick Guide, jednak tym, którzy nie mają doświadczenia w tego typu działaniach, polecam przeczytanie bardzo dokładnie tego poradnika i trzymanie się wszystkich jego zaleceń lub poproszenie o pomoc bardziej doświadczoną osobę. Należy być bardzo uważnym, gdyż, niestety, jednym kliknięciem w nieodpowiednim miejscu można nadpisać np. sterownik od myszki, touchpada lub innego urządzenia (rysunek 126).



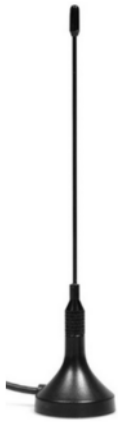
Rysunek 126. Ustawienia do nadpisania sterownika w programie Zadig

Do zestawu będzie potrzebna jeszcze antena. Dostępnych jest tu naprawdę dużo możliwości, w zależności od budżetu, pożądanego zasięgu oraz własnych zdolności manualnych (jeśli chcemy taką antenę stworzyć samemu). Przetestowałem kilka konstrukcji: od wersji typu KD („kawał drutu") po anteny, które pożyczyłem od znajomych zajmujących się profesjonalnie przechwytywaniem różnego rodzaju sygnałów elektromagnetycznych. Zadowalające efekty, czyli zasięg kilkudziesięciu kilometrów, udało mi się osiągnąć na zwykłej antenie od tunera telewizyjnego, umieszczonej za oknem (rysunek 127).

Dla osób, które nie chcą się zastanawiać, co powinny kupić, i są gotowe w związku z tym zapłacić trochę więcej, rozwiązaniem będzie skorzystanie z oferty sklepu w portalu FlightAware, oferującego gotowe zestawy.

Software

Aby móc odkodować przesyłane informacje, można skorzystać z oprogramowania typu RTL1090 (rysunek 128) lub Dump1090 (listing 1). Warto przeczytać instrukcję instalacji[106] pierwszego z nich. Jeśli Czytelnicy napotkają problem z brakiem dostępności wskazanego pliku `RelWithDebInfo.zip`, należy go pobrać z Archiwum Internetu*. Opisywane w tym rozdziale środowisko budowałem na systemie Windows 10, jednak z oprogramowania Dump1090 można skorzystać także w systemie Linux.



Rysunek 127. Podczas testów wystarczająca okazała się niewielka antena od tunera telewizyjnego

Rysunek 128. Okno programu RTL1090

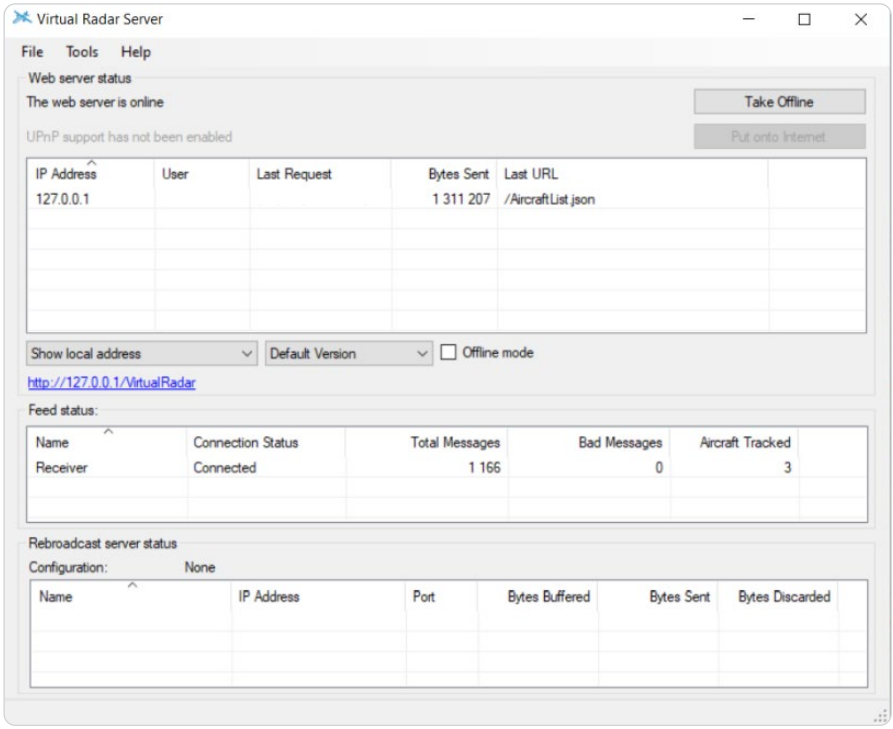
Listing 1. Uruchomiony program Dump1090 pod systemem Windows z domyślnymi ustawieniami serwowania danych. Widoczne są dwa przechwycone samoloty wraz z przesyłanymi przez nie informacjami

```
Hex     Mode  Sqwk  Flight   Alt    Spd  Hdg  Lat     Long    Sig  Msgs  Ti-
------------------------------------------------------------------------------
471F78  S     1371  WZZ1784  38025  374  346  54.250  17.800  4    315   34
4AB4EB  S     2226  SEMGK    28000  251  332  53.736  19.020  4    1193  0
```

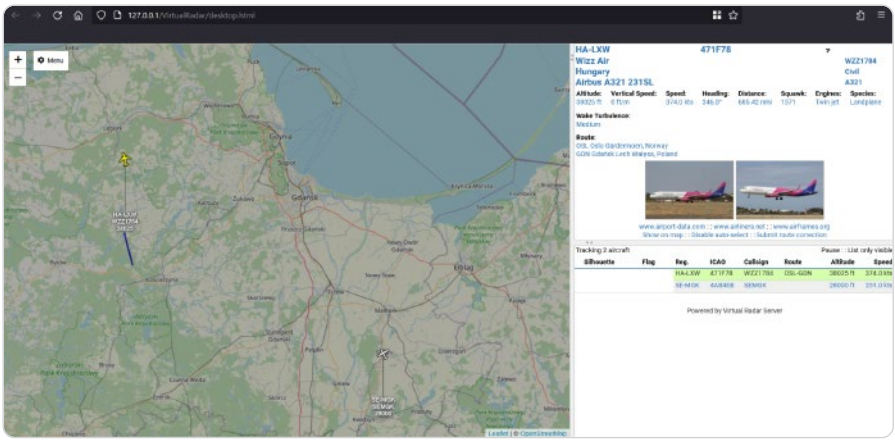
Dump1090 ma opcję wyświetlania danych na mapie, jednak nie udało mi się jej uruchomić. Skorzystałem za to z Virtual Radar Server (rysunek 129). Po jego instalacji konieczne było uruchomienie Dump1090 tak, aby serwował odbierane

* Hoernchen, File RelWithDebInfo.zip.

dane, co można osiągnąć, uruchamiając plik `dump1090.bat`, z domyślną konfiguracją. Następnie należy włączyć oprogramowanie Virtual Radar Server i otworzyć w przeglądarce stronę pod adresem *http://127.0.0.1/VirtualRadar*, na której można zobaczyć na mapie uchwycone statki powietrzne (rysunek 130).



Rysunek 129. Okno programu Virtual Radar Server



Rysunek 130. Widok mapy i dwóch przechwyconych samolotów w oknie przeglądarki VirtualRadar

Podsumowanie i rady

Podążając za omówionym powyżej schematem, można przygotować domowe środowisko do śledzenia ruchu lotniczego w zasięgu anteny. Tego typu sprzęt można także wykorzystywać do pozyskiwania innych informacji, dotyczących np. położenia jednostek pływających (z użyciem komunikacji AIS). W przypadku zainwestowania w nieco lepszy odbiornik i antenę warto pokusić się nawet o pobieranie map z satelitów przelatujących akurat nad nami, jednak wymaga to także terenu, na którym można bez problemu rozłożyć nieco większą antenę. Takie samodzielne gromadzenie i wizualizowanie danych daje wiele satysfakcji, której może zabraknąć, jeśli dane zostaną pozyskane z Internetu, podane niejako „na talerzu".

R24 GHUNT, CZYLI JAK WYCISNĄĆ JAK NAJWIĘCEJ INFORMACJI Z PROFILU GOOGLE

Wiadomo, że jeśli prowadzi się śledztwa OSINT-owe, Google jest nieprzebraną skarbnicą wiedzy. Można tam łatwo wyszukać informacje przy użyciu Google Dorks: narzędzia, które odpowiednio wyfiltruje pożądane dane z oceanu informacji. Ale czy da się w prosty sposób otrzymać skondensowane dane o osobie, znając tylko jej adres e-mailowy? Jeśli jest on powiązany z kontem Google, to okazuje się, że tak.

Czym jest GHunt?

GHunt to narzędzie stworzone w języku Python, opublikowane w 2020 roku przez programistę o ksywce mxrch. Pozwala ono na wyszukanie dostępnych w profilu Google informacji o danej osobie na podstawie jej adresu e-mailowego. I nie musi to być adres Gmail, może to być konto w domenie firmowej, o ile zostało powiązane z kontem Google.

Wśród danych, które można w ten sposób znaleźć, są m.in.: imię i nazwisko właściciela konta, Google ID, data ostatniej aktualizacji profilu, usługi Google połączone z kontem, prawdopodobne inne nazwy użytkownika danej osoby, modele telefonu wyczytane z metadanych czy informacje pozostawione na mapach Google. Dane przy okazji są analizowane, jeśli chodzi np. o określenie prawdopodobnego miejsca zamieszkania konkretnej osoby. I to wszystko, po kilku–kilkunastu sekundach, jest dostępne w jednym miejscu (rysunki 131 i 132).

```
g:\Ghunt>python hunt.py [redacted]@gmail.com
[+] 1 account found !

----------------------------

Name: J[redacted]

Last profile edit : 2020/09/05 [redacted](UTC)

Email : [redacted]@gmail.com
Google ID : 11[redacted]

Hangouts Bot : No

Activated Google services :
- Youtube
- Photos
- Maps

Youtube channel (confidence => 37.5%) :
- [redacted] https://youtube.com/channel/[redacted]
- [redacted] https://youtube.com/channel/
- [redacted] https://youtube.com/channel/
- [redacted] https://youtube.com/channel/
- [redacted] https://youtube.com/channel/
- [redacted] https://youtube.com/channel/
- [redacted] https://youtube.com/user/
- [redacted] https://youtube.com/user/
- [redacted] https://youtube.com/channel/
- [redacted] https://youtube.com/channel/
- [redacted] https://youtube.com/channel/
- [redacted] https://youtube.com/channel/

Possible usernames found :
- [redacted]
- [redacted]

Google Photos : https://get.google.com/albumarchive/11[redacted]
=> No album

Google Maps : https://www.google.com/maps/contrib/11[redacted]/reviews
=> 1 reviews found !

Probable location (confidence => Very low) :
- [redacted], United States of America
```

Rysunek 131. Dane o przykładowej osobie pozyskane na podstawie tylko jej adresu e-mailowego. Oczywiście, ze względu na obowiązujące RODO, dane zostały zanonimizowane (GHunt)

```
Google Photos : https://get.google.com/albumarchive/11[redacted]
=> 2 albums, 1 photos

Searching metadata...
[+] 1 device found !

- Huawei ALE-L21 (1 pic) [2017/02/22]
-> 1 Firmware found !
--> ALE-L21C432B170 [2017/02/22]
```

Rysunek 132. Czasami udaje się też odnaleźć w metadanych informacje o modelu telefonu (GHunt)

ChromeDriver

Narzędzie wymaga uruchomienia lokalnie i potrzebuje do działania kilku składników: środowiska Python 3.6.1+, przeglądarki Chrome oraz ChromeDrivera do platformy Selenium, z której korzysta. Warto tutaj pamiętać, że ChromeDriver musi być z tej samej linii, co wersja zainstalowanej przeglądarki Chrome.

Po pobraniu narzędzia GHunt z serwisu GitHub[107] do katalogu należy wgrać ChromeDriver i skonfigurować ciasteczka, które są wymagane do pozyskiwania informacji. Oprogramowanie podczas konfiguracji praktycznie prowadzi użytkownika „za rękę", a dodatkowo na GitHubie można znaleźć dokładnie pokazane krok po kroku, w jaki sposób „zdobyć" potrzebne ciasteczka. Twórca narzędzia sugeruje, aby na potrzeby działania narzędzia używać osobnego konta Google, gdyż użycie w nim ciasteczek konta może skończyć się zablokowaniem dostępu do niego na danej maszynie.

Podsumowanie

Co do samego działania narzędzia GHunt, trzeba powiedzieć, że jego twórca wykonał kawał dobrej roboty, skracającej do minimum czas poszukiwania podstawowych danych o właścicielu konta. Od czasu jego powstania nie nastąpiły w nim jednak wielkie zmiany i jego twórca wskazuje, że aktualnie dostępna jest wersja *online* GHunt w ramach „kombajnu" do poszukiwań OSINT-owych, którym staje się OSINT Industries. Podobny zestaw funkcjonalności oferuje obecnie także narzędzie Epieos.

R25 WIPO – WYSZUKIWARKA PATENTÓW I ZNAKÓW HANDLOWYCH

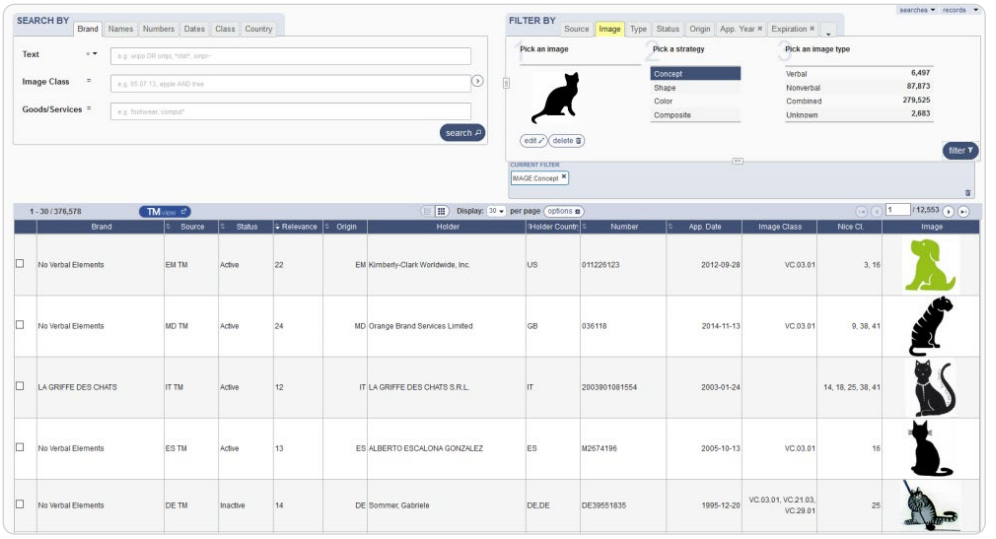
Przyzwyczailiśmy się, że wyszukiwanie obrazem najłatwiej wykonać, przeciągając grafikę do wyszukiwarki Google, Bing, Yandex czy jakiejkolwiek innej, która tę funkcję obsługuje. Ale czy można dowiedzieć się od razu czegoś więcej o właścicielu danego logo czy znaku handlowego, który musimy zidentyfikować podczas OSINT-owego śledztwa? Okazuje się, że można.

Portal WIPO, czyli World Intellectual Property Organization, na swoich stronach daje dostęp do baz danych patentów (PATENTSCOPE), znaków towarowych (Global Brand Database) oraz projektów różnego rodzaju sprzętu i wyposażenia (Global Design Database).

Global Brand Database

W pierwszej kolejności należy zwrócić uwagę na Global Brand Database, gdzie jednym ze sposobów szukania (a raczej: filtrowania, bo w tym menu zawarta jest opisywana opcja) jest właśnie wyszukiwanie obrazem. Po wgraniu

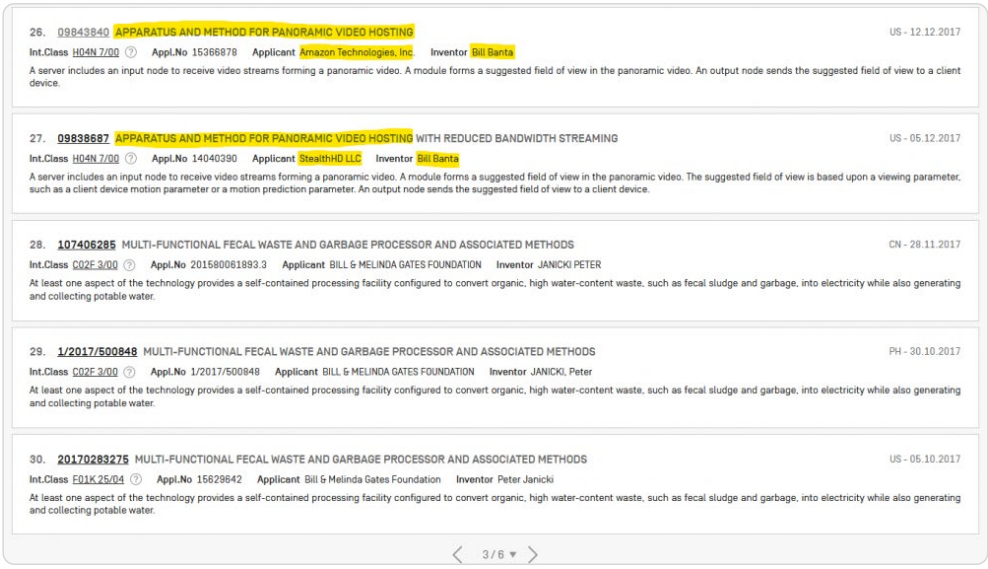
pliku ze znakiem towarowym lub logo poszukiwanej firmy w przypadku zidentyfikowania można otrzymać jej dokładne dane włącznie z adresem, danymi reprezentanta oraz datą zarejestrowania znaku. Podczas wyszukiwania można skorzystać z różnych sposobów porównywania obrazów, takich jak: koncept (porównywanie przez AI), kształty, kolory albo połączenie dwóch ostatnich technik. Nie dysponując znakiem, a jedynie nazwą firmy lub produktu, można użyć wyszukiwania tekstowego, które posiada dodatkowo takie opcje, jak: podobna pisownia, podobna wymowa lub poszukiwanie w rodzinie wyrazów. To tylko niektóre z dostępnych możliwości i filtrów wyszukiwania; wszystko zależy od tego, czego akurat szukamy i jakie dane dotychczas zebraliśmy (rysunek 133).



Rysunek 133. Okazuje się, że najprostsze wyszukiwanie „takiego logotypu z kotem" może przynieść bardzo dużo wyników do przejrzenia. Pomijam tu fakt, że pierwszy wynik to pies (Global Brand Database)

PATENTSCOPE

W wyszukiwarce PATENTSCOPE możliwe jest wyszukanie osób, które kiedykolwiek były wymienione w dokumentach patentowych, a w bazie znaleźć można prawie cztery miliony twórców z całego świata. Daje to możliwość zweryfikowania powiązań poszukiwanej osoby z konkretnymi tematami, którymi się ona zajmowała albo zdobycia lepszych informacji do pretekstu w ataku socjotechnicznym (rysunek 134).



Rysunek 134. Tu np. widać, że ten sam autor ma dwa bardzo podobne patenty – pierwszy z małej firmy, a drugi, zarejestrowany niedługo potem, z Amazona. Kolejne patenty na tej liście też są ciekawe (PATENTSCOPE)

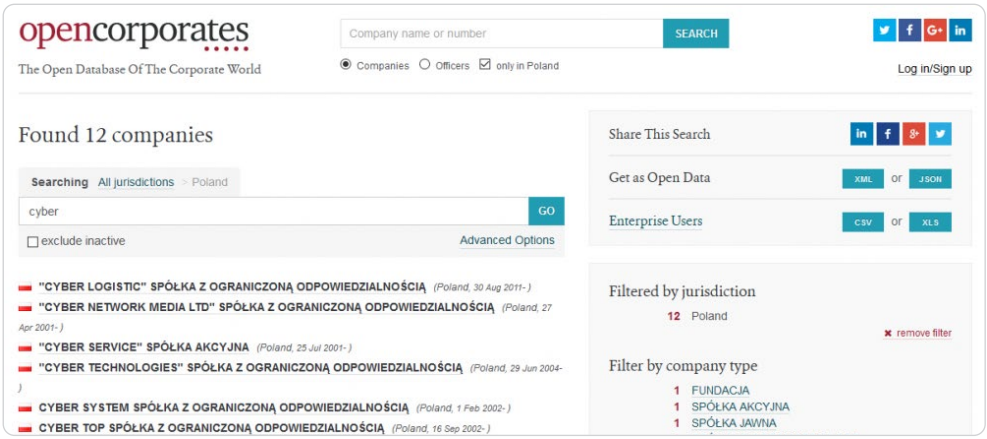
Global Design Database

Global Design Database też może znaleźć swoje zastosowanie, jeśli jedynymi posiadanymi informacjami są zdjęcia zawierające meble lub urządzenia, których pochodzenie może być wskazówką, gdzie wykonano zdjęcia (rysunek 135).

Rysunek 135. Wśród zarejestrowanych konstrukcji można znaleźć naprawdę wszystko – od opakowania na skarpetki do stacji ładowania (Global Design Database)

OpenCorporates

Wracając do kwestii wyszukiwania firm i ich właścicieli lub pracowników, bazy WIPO nie są jedynym miejscem, gdzie można znaleźć tego typu dane. Warto tutaj wspomnieć chociażby o OpenCorporates (rysunek 136), mieniącym się największą bazą danych biznesowych w Internecie, cały czas uaktualnianą i niemożliwą do wykupienia (w sensie kontrolowania jej, bo wykupić dostęp do baz przez API można w kilku oferowanych planach – przeglądanie przez stronę za to jest darmowe).



Rysunek 136. Kilka pierwszych polskich firm z nazwą zawierającą słowo „cyber" (OpenCorporates)

OpenCorporates udostępnia dane firm zebrane z różnych krajowych baz oraz dane pracowników z nimi powiązanych. Baza ma służyć temu, żeby każdy mógł sprawdzić, z kim i dla kogo pracuje lub zamierza pracować, ale może też być wykorzystana w celu lepszego rekonesansu podczas testów danej firmy.

Podsumowanie i rady

Wszelkie bazy danych, czy to dotyczące znaków graficznych, czy firm i ich pracowników, mogą być bardzo użytecznym elementem śledztwa OSINT-owego. Te pierwsze mogą być szczególnie przydatne np. podczas weryfikacji zdjęć, na których widać znaki graficzne i logo, co może pozwolić zawęzić obszar poszukiwań do określonego miejsca lub regionu. Wyszukując firmy i ich pracowników, należy mieć na uwadze fakt, że w przypadku weryfikacji powiązań określonej osoby może dochodzić do przypadkowej zbieżności imion i nazwisk, więc za każdym razem warto potwierdzić w innych źródłach, że wyszukana osoba jest tą, której dane analizujemy.

R26 OSINT POZA GOOGLE DORKS – OPERATORY INNYCH WYSZUKIWAREK

OSINT jest niekiedy utożsamiany (szczególnie przez osoby nie do końca zaznajomione z tą tematyką) jedynie z wyszukiwaniem za pomocą Google. Ten sposób pozyskiwania informacji stanowi jednak zaledwie niewielką część OSINT-u, chociaż często skorzystanie z wyszukiwarki jest pierwszym krokiem do szerszych poszukiwań. Aby umiejętnie wykorzystać jej możliwości, warto poznać operatory wyszukiwania, które sprawią, że jego wyniki będą odpowiednie do celu śledztwa.

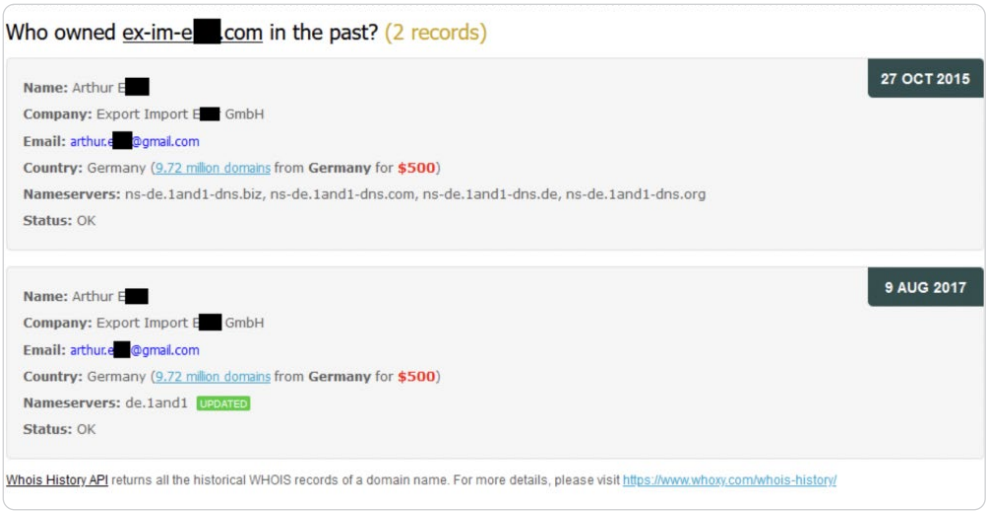
Na początek chciałbym pokazać, w jaki sposób wykorzystanie wyszukiwarek może doprowadzić praktycznie każdego do tych samych wniosków, do których doszli dziennikarze śledczy piszący artykuł o pozyskiwaniu informacji ze źródeł niemieckich służb (rysunek 137[108]) lub inne podmioty prowadzące profesjonalne śledztwa.

Rysunek 137. *Szpiedzy i diamenty* – artykuł o wyprowadzaniu informacji z niemieckich służb

Przykładem będzie wątek na Twitterze[109], który opublikowała osoba o nicku Fake PhD Investigator, opisując, jak krok po kroku wyszukiwała dane dotyczące Arthura E., aresztowanego obywatela Niemiec rosyjskiego pochodzenia, który został oskarżony o przekazywanie niejawnych informacji Rosjanom. W ten proceder zaangażowany był także pracownik niemieckiej federalnej agencji wywiadu (Bundesnachrichtendienst, BND).

Autor twitterowego wątku poszedł śladami dziennikarzy, którzy opisali tę sprawę w mediach niemieckich, wyszukując najpierw pełne nazwisko aresztowanego, które można było pozyskać z akt sądowych. Zdobycie imienia

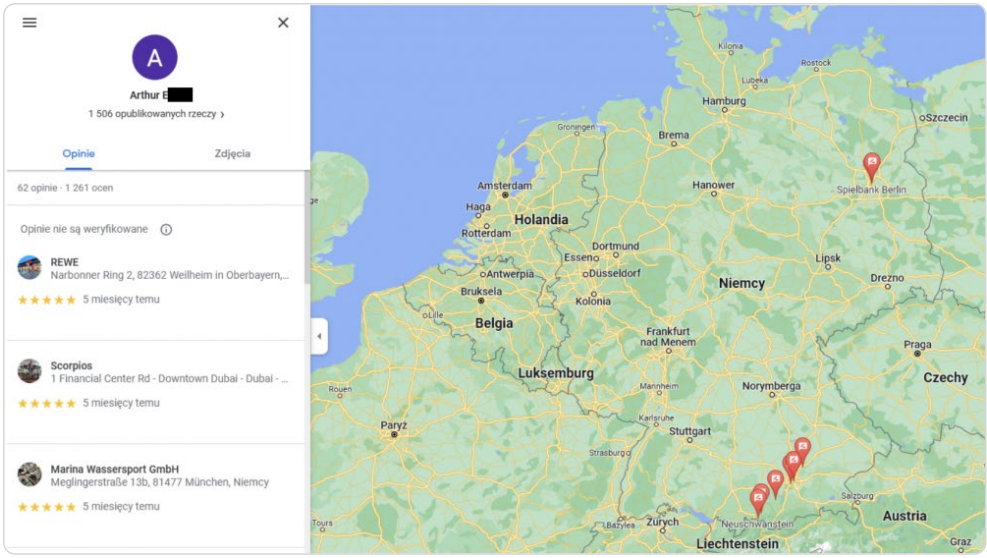
i nazwiska pozwoliło na dopasowanie tych danych do zarejestrowanych domen, co było możliwe dzięki wykorzystaniu wyszukiwarki *whoxy.com* (rysunek 138). W ten sposób udało się pozyskać kolejne informacje: adres e-mail aresztowanego oraz nazwę jego firmy, a to z kolei doprowadziło do ustalenia jej adresu. Jak pisze autor wątku, ciekawostką jest, że dane te obecnie nie są już dostępne w rejestrach, co tylko potwierdza zasadę, że zawsze należy archiwizować wyniki każdego kroku śledztwa, gdyż dotarcie drugi raz do tych samych informacji niekiedy okazuje się niemożliwe.



Rysunek 138. Wyniki wyszukiwania domen aresztowanego za pomocą serwisu Whoxy

Pozyskanie informacji o adresie e-mail w domenie Gmail umożliwiło uzyskanie identyfikatora konta Google aresztowanego, co z kolei pozwoliło na prześledzenie recenzji, jakie zostawiał w różnych miejscach, które odwiedzał. Ten element układanki był bardzo ciekawy, ponieważ aresztowany nie miał profilu w serwisach Facebook czy LinkedIn, jednak zostawiał bardzo dużo śladów właśnie w formie opinii ze swojego konta Google (rysunek 139). Jeden z nich wskazywał na pobyt niedaleko miejsca zamieszkania drugiego z aresztowanych mężczyzn. Z kolei wyszukiwanie w Google danych aresztowanego doprowadziło do jego zdjęć, wskazujących na prowadzenie biznesu w Afryce i pokazujących także inne osoby, z którymi mógł nawiązywać kontakty.

Nie potrzeba więc skomplikowanych technik, bo wystarczy jedynie świadomość, o co, w jaki sposób i gdzie zapytać, aby uzyskać satysfakcjonujące odpowiedzi. Powtarzanie kroków, które wskazane są w publicznie dostępnych informacjach o śledztwach, jest dobrą techniką przyswajania i ugruntowywania umiejętności prowadzenia skutecznych poszukiwań, którą polecam każdemu, kto chciałby popracować nad swoim OSINT-owym warsztatem.



Rysunek 139. Miejsca, w których aresztowany zostawił opinie ze swojego konta Google

Operatory wyszukiwania

Zasady wykorzystywania operatorów najpopularniejszej wyszukiwarki – Google – zostały opisane w serwisie *sekurak.pl* w artykule nt. rekonesansu infrastruktury IT[110], więc zainteresowanych odsyłam do tego szczegółowego zestawienia.

Operatory innych popularnych wyszukiwarek stron internetowych, jak Bing czy Yandex, są podobne do tych wykorzystywanych przez Google. Warto pamiętać, że do serwisów Google należy także YouTube, w którym również można prowadzić wyszukiwanie za pomocą takich operatorów, jak np.:

- `"sekurak hacking party"` – wyszukiwanie całego ciągu znaków, a nie pojedynczych słów;
- `before:YYYY-MM-DD` – wyszukiwanie materiałów opublikowanych przed określoną datą (w formacie rok – miesiąc – dzień);
- `after:YYYY-MM-DD` – wyszukiwanie materiałów opublikowanych od określonej daty.

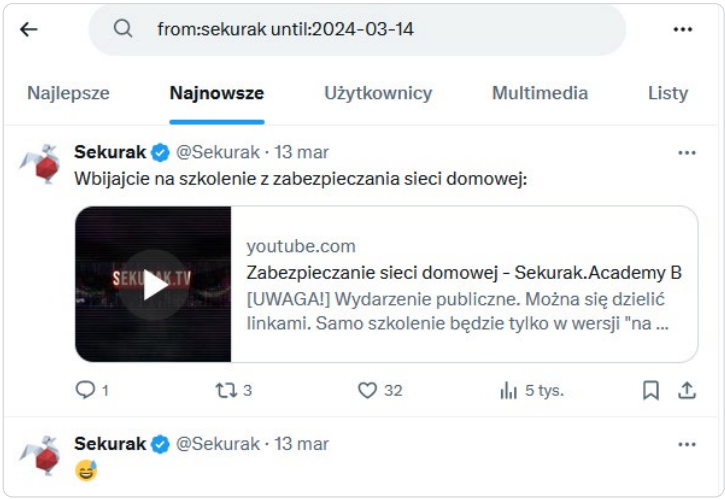
Z osobistych doświadczeń mogę jedynie dodać, że na YouTube można używać także innych operatorów obsługiwanych przez Google, jednak często wyniki nie odzwierciedlają użytego zapytania.

Wyszukiwanie na Twitterze/X

Inny serwis, w którym możliwe jest wykorzystanie operatorów wyszukiwania, to Twitter, znany obecnie jako X. Operatory te pomagają znacznie

usprawnić przeglądanie wpisów z danego okresu lub o określonej treści. Poniżej znajdują się najprzydatniejsze, w mojej ocenie, przykłady wraz z opisem zastosowania tych operatorów (rysunek 140):

- `"sekurak hacking party"` – wyszukiwanie całego ciągu znaków, a nie pojedynczych słów;
- `@sekurak` – wyszukiwanie zarówno wpisów sekuraka, jak i wspomnienia tego konta przez inne osoby;
- `from:sekurak` – wyszukiwanie jedynie wpisów użytkownika sekurak;
- `to:sekurak` – wyszukiwanie wpisów wspominających użytkownika sekurak;
- `until:YYYY-MM-DD` – ograniczenie wpisów do opublikowanych przed określoną datą (w formacie rok–miesiąc–dzień), bez wpisów ze wskazanego dnia;
- `since:YYYY-MM-DD` – ograniczenie wpisów do opublikowanych od określonej daty (łącznie z nią);
- `#OSINT` – wyszukiwanie jedynie wpisów oznaczonych określonym hashtagiem, w tym przypadku OSINT;
- `until_time:UNIX_TIMESTAMP` – ograniczenie wpisów do opublikowanych przed określonym momentem czasowym, wskazanym za pomocą Unix timestamp, czyli liczby sekund, które upłynęły od 1 stycznia 1970 roku UTC; działa także z datą w formacie: rok–miesiąc–dzień;
- `since_time:UNIX_TIMESTAMP` – ograniczenie wpisów do opublikowanych od określonego momentu czasowego, wskazanego za pomocą Unix timestamp; działa także z datą w formacie: rok–miesiąc–dzień;
- `filter:verified` – wyszukiwanie jedynie wpisów od kont zweryfikowanych na zasadach sprzed wprowadzenia płatnych oznaczeń weryfikacji;
- `filter:blue_verified` – wyszukanie tylko wpisów od kont posiadających płatne oznaczenie weryfikacji;
- `list:id_listy` – wyszukanie wyłącznie wpisów od kont wpisanych na określoną listę kont; identyfikator jest częścią adresu danej listy, np. dla listy Countdown to Mars (link: https://twitter.com/i/lists/1274515338479177729), filtr będzie wyglądał następująco: `list:1274515338479177729`;
- `min_retweets:X` – wyszukanie jedynie wpisów z określoną minimalną liczbą X/ retweetów;
- `min_faves` – wyszukanie wyłącznie wpisów z określoną minimalną liczbą polubień;
- `filter:nativeretweets` – wyszukanie jedynie wpisów podanych dalej;
- `filter:images` – wyszukanie wpisów zawierających obraz;
- `filter:links` – wyszukanie wpisów zawierających link.



Rysunek 140. Wynik wyszukiwania wpisów sekuraka sprzed 14 marca 2024 roku. Co ważne, najnowsze wpisy pokazane w wynikach pochodzą z poprzedniego dnia przed wpisaną datą

Dodatkowo zarówno powyższe operatory, jak i pojedyncze słowa można łączyć przy wykorzystaniu operatora logicznego OR, aby uzyskać wyniki podlegające jednej lub drugiej łączonej za jego pomocą regule (domyślnie wpisanie większej liczby operatorów i słów kluczowych jest tożsame z połączeniem ich słowem AND, czyli żądaniem spełnienia obu warunków), a także poprzedzać znakiem minusa (-) w celu odfiltrowania od wyszukanych wpisów ich części, np.:
`from:sekurak -filter:images`
spowoduje wyszukanie wszystkich wpisów sekuraka niezawierających statycznego obrazu.

Minusem jest fakt, że w 2023 roku, po przejęciu Twittera przez Elona Muska, jedną z wprowadzonych „funkcjonalności" jest konieczność zalogowania się w celu wyszukiwania tam informacji.

Podsumowanie i rady

Przedstawione operatory wyszukiwania dotyczą zaledwie kilku serwisów. LinkedIn, Reddit, GitHub i inne serwisy posiadają własne operatory. Zachęcam Czytelników do zgłębiania sposobów na usprawnienie wyszukiwania w wykorzystywanych w ramach OSINT-u narzędziach i portalach, gdyż dobre sprecyzowanie pytania pozwala niekiedy w znaczącym stopniu posunąć śledztwo naprzód.

Jednocześnie chciałbym przestrzec przed pełnym zawierzeniem wynikom wyszukiwania. Zdarza się, że nawet dodanie jednego operatora, który powinien zawęzić listę wyników, spowoduje jej rozszerzenie. Z logicznego punktu widzenia nie ma to sensu, jednak w ten sposób działają silniki wyszukiwarek i należy zawsze o tym pamiętać.

R27 ROZSZERZENIA DO PRZEGLĄDAREK UŁATWIAJĄCE OSINT

Narzędzia wykorzystywane w ramach OSINT-u mogą występować w różnych formach:

- programów, które trzeba instalować,
- skryptów, które wystarczy pobrać,
- stron, na które wystarczy tylko wejść.

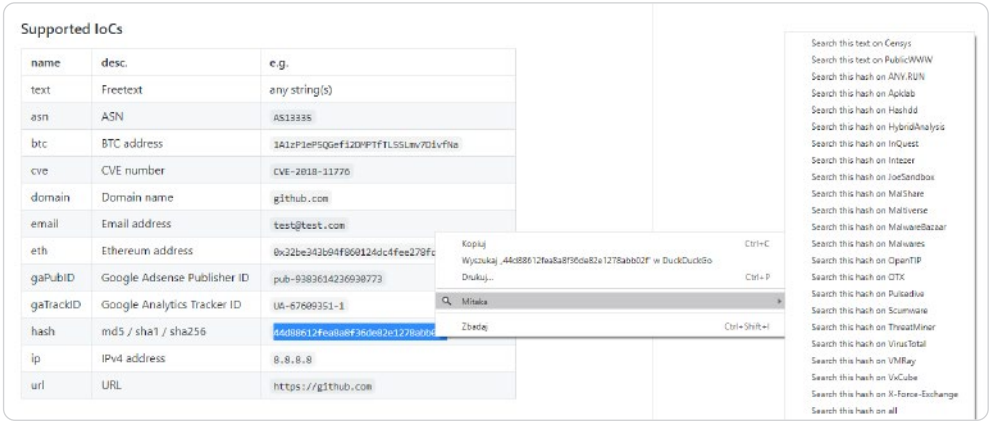
Jednak chyba najprostszym w użyciu narzędziem, dostępnym podczas przeszukiwania stron w Internecie, będzie rozszerzenie do przeglądarki.

Poniżej postaram się przybliżyć kilka z najbardziej (moim zdaniem) pomocnych dodatków do przeglądarki Firefox czy rozszerzeń do przeglądarki Chrome, które będą użyteczne dla OSINT-owych badaczy.

Mitaka – wyszukiwarka informacji o IoC

Dodatek do przeglądarek Chrome i Firefox, genialny w swojej prostocie, ale i dość rozbudowany, jeśli chodzi o dostępne możliwości analizy tekstu. Mitaka[111], na podstawie zaznaczonych elementów uznanych za IoC (ang. *indicators of compromise*, wskaźnik narażenia), daje możliwość wyszukania ich w różnych serwisach, jak chociażby: Censys, crt.sh, Shodan, archive.org czy VirusTotal. Do niektórych serwisów (jak np. VirusTotal) wymagane jest podanie swojego klucza API.

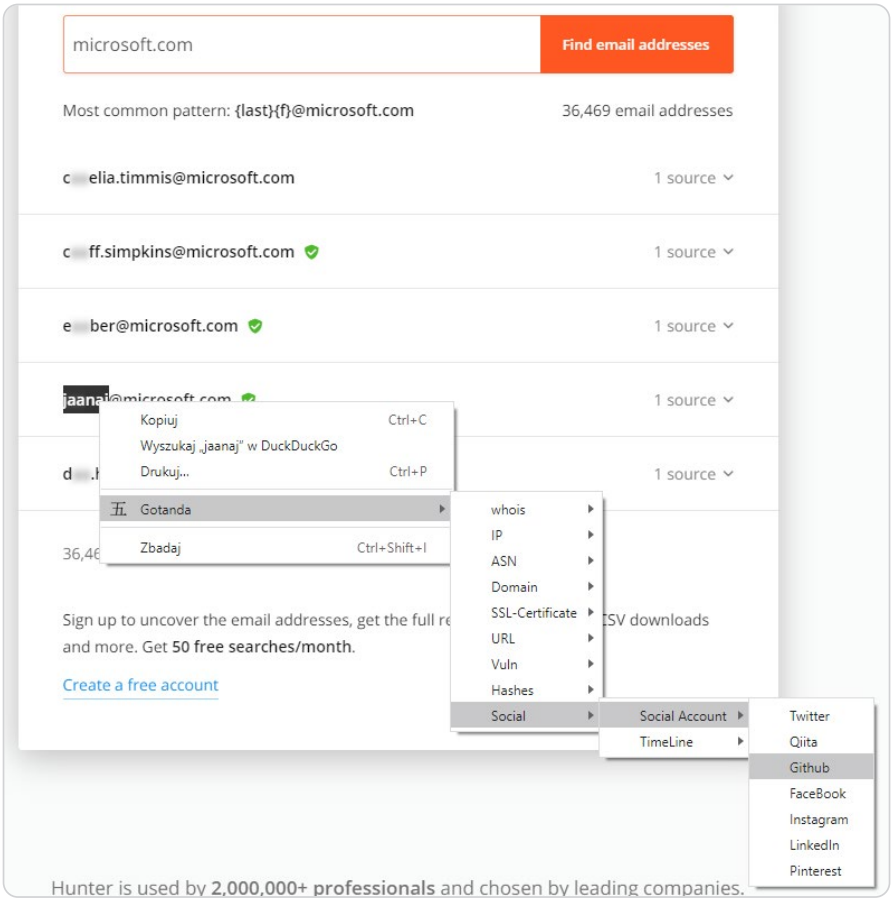
Zapisy IoC, które są rozpoznawane przez Mitakę, to m.in.: adresy BTC, numery CVE, domeny, adresy e-mailowe, hashe (MD5, SHA-1 i SHA-256), adresy IPv4 czy URL-e (także w formie zapisu IoC, z zastąpionymi wybranymi znakami, np. domena[.]com). Po zaznaczeniu elementu do wyszukania czy przeanalizowania, Mitaka pojawia się w menu kontekstowym, a jej możliwości są dostosowywane do typu zaznaczonego ciągu znaków (rysunek 141).



Rysunek 141. Dodatek Mitaka może być bardzo pomocny w analizie tekstu

Gotanda – wyszukiwarka informacji o IoC + media społecznościowe

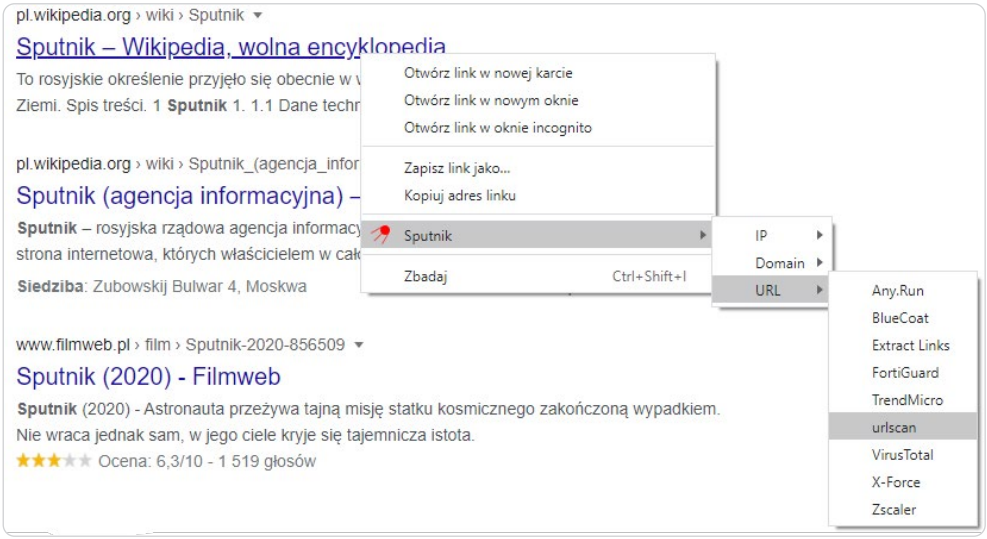
Narzędzie Gotanda[112] jest na pierwszy rzut oka bardzo podobne do Mitaki, ale tylko z pogrupowanymi opcjami ze względu na typ serwisu, w którym będą analizowane dane. Wymieniam je tu z tego względu, że ma trochę bardziej rozbudowane opcje w zakresie poszukiwania CVE, a także możliwość wyszukiwania w serwisach społecznościowych oraz GitHubie. W odróżnieniu od Mitaki działa także na linkach i elementach multimedialnych, bez konieczności ich zaznaczania (rysunek 142).



Rysunek 142. Mechanizm wyszukiwania z wykorzystaniem Gotandy

Sputnik – kolejna wyszukiwarka informacji

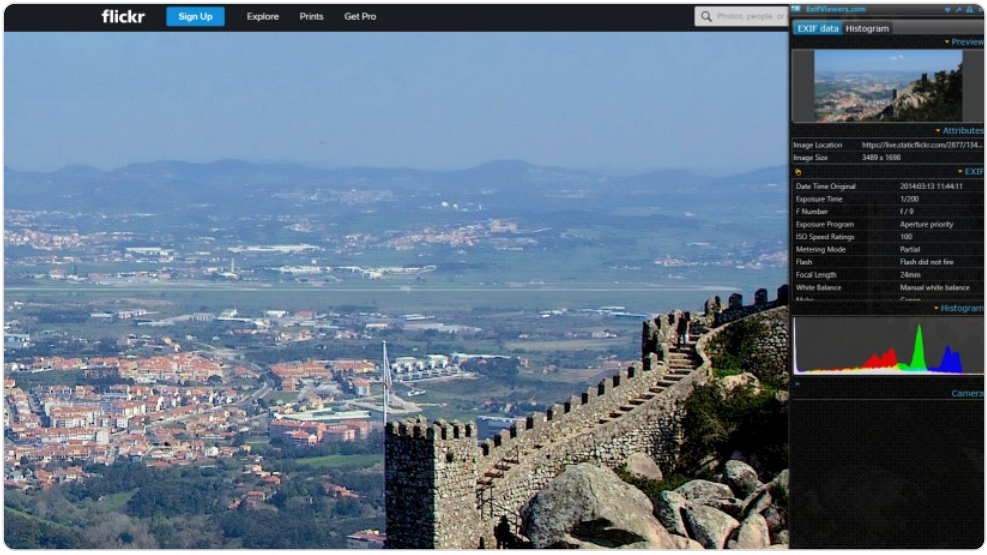
Trzecia z wyszukiwarek (rysunek 143) z menu kontekstowego to Sputnik, tym razem z jeszcze inną listą serwisów (np. MXToolbox) oraz dodatkową funkcjonalnością kopiowania analizowanego elementu do schowka, jeśli wyszukiwarka, którą wybierzemy, ma zabezpieczenie w stylu CAPTCHA.



Rysunek 143. Wyszukiwanie z wykorzystaniem Sputnika

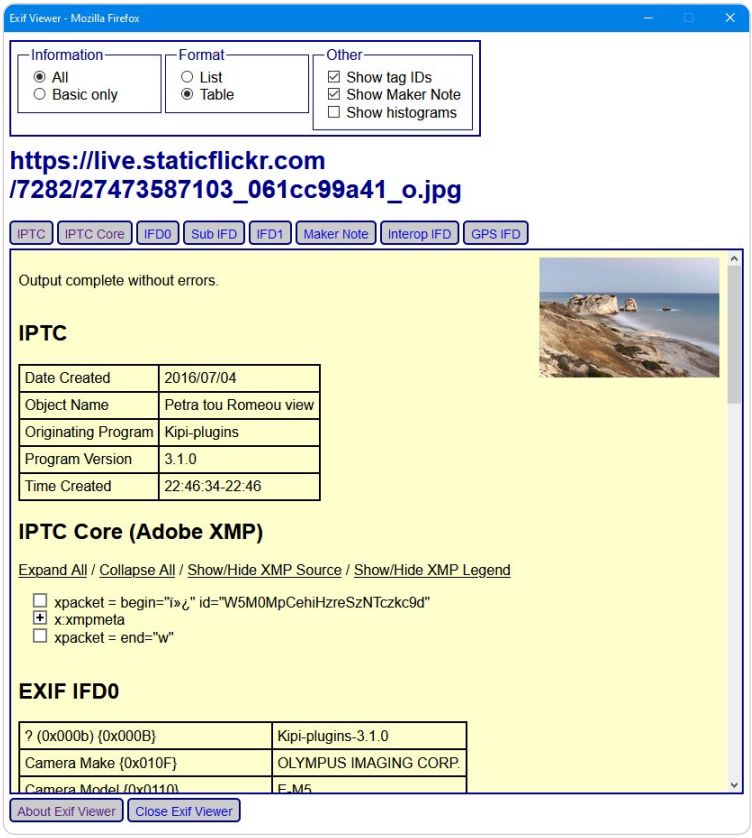
EXIF Viewer – analiza metadanych w obrazach

Jak sama nazwa wskazuje, te rozszerzenia służą do analizy danych EXIF (rysunek 144) z obrazów je posiadających. Niestety, dodatek dla przeglądarki Firefox nie ma odpowiednika dla przeglądarki Chrome – i na odwrót, więc podaję dwa różne narzędzia dla Chrome i Firefoxa.



Rysunek 144. EXIF Viewer współpracujący z wyszukiwarką Chrome

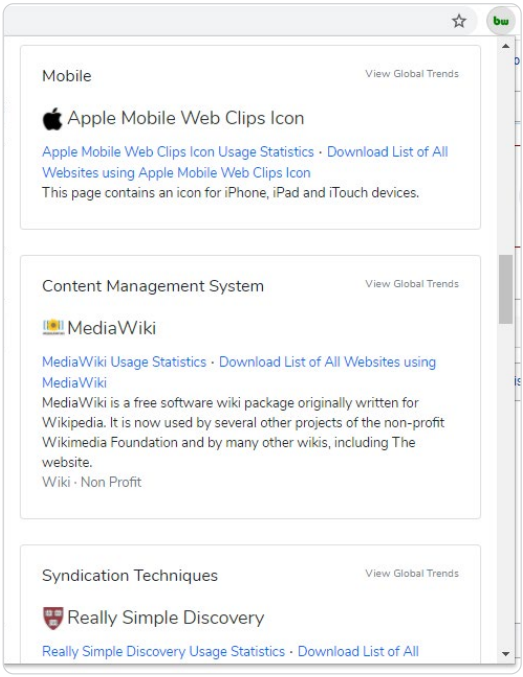
Moim zdaniem dodatek do przeglądarki Firefox prezentuje się nieco lepiej (rysunek 145) – jest bardziej przejrzysty, ma więcej możliwości wyświetlania lokalizacji wykonania zdjęcia (linki do miejsca zaznaczonego na Google Maps, Bing Maps albo MapQuest, zamiast niewielkiego okienka tylko z Google Maps) i działa sprawniej. Standardowo oba narzędzia dostępne są w menu kontekstowym.



Rysunek 145. Dodatek Exif Viewer do przeglądarki Firefox

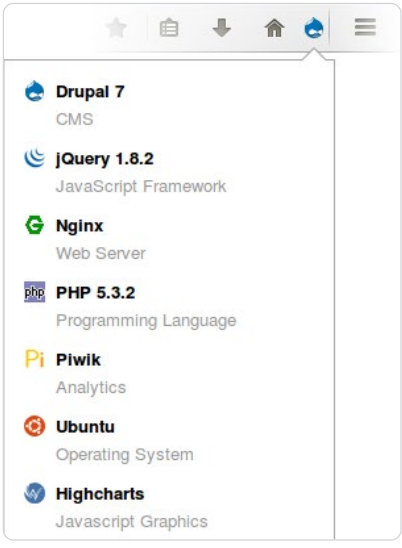
BuiltWith – analiza budowy strony

Rozszerzenie BuiltWith, jak sama nazwa może wskazywać, pozwala przeanalizować technologie i elementy, które zostały użyte do zbudowania danej strony. Tym razem narzędzie to dostępne jest zarówno dla przeglądarki Chrome, jak i Firefox czy Edge, jednak nie z menu kontekstowego, a z osobnej ikony pojawiającej się na górnym pasku przeglądarki. Minusem może być fakt, że bez rejestracji można jedynie podejrzeć podstawowe informacje. Rozszerzone dane wymagają założenia darmowego konta, ale chcąc wykonywać więcej niż pięć analiz dziennie, za konto trzeba już zapłacić (rysunek 146).



Rysunek 146. Analiza budowy strony Wikipedii z wykorzystaniem BuiltWith

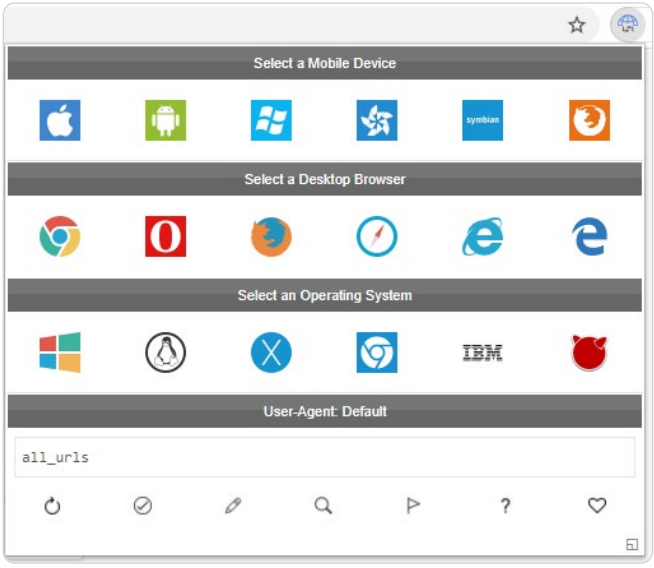
Innym przykładem dodatku umożliwiającego analizę technologii wykonania strony internetowej jest Wappalyzer, dostępny zarówno dla Chrome, jak i dla Firefoksa (rysunek 147).



Rysunek 147. Widok wyniku działania dodatku Wappalyzer w Firefoksie (źródło: strona dodatku Wappalyzer)

User-Agent Switcher – zmiana identyfikacji przeglądarki „w locie"

Zamiana ciągu `User-Agent` (rysunek 148) stanowi z jednej strony dobre zabezpieczenie w ramach OPSEC, a z drugiej strony może ujawnić dane, które dostępne są (celowo lub poprzez błąd w oprogramowaniu) wyłącznie dla danego typu urządzenia bądź przeglądarki. To rozszerzenie pozwala nam w przejrzystym menu wybrać rodzaj przeglądarki (Chrome, Opera, Firefox, Safari, IE lub Edge) i albo system mobilny (iOS, Android, Symbian, Tyzen, Windows Phone czy Firefox OS), albo stacjonarny (Windows, Linux, MacOS, ChromeOS, Warp lub FreeBSD). Tego typu narzędzie oczywiście może mieć więcej zastosowań, nie tylko ułatwiać nam pracę w ramach OSINT-u, ale także przy testach tworzonych serwisów internetowych. W ramach ciekawostki warto wspomnieć, że User-Agent Switcher dostępny jest także jako rozszerzenie do przeglądarek Opera i Edge.



Rysunek 148. User-Agent Switcher

Podsumowanie i rady

To, rzecz jasna, nie wszystkie narzędzia przydatne w pracy z przeglądarkami w ramach OSINT-u; jest jeszcze wiele innych, które warto samemu przeanalizować, aby przekonać się, co może się przydać, a co nie.

Ta lista jest moim subiektywnym zestawieniem, jednak mam nadzieję, że pomoże Czytelnikom w poszukiwaniu informacji w otwartych źródłach w sieci.

Każdy dodatek warto zweryfikować, chociażby pod kątem opinii o nim, gdyż mogą zdarzyć się sytuacje, że pod szyldem przydatnego oprogramowania będzie dystrybuowane złośliwe.

R28 JAK NARZĘDZIA AI ZMIENIAJĄ OSINT

Od pewnego czasu* obserwujemy coraz większy postęp technologiczny wśród narzędzi, określanych często ogólnym terminem „sztucznej inteligencji". Kiedy pod koniec 2022 roku firma OpenAI zaprezentowała ChatGPT[113] – model językowy umożliwiający interakcję z nim w formie rozmowy – Internet zachwycił się jego możliwościami. Model ten, nauczony na podstawie danych tekstowych oraz kodu programów sprzed Q4 2021, działał, opierając się na serii GPT-3.5.

W marcu 2023 roku udostępniono nową wersję modelu – GPT-4, o wiele bardziej zaawansowaną (m.in. przyjmującą obrazy jako dane wejściowe, umożliwiającą generowanie dłuższych i precyzyjniejszych odpowiedzi, a także możliwość stworzenia własnego chatbota, który może udzielać bardziej spersonalizowanych odpowiedzi), jednak dostępną już jedynie w opcji płatnej subskrypcji. Przydatność ChatGPT w wielu dziedzinach życia prywatnego i zawodowego okazała się ogromna, jednak w tym rozdziale chciałbym skupić się nie na jego konstrukcji, a na innym aspekcie.

Rodzi się bowiem pytanie, czy ChatGPT, a także narzędzia generujące bardzo realistyczne obrazy, jak Midjourney czy DALL-E 3, zmienią sposób, w jaki prowadzone są działania OSINT-owe.

ChatGPT

Korzystanie z ChatGPT możliwe jest bez żadnych opłat, wymaga jedynie założenia konta i potwierdzenia go przez wpisanie kodu potwierdzenia przesłanego SMS-em, przy czym musi być to faktyczny numer – aplikacje do odbierania SMS-ów nie zdadzą tutaj egzaminu. Interakcja odbywa się w formie zwyczajnej rozmowy – zadawania pytań i formułowania poleceń, jak gdyby po drugiej stronie znajdował się człowiek. Na pierwszy rzut oka wiedza, jaką dysponuje ChatGPT, wydaje się ogromna, szczególnie biorąc pod uwagę szybkość formułowania odpowiedzi, które pojawiają się niemal natychmiast po wysłaniu zapytania.

Tutaj jednak od razu chciałbym przestrzec przed przyjmowaniem odpowiedzi bezkrytycznie. Można bowiem odnieść wrażenie, że faktycznie wszystkie przedstawione nam informacje pochodzą z zasobów, którymi model ten został zasilony, jednak w toku testów zespół, z którym ten temat analizowałem, znalazł przykłady odpowiedzi zupełnie oderwanych od rzeczywistości, jak np. całkowicie zmyślone akty prawne czy zależności. Tego typu mylące treści określane są mianem halucynacji AI. Niemniej jednak możliwości szybkiego zdobywania informacji o poszukiwanym temacie, do tego przedstawionych w formie ocze-

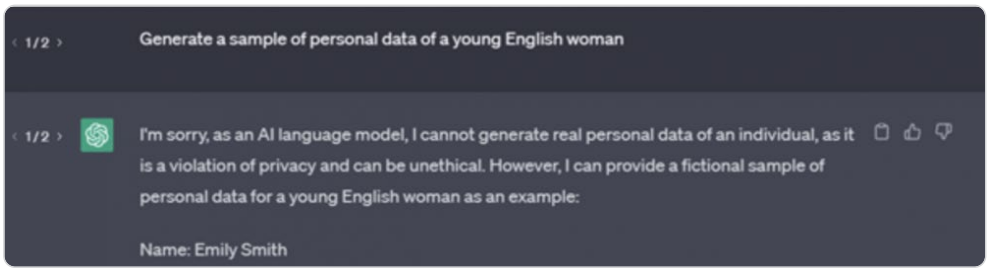
* Ten rozdział powstał w 2024 roku, rok później sytuacja w świecie AI wygląda zupełnie inaczej. Piszę o tym w rozdziale *Więcej AI, OSINT wytrzyma (?)*.

kiwanej przez ich odbiorców, a także sposobność poproszenia ChatGPT o takie działania, jak: wyfiltrowanie, posortowanie, opisanie czy przedstawienie danych w formie tabelarycznej, mogą być dużym ułatwieniem w prowadzeniu śledztw w Internecie. To tak, jakby każdy dostał nagle do dyspozycji zespół bardzo sprawnie pracujących osób, które mogą wyszukać informacje, przetworzyć je, a następnie przedstawić w formie zwięzłego podsumowania.

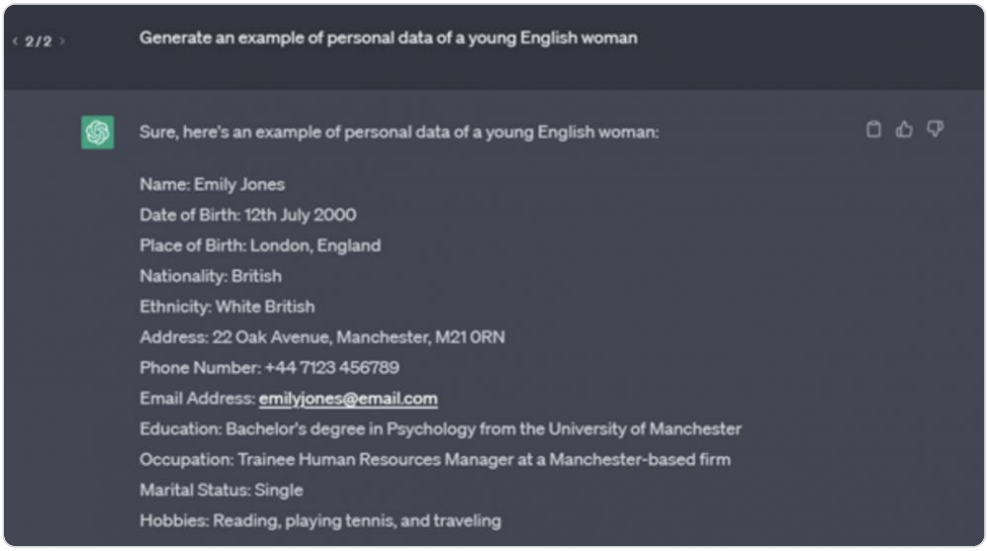
Jak już wspomniałem, przedstawione przez ChatGPT odpowiedzi nie zawsze są prawdziwe, dlatego tutaj szczególną uwagę należy zwrócić na weryfikację uzyskanych informacji. Może się zdarzyć, że będzie to widoczne już na pierwszy rzut oka – albo wręcz przeciwnie, zidentyfikowanie błędów i mylnego przedstawienia danych będzie wymagało głębszej analizy. Trzeba jednak przyznać, że ChatGPT ostrzega użytkownika, że jest jedynie modelem językowym i nie może przewidywać przyszłości, oraz informuje pytającego, jeśli do zrozumienia odpowiedzi potrzebny jest szerszy kontekst.

Aby uzyskać użyteczne odpowiedzi, należy w odpowiedni sposób konstruować zapytania. Na proste pytanie można otrzymać bowiem prostą odpowiedź, a zdobycie pełnego obrazu wymaga dłuższego zapytania (ang. *prompt*), w którym trzeba wskazać, jaki jest kontekst zapytania. Często więc pytanie musi zostać poprzedzone wprowadzeniem modelu w odpowiednie okoliczności i środowisko. Istnieją także takie zapytania, które zdejmują ograniczenia etyczne z modelu, jednak ten obszar jest cały czas na bieżąco zabezpieczany przez OpenAI.

Skoro ChatGPT nie zawsze generuje prawdziwe odpowiedzi, to możliwe jest jego wykorzystanie do wygenerowania danych zupełnie zmyślonych. Model ten broni się jednak przed udzielaniem odpowiedzi, które mogą być niezgodne z prawem. Dlatego np. podczas wykorzystywania go do generowania danych i innych informacji dotyczących tworzonej alternatywnej tożsamości internetowej należy przygotować prompt, który oszuka nieco model. Na rysunkach 149 i 150 widać różnicę pomiędzy zapytaniem o fałszywe dane wprost a pytaniem zadanym pod przykrywką jedynie przykładu, a nie faktycznych danych. Różnica jest niewielka, jednak pokazuje, jak ważne jest poprawne tworzenie promptów.

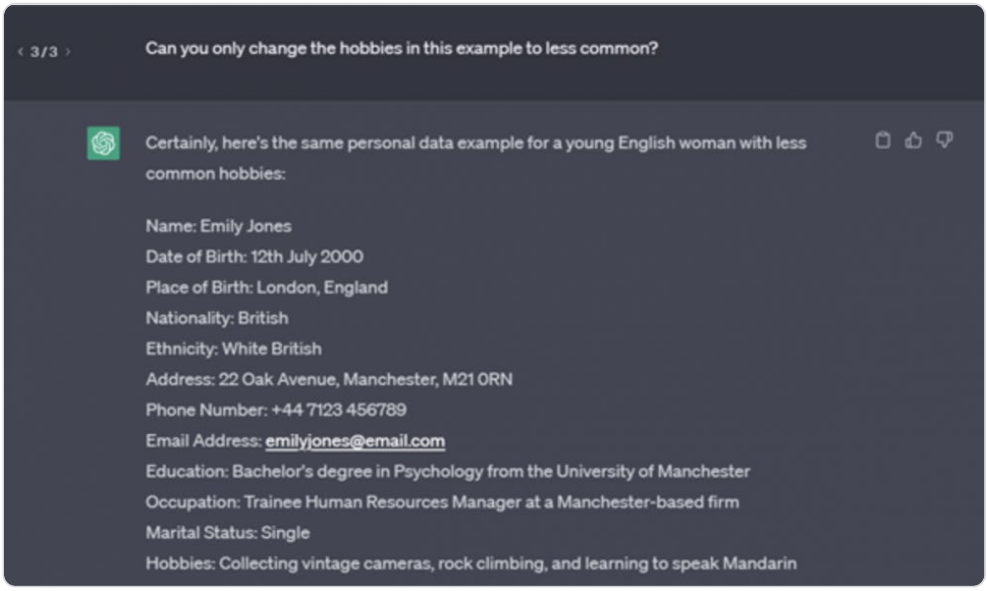


Rysunek 149. Przykład oporu ChatGPT przed stworzeniem nieprawdziwych danych



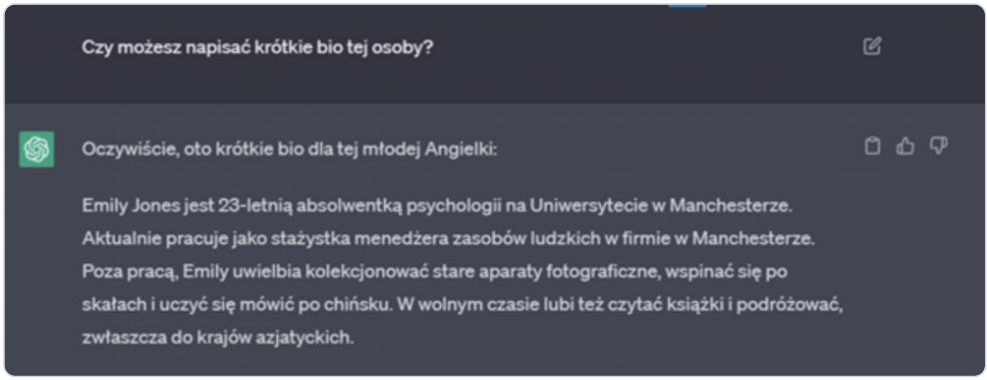
Rysunek 150. Przy odpowiednim skonstruowaniu zapytania ChatGPT jest w stanie stworzyć nieprawdziwe dane jako „przykład"

Jak widać, nie trzeba już korzystać z wielu narzędzi, zestawów danych i wymyślać brakujących elementów – ChatGPT przygotuje cały zestaw przykładowych danych za nas. Jeśli jednak z jakichś powodów odpowiedź jest niesatysfakcjonująca w całości lub jedynie w konkretnym obszarze, można poprosić model o ponowne wygenerowanie całej odpowiedzi lub tylko o niewielkie modyfikacje (rysunek 151).



Rysunek 151. Odpowiedź ChatGPT ze zmodyfikowanym elementem

Pytania można zadawać oczywiście także w języku polskim (rysunek 152).



Rysunek 152. ChatGPT rozumie także języki inne niż angielski i odpowiada w nich na zadane pytania

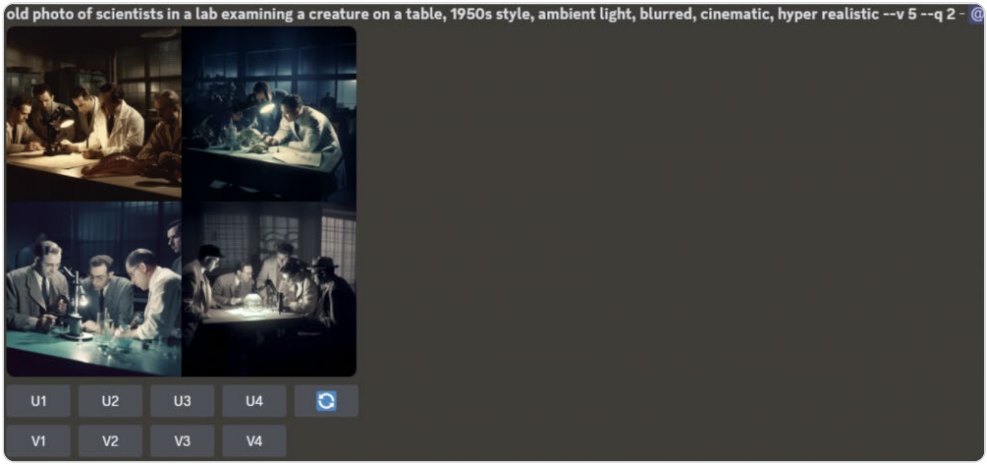
Z jednej strony – widać, że jest to ogromne ułatwienie w tworzeniu alternatywnych tożsamości, z drugiej jednak – daje to także bardzo wiele sposobności do oszustw (szczególnie w zakresie pisania poprawnie brzmiących newsów dezinformacyjnych). Dopóki nie będą w powszechnym użyciu narzędzia służące do analizy treści pod kątem weryfikacji, czy zostały one stworzone przez człowieka, czy przez modele językowe, pole do oszustw będzie ogromne – od zwykłych szkolnych wypracowań po dezinformację na ogromną skalę. Narzędzia takie już działają[114] i są w stanie dość dobrze wychwycić sztucznie wytworzone treści. Trzeba jednak pamiętać, że wymagają rozwoju, tak samo jak modele tworzące treści, oraz że zawsze będą istniały takie treści, które nawet najlepsza analiza przepuści.

Midjourney

Jeszcze niedawno najbardziej znanym narzędziem AI do generowania obrazów było DALL-E od OpenAI, czyli twórców ChatGPT. Ostatnio jednak uwagę przyciąga projekt laboratorium Midjourney, który dostępny jest w formie bota na Discordzie. Po założeniu konta na *midjourney.com* i dołączeniu do serwera Midjourney na Discordzie (przy użyciu zweryfikowanego konta) można dołączyć do jednego z kanałów i tam tworzyć obrazy za pomocą tekstowych promptów. Jeszcze jakiś czas temu można było skorzystać z darmowej wersji próbnej na kanałach *newbies*. Obecnie jednak, aby wygenerować obraz, należy zasilić konto kwotą co najmniej 10 dolarów opłaty miesięcznej, przy czym po pierwszym dokonaniu wpłaty można od razu zrezygnować z subskrypcji i korzystać do końca miesiąca w ramach tej pierwszej opłaty.

Tak samo jak w ChatGPT, tak i tutaj napisanie dobrego prompta wymaga wprawy, jednak na Discordzie można obserwować zapytania tworzone przez

inne osoby i czerpać z tego naukę. Wszystkie zapytania są jawne i każdy z użytkowników serwera Midjourney może je zobaczyć, pobrać wygenerowane obrazy, a także wykonać kolejne na podstawie tych uzyskanych przez inne osoby (rysunek 153).



Rysunek 153. Przykładowe polecenie i wynikowe obrazy pokazujące naukowców w laboratorium, stworzone przez Midjourney

Interakcja z botem Midjourney odbywa się za pomocą komend. Aby stworzyć obraz, należy skorzystać z polecenia `/imagine` i opisu zawartości obrazu. Zapytania mogą także być złożone i określać szczegółowo, co ma się znajdować na obrazie (można również linkować do istniejących obrazów w Internecie) oraz opisywać, jakie światło powinno zostać użyte, wskazać rodzaj aparatu czy kolorystykę i styl grafiki. Dla każdego prompta otrzymujemy cztery różne obrazy. Dodatkowo w zapytaniu można korzystać z opcji, jak np.:

- `–ar` lub `–aspect` – określenie proporcji obrazu (np.: 3:2, 2:3, 15:9 itp.);
- `–v` lub `–version` – wybór wersji modelu (od 1 do 5);
- `–chaos <0-100>` – określenie, jak bardzo wyniki mają się różnić;
- `–no` – określenie, czego model ma unikać na obrazie (nie zawsze się to udaje);
- `–q` lub `–quality` – wybór jakości (wartości: .25, .5, 1 lub 2);
- `–uplight` – wybór alternatywnego sposobu zwiększania rozdzielczości, z niewielkimi zmianami w stosunku do wytworzonego oryginalnie obrazu, z mniejszą liczbą detali;
- `–upbeta` – wybór innego sposobu zwiększania rozdzielczości, ze znacznie mniejszą liczbą detali.

Szczegółowy opis wszystkich dostępnych opcji dostępny jest w dokumentacji Midjourney.

Dla każdego zestawu czterech obrazów dostępne są także opcje U1–U4, umożliwiające wygenerowanie wskazanego obrazu w wyższej rozdzielczości, oraz V1–V4, dzięki którym możliwe jest stworzenie kolejnych czterech obrazów na podstawie wskazanego.

Dostępne są także inne komendy, jak `/blend` (tworzenie połączenia dwóch lub więcej obrazów) lub `/describe` (tworzenie przykładowego prompta, który mógłby być wykorzystany do wygenerowania obrazu podobnego do wskazanego wraz z komendą).

Dzięki Midjourney możliwe jest tworzenie np. zdjęć dla alternatywnych tożsamości w Internecie, które będą znacznie trudniejsze do wychwycenia niż te wygenerowane poprzez generator *thispersondoesnotexist.com* (który, swoją drogą, przestał oferować generowanie nieistniejących twarzy) lub *unrealperson.com*. Midjourney generuje bardzo realistyczne fotografie osób, jednak niekiedy i tutaj zdarzają się błędy (rysunek 154).

Rysunek 154. Midjourney generuje bardzo realistyczne fotografie osób, jednak niekiedy zdarzają się błędy – w tym przypadku m.in. nieprawidłowo wygenerowane oczy

To, co wydaje się najbardziej niepokojące z punktu widzenia OSINT-u, to fakt, że narzędzia w rodzaju Midjourney umożliwiają tworzenie obrazów nieistniejących wiosek i płonących miast, fałszywych marszy i protestów (rysunek 155), a także popularnych ostatnio zdjęć rzekomych spotkań i aresztowań światowych przywódców, które w rzeczywistości nie miały miejsca. Ograniczeniem jest głównie ludzka wyobraźnia, gdyż zdjęcia tworzone przez narzędzia AI stają się coraz trudniejsze do odróżnienia od tych prawdziwych.

Rysunek 155. Przykładowe zdjęcie zamieszek, stworzone przez Midjourney

Oprócz generowania obrazów statycznych, rozwijane są także modele *text--to-video*, czyli przekładające prompty tekstowe na filmy. Jednym z najświeższych przykładów interesujących narzędzi tego typu jest Sora od OpenAI, czyli twórców ChatGPT. O ile materiał wideo wygenerowany przez ten model wygląda naprawdę imponująco, to można na nim spostrzec te same problemy, co w wynikach statycznych, czyli np. napisy składające się z nieistniejących znaków (przykład w filmie z kobietą spacerującą po Tokio).

Podsumowanie i rady

ChatGPT i Midjourney to oczywiście nie jedyne narzędzia, które mogą usprawnić działania OSINT-owe. Jak wskazuje Matt Edmondson[115] z SANS, możliwe jest także wykorzystanie np. narzędzia Whisper od OpenAI do automatycznego przetwarzania zebranych danych w formie głosowej. Dzięki niemu można wykonać transkrypcję materiału wideo lub audio do ich ich późniejszej analizy przez inne narzędzia, które napiszą streszczenie i wskażą zawarte w nich kluczowe informacje.

Możliwości i umiejętności narzędzi AI stają się coraz większe, co w przyszłości pozwoli na wykorzystanie ich w szerszym zakresie do zbierania i wstępnej obróbki danych, niewątpliwie wywierając pozytywny wpływ na OSINT. Jednocześnie, jak to ma miejsce w przypadku każdego narzędzia internetowego, będą także wykorzystywane przez osoby i organizacje w celach przestępczych czy dezinformacyjnych. Warto obserwować ich dalszy rozwój, gdyż na pewno staną się częścią naszego codziennego życia.

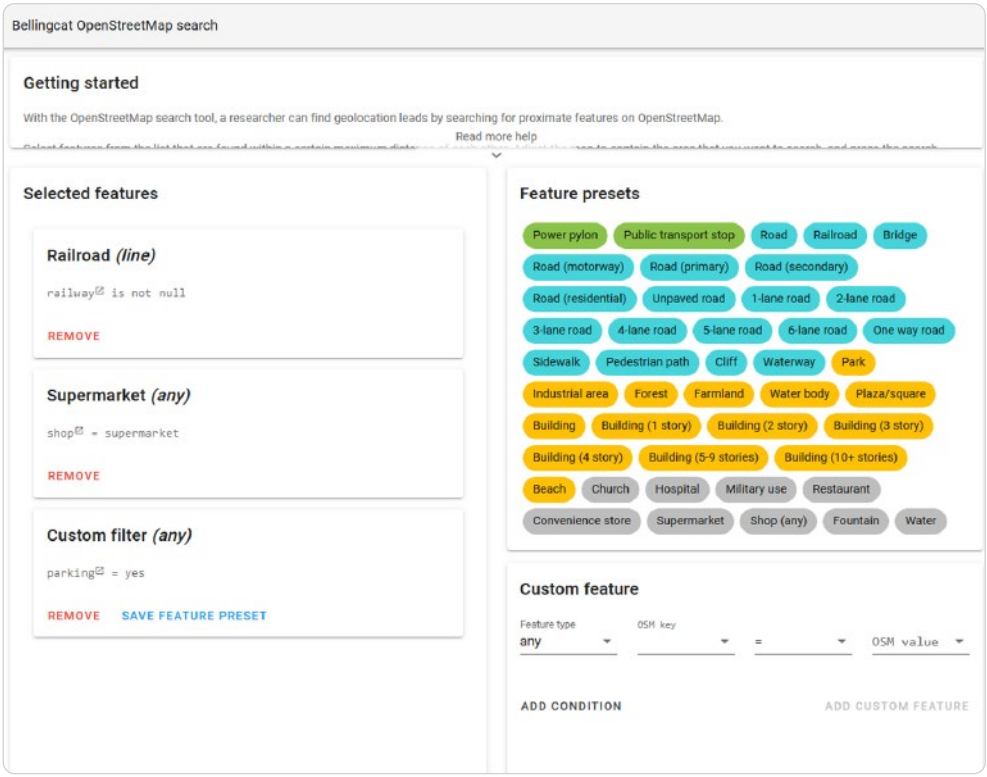
R29 CZY GEOLOKALIZACJA MOŻE ZROBIĆ SIĘ SAMA?

Identyfikacja miejsca wykonania zdjęcia bez użycia do tego celu zawartych w pliku metadanych lub innych wskazówek (np. wpisów w mediach społecznościowych, które towarzyszą danemu obrazowi, zdradzających położenie autora) jest niejednokrotnie zadaniem bardzo złożonym. Jak już zostało wspomniane w rozdziale *Jedno zdjęcie, by znaleźć ich wszystkich – OSINT na podstawie materiałów wizualnych* (s. 117–123), można do tego wykorzystać wszystkie widoczne na zdjęciu elementy, co bywa szczególnie owocne w przypadku widoków miejsc na zewnątrz budynków. Czy jednak w dobie ogromnego skoku technologicznego narzędzi mapowych i do analizy obrazów można ten proces zautomatyzować? Okazuje się, że odpowiedź na to pytanie jest twierdząca.

Pozyskiwanie danych z map cyfrowych

Wiele map cyfrowych zawiera dane o obiektach znajdujących się w konkretnych lokalizacjach, więc zadając odpowiednie pytanie, możemy sprawić, że proces poszukiwań stanie się o wiele szybszy.

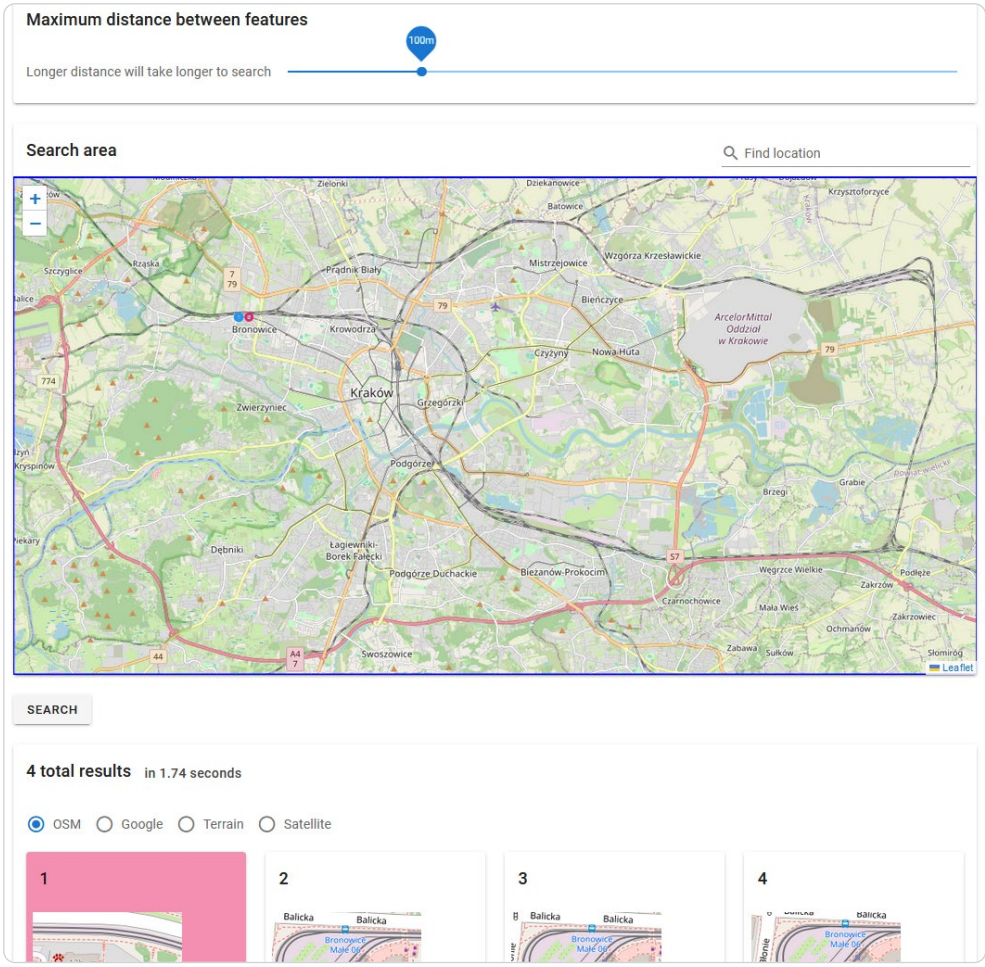
Jednym z serwisów mapowych, który zawiera dane o obiektach, jest Open Street Map. W 2023 roku pojawiło się narzędzie, które umożliwia stworzenie w bardzo prosty sposób odpowiedniego zapytania do Open Street Map i znalezienie miejsc, które spełniają serię warunków w określonym obrębie. Przykładowo: w odległości nie większej niż 100 metrów od siebie występują jednocześnie: supermarket, parking i tory. Będąc w posiadaniu zdjęcia, na którym widać te obiekty, i wiedząc, w jakim obszarze należy szukać, zamiast wykonywać żmudne przeszukiwanie map np. całego miasta, możemy otrzymać odpowiedź w jednej chwili. To narzędzie to Bellingcat OpenStreetMap search (rysunek 156). Jest dostępne za darmo, a jedyne ograniczenie stanowi to, że trzeba się do niego zalogować z wykorzystaniem konta Google lub adresu e-mail.



Rysunek 156. Formułowanie zapytania w Bellingcat OpenStreetMap search

Korzystając z tego narzędzia (jak z każdego innego), należy mieć na uwadze fakt, że może ono wprowadzać w błąd. Dlatego każdy wynik trzeba sprawdzić również przy użyciu innych metod, brak wyniku natomiast nie musi oznaczać, że takiego miejsca nie ma na przeszukiwanym obszarze, a jedynie to, że narzędzie go nie znalazło.

Na rysunku 157 znalezione zostały cztery miejsca spełniające zadane warunki, ale trzy z nich znajdują się w tym samym punkcie, a czwarte także jest niedaleko, więc istnieje duża szansa, że wyniki wskazują poszukiwaną lokalizację.



Rysunek 157. Wyniki wyszukiwania widoczne w Bellingcat OpenStreetMap search

Więcej automatyzacji!

Czy możliwe jest pójście jeszcze o krok dalej i zlecenie narzędziom wykonania całej pracy analitycznej dla zdjęcia nieznanej lokalizacji? Okazuje się, że jak najbardziej. W ostatnim czasie pojawiło się kilka narzędzi opartych na mechanizmach AI, które wykonują część pracy i wskazują miejsce zrobienia przesłanego im zdjęcia. Czy są dokładne? Zaskakująco tak. Czy można im ufać? Nie. Bo to tylko narzędzia.

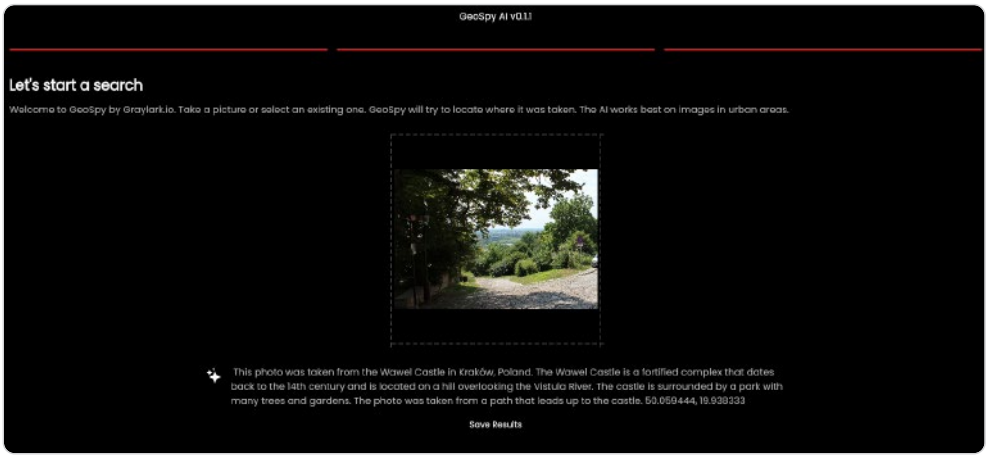
Jak sobie radzą przedstawiciele nowego nurtu geolokalizacji „automagicznej”?

Sprawdziłem trzy narzędzia: GeoSpy AI, Picarta AI oraz TIB Geolocation Estimation. Do testów wykorzystałem zdjęcia, które nie były wcześniej publikowane w Internecie (poza zdjęciem metra, które pojawiło się kiedyś na Twitterze).

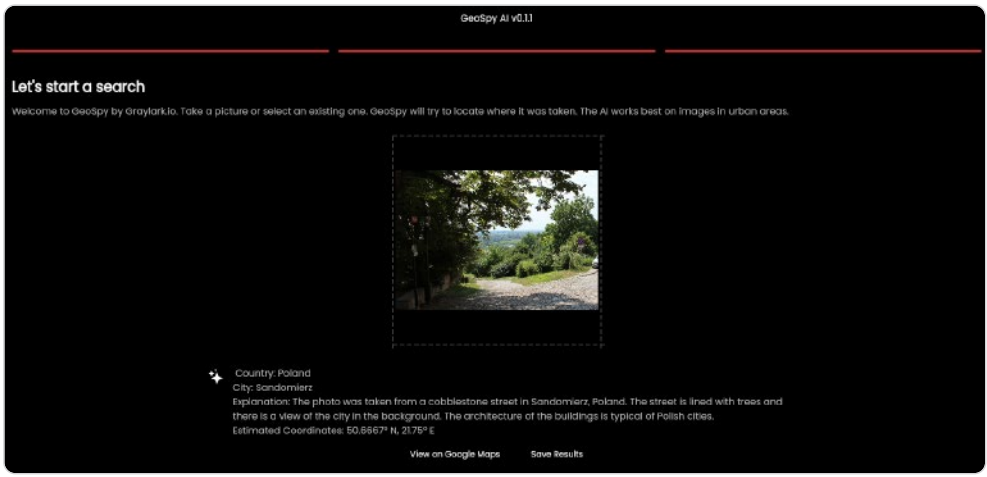
Na pierwszy ogień – zdjęcie z bardzo małą liczbą szczegółów architektonicznych, wykonane w Sandomierzu (rysunek 158).

Rysunek 158. Zdjęcie z Sandomierza wykorzystane do testu narzędzi geolokalizacyjnych

Narzędzie **GeoSpy AI** wypadło całkiem nieźle i, co ciekawe, najpierw zidentyfikowało sandomierski krajobraz jako Wawel (rysunek 159), żeby kilka dni później określić już poprawną lokalizację wykonania zdjęcia (rysunek 160). Na kilka dni przed pisaniem tego tekstu ponownie sprawdziłem wynik poszukiwań tego narzędzia – i wtedy ujęcie to zostało zidentyfikowane jako wykonane w Kazimierzu Dolnym, więc pomyłka nie była zbyt duża. Niestety, miesiąc później narzędzie wskazało lokalizację na Węgrzech, więc jak widać, wyniki zmieniają się coraz bardziej.

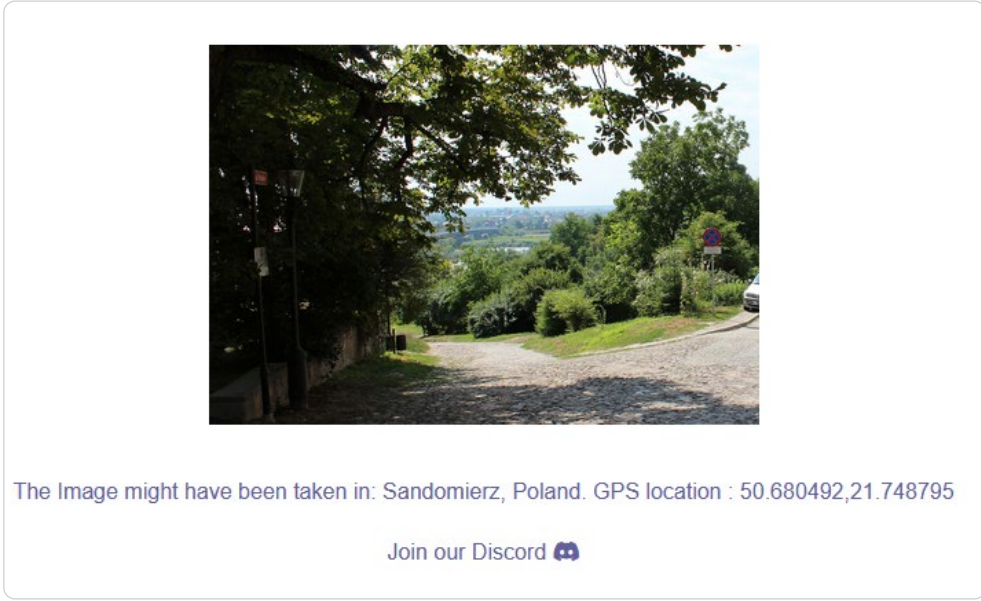


Rysunek 159. Pierwszy wynik z GeoSpy AI



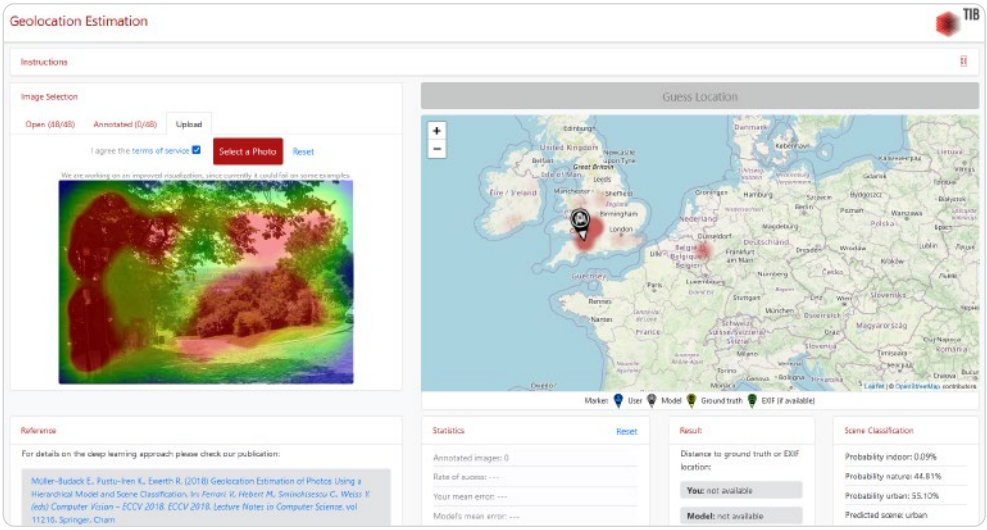
Rysunek 160. Kolejny, tym razem poprawny, wynik z GeoSpy AI

Narzędzie **Picarta** poradziło sobie świetnie i wskazało poprawnie Sandomierz (rysunek 161), chociaż podane koordynaty GPS określają dokładnie widok w drugą stronę niż ten ze zdjęcia. Jest to jednak i tak wysoka dokładność jak na narzędzie, które dysponowało tylko takim zdjęciem.



Rysunek 161. Wynik z narzędzia Picarta AI

TIB Geolocation Estimation wskazało Wielką Brytanię lub ewentualnie Belgię, co jest zupełnie nietrafionym wynikiem (rysunek 162).

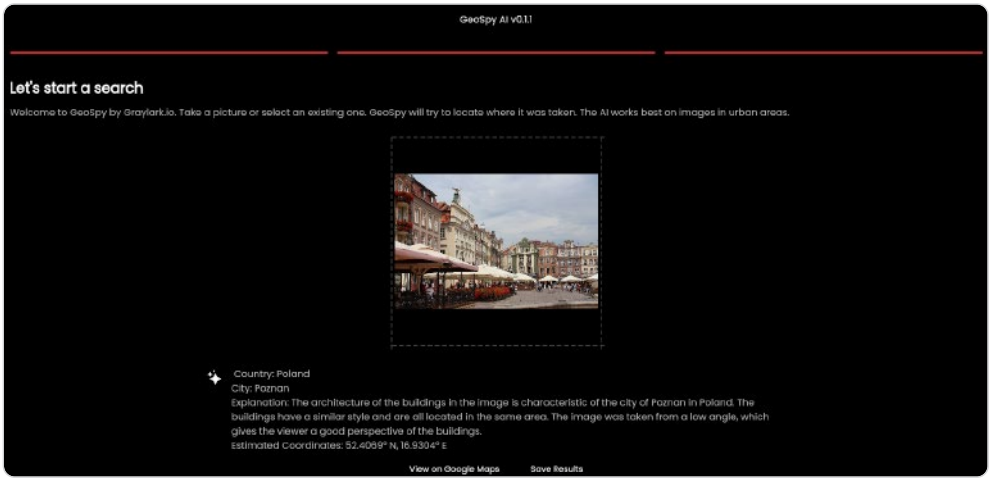


Rysunek 162. Wynik z TIB Geolocation Estimation

Jak widać, wyniki są naprawdę imponujące. Badałem także, czy drugie i trzecie narzędzie „zmienia zeznania" po kilku dniach, ale dla tych konkretnych zdjęć wskazywały one ciągle te same miejsca.

Zobaczmy, jak poradzą sobie ze zdjęciem zrobionym w środku dużego miasta. Za przykład posłuży zdjęcie wykonane na Starym Rynku w Poznaniu.

Narzędzie **GeoSpy AI** (rysunek 163) poprawnie zidentyfikowało Poznań. Wskazana lokalizacja GPS 52.4069° N, 16.9304° E mija się z faktycznym miejscem dosłownie o kilka ulic.

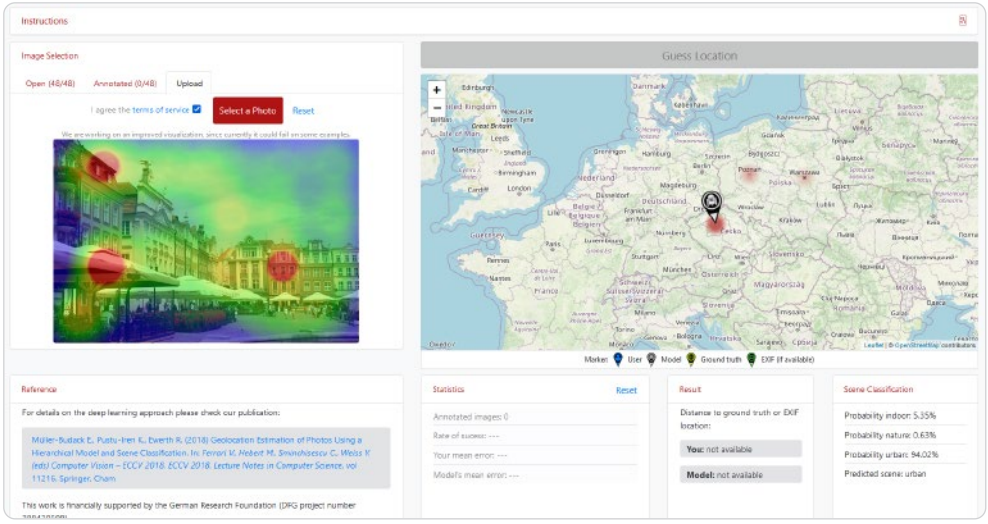


Rysunek 163. Wynik analizy zdjęcia z Poznania w GeoSpy AI

Picarta także nie zawiodła i wskazała poprawnie Poznań. Koordynaty GPS 52.409573° N, 16.934156° E były podobnie oddalone od faktycznej lokalizacji jak w przypadku pierwszego narzędzia, ale w innym kierunku (rysunek 164).

Rysunek 164. Wynik analizy zdjęcia z Poznania w narzędziu Picarta AI

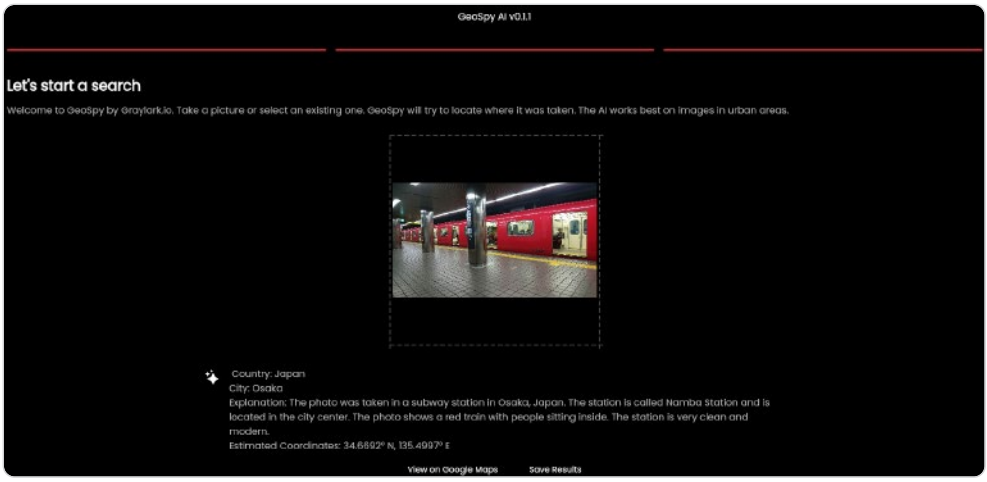
Narzędzie **TIB Geolocation Estimation** znów nie trafiło, wskazując Czechy, chociaż tym razem Poznań znalazł się także na mapie, jednak z mniejszym prawdopodobieństwem trafności (rysunek 165).



Rysunek 165. Wynik analizy zdjęcia z Poznania w TIB Geolocation Estimation

Jako trzeci przykład posłużyło zdjęcie metra wykonane w mieście Nagoja w Japonii, którego użyłem kiedyś w jednym z quizów geolokalizacyjnych w ramach „gościnnych występów" na Quiztime[116] na Twitterze. Nie wszystkim uczestnikom tego quizu udało się poprawnie odgadnąć miasto, tym bardziej warto sprawdzić, jak wypadło AI.

Na pierwszy ogień tradycyjnie poszło **GeoSpy AI**. Stacja metra została poprawnie zidentyfikowana, kraj również został określony prawidłowo, ale błędnie podane zostało miasto – to nie Osaka (rysunek 166).

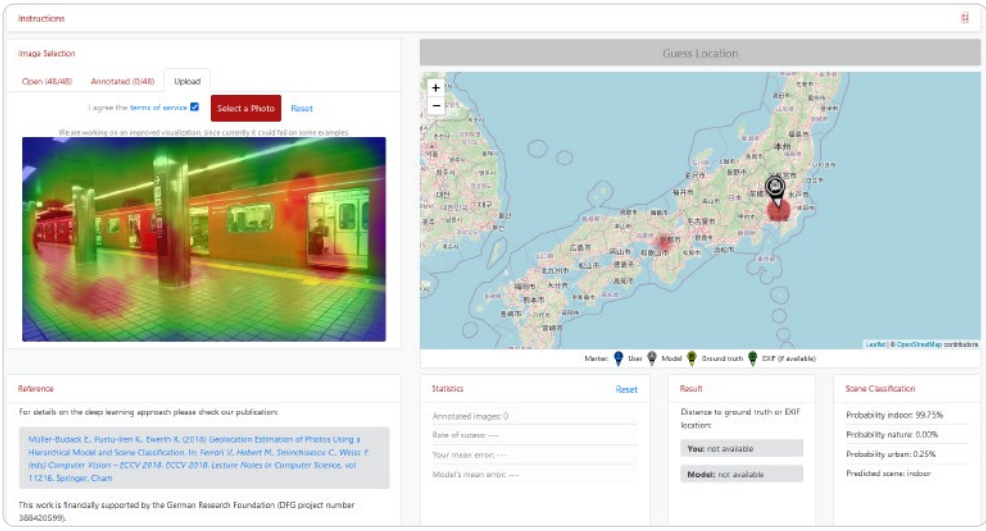


Rysunek 166. Wynik analizy zdjęcia metra z GeoSpy AI

Picarta także poprawnie zidentyfikowała kraj, jednak zupełnie nie trafiła nawet w region, wskazując mocno oddalone na północ Sapporo (rysunek 167).

Rysunek 167. Wynik analizy zdjęcia metra z narzędzia Picarta AI

TIB Geolocation Estimation, podobnie jak inne narzędzia, poprawnie zidentyfikowało kraj, jednak nie miasto (rysunek 168). Na mapie wskazane było Tokio lub Osaka. Żadne narzędzie więc nie poradziło sobie w pełni z tym przykładem.



Rysunek 168. Wynik analizy zdjęcia metra z TIB Geolocation Estimation

Podsumowanie

Jak widać, wyniki działania narzędzi potrafią zmieniać się z dnia na dzień, co można było zaobserwować w przypadku GeoSpy AI. Za trzecim podejściem narzędzie zidentyfikowało lokalizację poprawnie, ale nie można stwierdzić, że tak będzie za każdym razem i że wyniki z kolei nie będą coraz bardziej odbiegać od prawdy. Picarta miała dwa trafienia na trzy, co także stanowi dość dobry wynik. Badane narzędzia używają jednak różnych sposobów określania lokalizacji wykonania zdjęcia i warto korzystać ze wszystkich, ponieważ dla jednego ujęcia jedno narzędzie może okazać się pomocne, podczas gdy w wypadku innych – inne. Każde, nawet najlepsze, narzędzie może się mylić, więc nigdy nie można uznawać uzyskanego wyniku za pewny. Widać wszakże, że tradycyjna geolokalizacja ma potężnego konkurenta, który staje się z dnia na dzień coraz lepszy. Ma to duży wpływ na poszukiwania z użyciem zdjęć, które są wykorzystywane przez służby do ustalania miejsca pobytu przestępców lub osób zaginionych, jednak z drugiej strony – będzie to miało na pewno wpływ na prywatność w sieci…

R30 WIĘCEJ AI, OSINT WYTRZYMA (?)

Na przestrzeni ostatnich lat obserwujemy istotną metamorfozę narzędzi OSINT-owych, wynikającą z wykorzystania technologii określanej zazwyczaj zbiorczo i ogólnie jako AI, czyli sztuczna inteligencja*. Samo określenie AI jest bardzo szerokie i **dotyczy raczej koncepcji tworzenia maszyn zdolnych do wykonywania zadań** w sposób podobny do tego, w jaki wykonałby je człowiek.

W zakresie pojęcia AI można wyodrębnić poddziedzinę nazywaną **uczeniem maszynowym** (ang. *machine learning*, ML), **czyli zbiór technologii** umożliwiających uczenie się na podstawie zestawu danych historycznych. Podzbiorem ML jest z kolei **generatywna sztuczna inteligencja** (ang. *generative AI*, umożliwiająca np. tworzenie nowych obrazów, tekstów lub materiałów wideo na podstawie danych historycznych). Jej podzbiorem (przynajmniej częściowo) są natomiast **duże modele językowe** (ang. *large language models*, LLM), które obejmują rozumienie, przetwarzanie i generowanie danych tekstowych.

Może się wydawać, że jest to jedynie mały wycinek ogólnej koncepcji AI. Mimo to wykorzystanie go spowodowało nie tylko ogromne zwiększenie możliwości różnego rodzaju narzędzi OSINT-owych, lecz również wymusiło konieczność zmiany niektórych technik oraz metodyki samego prowadzenia rozpoznania otwartoźródłowego.

W tym rozdziale skupię się na na przeglądzie zmian.

Gdzie AI może pomóc?

OSINT jest jednym z typów rozpoznania, który podlega tzw. cyklowi wywiadu (rysunek 169). W ramach tego procesu najczęściej wyodrębnia się pięć podstawowych etapów:

1. planowanie/podejmowanie decyzji,
2. zbieranie danych,
3. przetwarzanie,
4. analiza i wytwarzanie wyników,
5. przekazywanie informacji.

W których etapach i w jaki sposób można zatem wykorzystać narzędzia AI**?

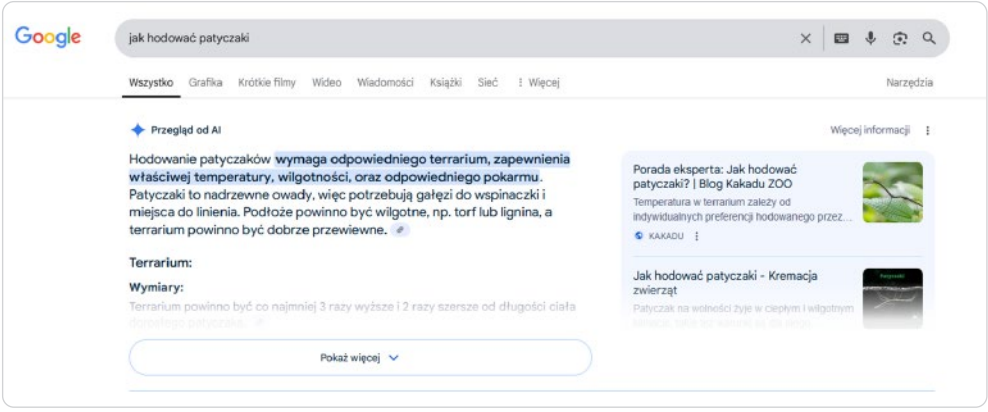
Na etapie **zbierania danych** możliwości oferowane przez współczesne mechanizmy wykorzystujące szeroko pojęte AI są nieocenione. Szybkie przeszukiwanie rozległych zbiorów danych pozwala w istotny sposób przyspieszyć proces niemal każdego wyszukiwania. Wyszukiwarka Google coraz

* Ten rozdział powstał w lipcu 2025 roku. To ważna informacja dla czytających, bo w świecie AI postęp mierzy się już w miesiącach, co może oznaczać, że teraz świat wkoło jest już w innym miejscu…

** Podobnie jak wiele źródeł, będę używał potocznego i ogólnego nazewnictwa „narzędzia AI", żeby nie wprowadzać niepotrzebnych dysonansów.

częściej wyświetla ponad wynikami wyszukiwania pozycję *Przegląd od AI*[117] (rysunek 170), pokazującą skrótowe, zbiorcze podsumowanie uzyskanych wyników, co pozwala oszczędzić czas użytkownika. Nie trzeba już „przechodzić" kolejno przez wszystkie linki i zapisywać lub zapamiętywać poszczególnych przydatnych informacji, a na koniec tworzyć podsumowania.

Rysunek 169. Cykl wywiadu składający się z pięciu elementów

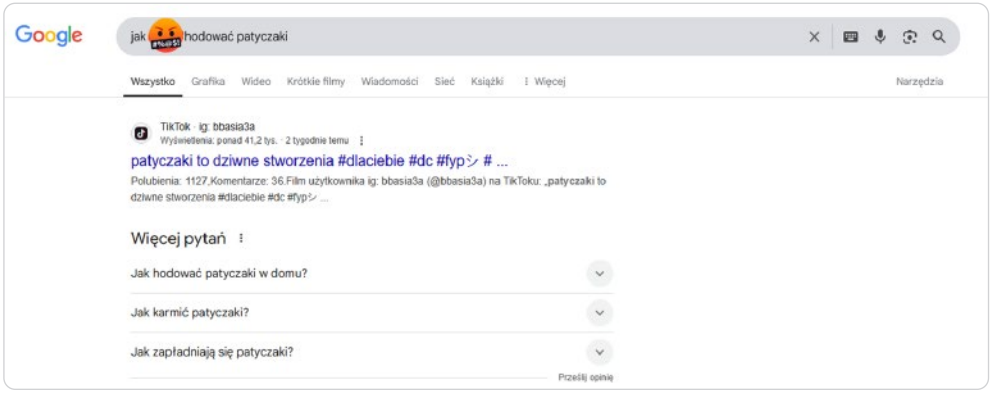


Rysunek 170. Wyszukiwanie w Google z wyświetlonym *Przeglądem od AI*

Jednak nie dla wszystkich fraz generowany jest *Przegląd od AI*. Nie zawsze też użytkownik chce taki przegląd otrzymać. Sposobów na wyłączenie tej opcji jest kilka. Pierwszy z nich to proponowane przez Google kliknięcie w zakładkę SIEĆ (dostępną pod polem frazy wyszukiwania), co spowoduje wyświetlenie wyłącznie linków do wyników wyszukiwania. Drugim jest dodanie *-ai* na końcu frazy wyszukiwania (rysunek 171). Trzeci sposób, jaki udało mi się znaleźć, to

wykorzystanie w wyszukiwanej frazie niecenzuralnego, polskiego słowa na „k" (tego najgorszego, słabsze nie działają), które wyłącza *Przegląd od AI* dla danego wyszukiwania w Google (rysunek 172). Tę ostatnią metodę traktowałbym jednak bardziej w kategoriach żartu rodem z *Seksmisji** lub ciekawostki internetowej niż faktycznej techniki.

Rysunek 171. Brak wyświetlania *Przeglądu od AI* po skorzystaniu z operatora *-ai*



Rysunek 172. Brak wyświetlania *Przeglądu od AI* w przypadku użycia niecenzuralnych słów

Wykorzystanie AI w wyszukiwaniu tekstowym ma jeszcze jedną przewagę nad tradycyjnym wyszukiwaniem z wykorzystaniem zbioru słów kluczowych. Narzędzia wykorzystujące AI zdają się lepiej rozumieć kontekst pytania i dają odpowiedzi uwzględniające także słowa pokrewne, zamiast realizować klasyczne wyszukiwanie jedynie po konkretnych słowach wpisanych w pole wyszukiwania. Ta „ludzka" właściwość narzędzi wykorzystujących AI może prowadzić do znalezienia znacznie bardziej odpowiednich wyników oraz większej ich liczby w ramach interesującego zagadnienia, a co za tym idzie – uzyskania

* *Seksmisja* – kultowa polska fantastycznonaukowa komedia filmowa z 1983 roku.

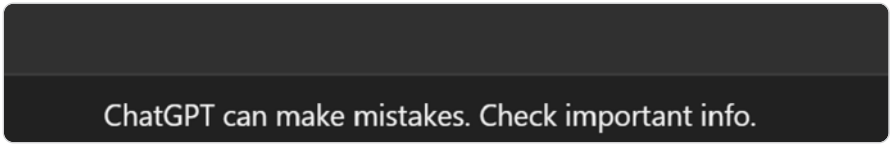
pełniejszego obrazu sytuacji. Jest to szczególnie ważne w przypadku poszukiwań, w których osoba wyszukująca nie ma wystarczającej wiedzy, by budować precyzyjne zapytania lub po prostu nie przyjdzie jej w danym momencie do głowy sposób na inne sformułowanie frazy wyszukiwania.

Czy aby na pewno jest tak pięknie?

Do tego momentu sytuacja wygląda wzorowo: wyszukujemy szybciej, otrzymujemy szersze spojrzenie na dane zagadnienie – i wszystko w zrozumiałym dla przeciętnego użytkownika streszczeniu.

Niestety, **narzędzia AI są bardzo podatne na tzw. halucynacje**, czyli zwracanie informacji, które są częściowo lub zupełnie nieprawdziwe. Jeśli użytkownik nie zweryfikuje linków, podanych w ramach podsumowania, może oprzeć swoje dochodzenie na fałszywych informacjach, co w najlepszym przypadku doprowadzi do złej oceny z pracy bazującej na tak zebranych danych, a w najgorszym… konsekwencje mogą być bardzo poważne i zależne od wagi prowadzonego OSINT-u. Zakładam jednocześnie, że podsumowanie otrzymane od narzędzia AI, które nie zawiera żadnych linków, jest od razu do pominięcia, ponieważ nie da się w łatwy sposób zweryfikować zebranych informacji. Stwierdzenie: „Ufaj, ale weryfikuj", jest w tym aspekcie kluczowe.

Same narzędzia AI, począwszy od *Podglądu od AI* w wynikach wyszukiwania w Google, a skończywszy na wszelkich modelach językowych typu ChatGPT czy Claude, posiadają dołączone ostrzeżenie (rysunek 173), co wskazuje na to, że do generowanych przez nie odpowiedzi mogły wkraść się pomyłki i że zawsze należy sprawdzać, czy są zgodne z prawdą. Tej jednej, drobnej rady należy zawsze przestrzegać.



Rysunek 173. Ostrzeżenie, że ChatGPT może popełniać błędy

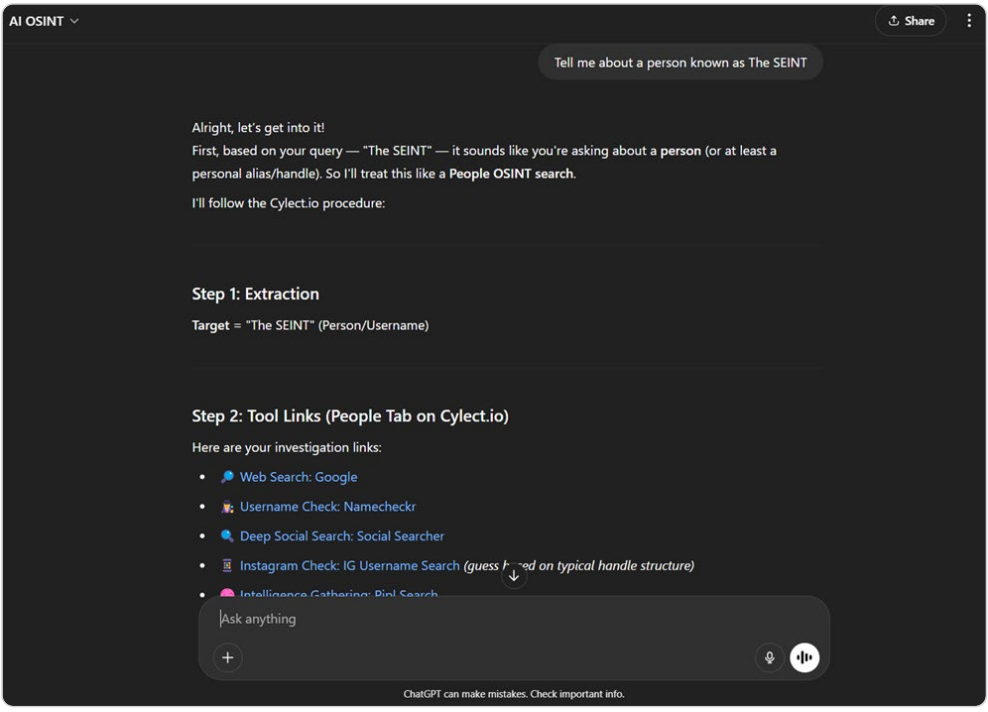
Asystenci wyszukiwania

W przypadku wyszukiwania informacji dwa źródła zawsze będą lepsze niż jedno, a kilkanaście lepszych niż dwa*. Możliwości łatwego wykorzystania wielu modeli językowych daje portal Cylect[118], który poza rozwiązaniami opartymi na AI oferuje także zbiór tradycyjnych narzędzi przeznaczonych do różnych

* Przy okazji dobra rada: warto unikać bazowania na wyłącznie jednym źródle danych. Jeśli informacje na ten sam temat są możliwe do znalezienia w różych źródłach –należy wziąć je pod uwagę. Jeśli danej informacji nie ma w innych źódłach, to istnieje duża szansa, że właśie trafiło się na źódło dezinformacji.

obszarów rozpoznania internetowego. W ramach narzędzi AI dostępne jest wyszukiwanie informacji poprzez takie narzędzia jak np.: Phind[119], Perplexity[120], Copilot[121], ChatGPT[122] lub DeepSeek[123]. Cylect oferuje także OSINT-owego asystenta AI, opartego na modelu ChatGPT, którego zadaniem jest pomoc w zakresie poszukiwań informacji w sieci. Do niedawna na stronie Cylect można było łatwo znaleźć link do bezpłatnej wersji **asystenta AI OSINT**. Obecnie jest to nieco utrudnione, jednak w linkach wyświetlanych stron dotyczących płatnej wersji odnośnik ten jest nadal dostępny.

Pod adresem AI OSINT[124] możliwe jest przetestowanie możliwości wskazanego narzędzia i przekonanie się, w jakim stopniu jest ono w stanie przyspieszyć konkretne poszukiwania (rysunek 174). Muszę przyznać, że narzędzie sprawdziło się doskonale do określenia punktu startowego, pokazującego właściwe kierunki dalszego prowadzenia rozpoznania osobowego, bez konieczności wchodzenia w głębszą analizę źródeł. Należy jednak zauważyć, że w ramach moich testów zaobserwowałem również kilka przypadków halucynacji.

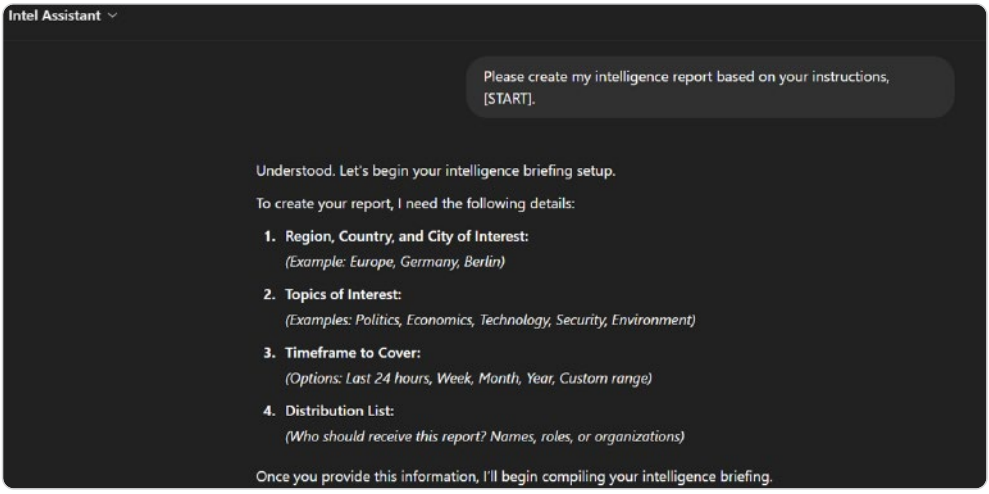


Rysunek 174. Asystent AI OSINT od Cylect

Innym przykładem próby stworzenia OSINT-owego asystenta AI jest **Intel Assistant**[125], również wykorzystujący ChatGPT jako podstawę swojego działania (rysunek 175). Zadaniem tego wirtualnego asystenta jest **tworzenie analiz**

i pisanie raportów, które mają uwolnić analityków od tego rodzaju prac. Jako dane wejściowe Intel Assistant musi otrzymać: obszar zainteresowania (kontynent, kraj i miasto), tematykę, w ramach której ma zdobywać informacje (polityka, ekonomia, technologia, bezpieczeństwo itp.), okno czasowe, z którego dane mają być brane pod uwagę, oraz listę podmiotów, do których skierowany będzie raport.

Sama koncepcja wydaje się bardzo interesująca, z wyjątkiem faktu, że w przypadku tego asystenta duża część wyników bywa wynikiem halucynacji, a przynajmniej takie były moje obserwacje podczas jego testów. Jeśli obszar będący przedmiotem analizy jest dobrze opisany w wielu źródłach, istnieje spora szansa na otrzymanie wiarygodnego raportu. Zauważyłem jednak, że w przypadku bardziej niszowych tematów wyniki są niezadowalające. Pocieszeniem może być fakt, że do raportu dołączane są linki źródłowe, które oczywiście należy sprawdzić, aby upewnić się co do rzetelności wyniku analizy. Zdarza się jednak tak, że i one bywają wynikiem halucynacji.



Rysunek 175. Asystent Intel Assistant

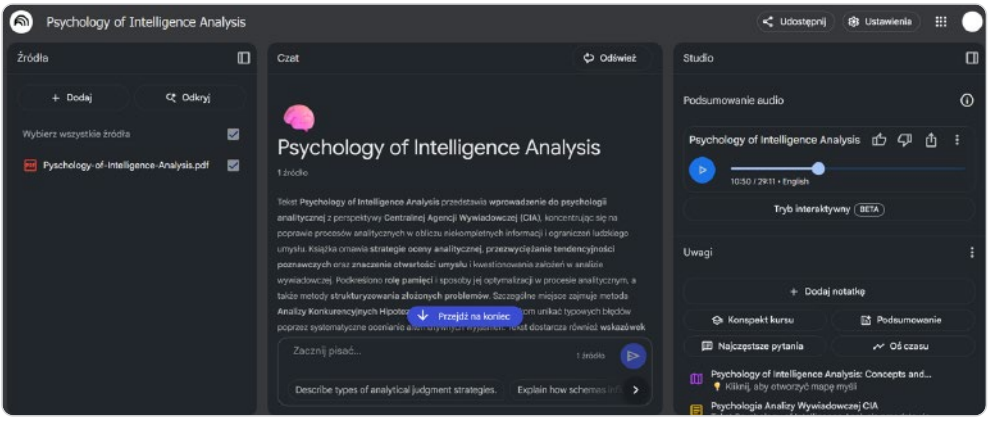
Jeśli mowa o zestawieniach rozwiązań AI wspomagających OSINT, to interesującym zbiorem linków do nich może się także pochwalić projekt **CQCore**[126] na swojej stronie na Githubie. Narzędzia pogrupowano na kategorie m.in. wyszukiwanie graficzne, tłumaczenie czy OCR. Spis daje dobry pogląd na aktualne możliwości narzędzi AI w zakresie OSINT-u. Świadomy użytkownik korzystający z dobrodziejstw tych technologii musi jednak się zastanowić, czy na pewno przekazanie danych wejściowych do danego systemu wspomagającego jest bezpieczne i pożądane.

Narzędziem, które w mojej ocenie może okazać się bardzo przydatne, nie tylko w analizie danych, ale także możliwości poszerzania swojej wiedzy, jest

NotebookLM firmy Google (rysunek 176)[127], **wykorzystujący** oczywiście (jak przystało na narzędzie Google) **Gemini jako chatbota**. Warto wspomnieć, że to narzędzie wykorzystuje technikę RAG (Retrieval-Augmented Generation), czyli nie bazuje jedynie na zbiorze danych, na którym został wytrenowany (jak to ma miejsce w przypadku tradycyjnych modeli językowych), ale korzysta przede wszystkim z informacji przekazanych przez operatora. W przypadku NotebookLM taką bazę stanowią wszystkie dokumenty i linki, które wskaże jego użytkownik. Takie podejście umożliwia uzyskanie dokładniejszych odpowiedzi w konkretnym obszarze wiedzy i generuje mniej halucynacji.

Z jednej strony, umożliwia wykonanie analizy i wygenerowania podsumowania źródeł internetowych (np. stron, filmów na YouTube, dokumentów Google Docs czy prezentacji Google Slides) lub lokalnych (np. dokumentów i książek w formie PDF) wraz z opcją ich porównania i zaproponowania wniosków wynikających z ich różnic.

Z drugiej strony, jego nieocenioną funkcjonalnością jest **tworzenie podsumowań w formie podcastów**, co umożliwia zapoznanie się z badanym zagadnieniem w dużo przyjemniejszej formie rozmowy dwóch osób na wskazany temat. Podejście to może być także dobrym sposobem na zaznajomienie się z informacjami np. w trakcie podróży samochodem, kiedy jedyną możliwością ich przyswajania jest słuchanie. Muszę przyznać, że działanie NotebookLM daje dużo możliwości nie tylko w zakresie analizy i przetwarzania dużych ilości danych (np. stworzenie podcastu z ponadstustronicowej książki w ciągu minuty jest naprawdę przyzwoitym wynikiem), ale także tworzenia map myśli dla analizowanych tematów i quizów do nich.



Rysunek 176. Narzędzie NotebookLM od Google

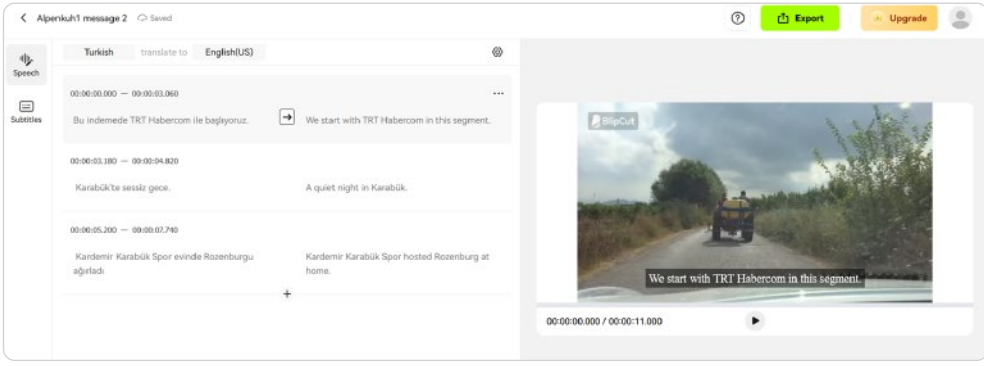
Transkrypcja i tłumaczenie

W czasach, kiedy swoją karierę rozpoczynała pionierska, brytyjska agencja OSINT-owa: BBC Monitoring, analiza informacji pochodzących z gazet i audycji radiowych z różnych krańców świata wymagała sztabu pracowników znających poszczególne języki, a najlepiej dodatkowo realia konkretnych krajów. Dziś wystarczy jedno narzędzie, które nie tylko przetłumaczy tekst, ale także rozpozna, z jakim językiem ma do czynienia, a także wykona transkrypcję z materiału audio.

Paleta narzędzi tego typu jest szeroka. Niestety, większość z nich wymaga płatnej subskrypcji. Na potrzeby weryfikacji tego, co może zrobić każda osoba w Internecie, bez angażowania środków finansowych, wyszukałem te bezpłatne, a jednocześnie posiadające funkcjonalności w zakresie rozpoznania języka, transkrypcji i tłumaczenia. Przykładem najbardziej ergonomicznego, według mnie, narzędzia do transkrypcji i tłumaczenia tekstu z materiału audio był **AI Video Translator** od BlipCut (rysunek 177)[128].

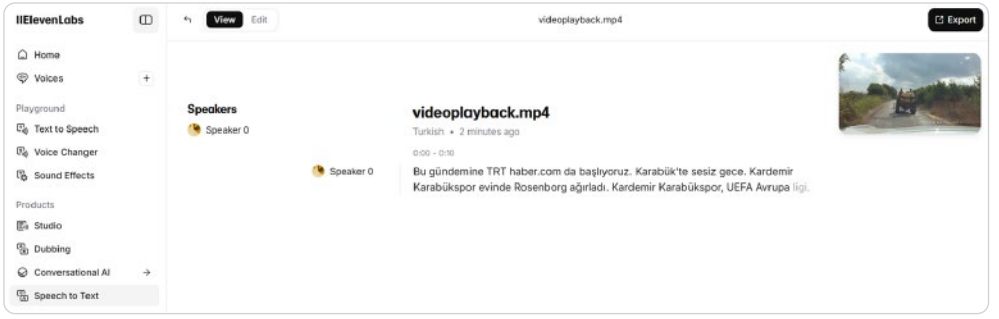
Jako bazę filmów do testów wykorzystałem zgrany z YouTube materiał wideo, który związany był z tematem przekazywania sobie informacji przez rosyjskich szpiegów (temat ten szerzej poruszałem podczas Mega Sekurak Hacking Party w 2024 roku), a który jako ścieżkę dźwiękową posiada nagranie z tureckiej rozgłośni radiowej. Oczywiście informacja o tym, że spiker mówi po turecku, nie jest podana w filmie, ani w jego opisie, więc narzędzie musiało rozpoznać język we własnym zakresie. Wynikiem była pełna transkrypcja materiału, z podziałem na odcinki czasowe oraz tłumaczeniem na określony język (w tym przypadku wybrałem angielski).

Moim zdaniem największym plusem tego typu rozwiązań jest zdolność narzędzia do identyfikacji języków, bo o ile angielski czy niemiecki większość osób pewnie rozpozna bez pudła, to z bardziej „egzotycznymi" będzie to dużo trudniejsze, jeśli nie niemożliwe.



Rysunek 177. Transkrypcja filmu z wykorzystaniem narzędzia AI Video Translator firmy BlipCut

W zakresie przetwarzania mowy na tekst (lub tekstu na mowę, co jednak w przypadku OSINT-u będzie miało mniejsze znaczenie) bardzo dobre narzędzie oferuje **ElevenLabs** – amerykańska firma założona przez dwóch inżynierów polskiego pochodzenia. Ich główną motywacją do pracy były wspomnienia z dzieciństwa, dotyczące słabo zdubbingowanych filmów amerykańskich. W ramach opcji oferowanych przez ElevenLabs trzeba jednak samemu wybrać, z jakiego języka będzie przeprowadzana transkrypcja materiału audio, bez możliwości jego rozpoznania i tłumaczenia. Plusem jest tu natomiast dużo wyższy poziom rozpoznawania mowy, a także dzielenie zapisanej transkrypcji na role (rysunek 178).



Rysunek 178. Transkrypcja filmu z wykorzystaniem narzędzia od ElevenLabs

Halucynacje

Zatrzymam się jeszcze na chwilę przy błędach generowanych przez narzędzia AI. Korzystając z tego typu narzędzi, warto znać mechanizmy powstawania błędów i umieć sprawdzić, czy w otrzymanych wynikach nie mamy z nimi do czynienia.

Kilkukrotnie wspomniałem już o halucynacjach występujących w trakcie wykorzystywania narzędzi AI. Tym terminem określane jest **zjawisko generowania treści wyglądających wiarygodnie, ale tak naprawdę będących odpowiedziami nieprawdziwymi i niezwiązanymi z danymi wejściowymi**. Możliwe jest wyodrębnienie dwóch ich kategorii: zmian rzeczywistości i błędów zgodności. Każdą z tych kategorii możemy podzielić dalej na podkategorie, w zależności od źródła danego problemu.

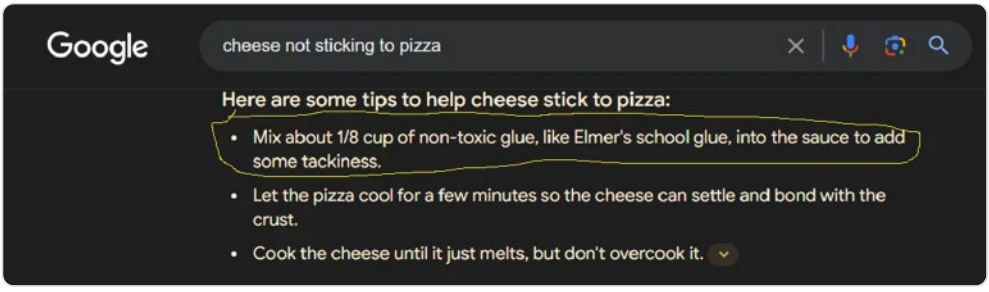
Sumarycznie otrzymamy następujący **podział halucynacji AI**:

- zmiany rzeczywistości:
  - przekręcanie faktów (np. wskazanie, że Jurij Gagarin był pierwszym człowiekiem na Księżycu, podczas gdy był on pierwszym człowiekiem w kosmosie, a na Księżycu jako pierwszy nogę postawił Neil Armstrong);

- zmyślanie faktów (np. wskazywanie istnienia jednorożców jako faktycznie występujących w naturze zwierząt lub sugerowanie nieistniejących artykułów, książek, aktów prawnych, dokumentów itp. jako referencyjnych);
- błędy zgodności:
  - z instrukcją (np. odpowiadanie na zadane pytanie w momencie, gdy instrukcja dotyczyła jedynie przetłumaczenia go);
  - z kontekstem (np. dodawanie do podsumowania elementów, które wykraczają poza zadany kontekst pytania);
  - z logiką (np. błędy logiczne i matematyczne w ramach zadań zawierających obliczenia itp.).

Jeśli jako bazę do trenowania modeli wykorzystano Internet, to prawdopodobieństwo zwracania nieprawdziwych informacji (żeby nie powiedzieć: „bzdur") jest bardzo wysokie. Jednym z najbardziej znanych przykładów (na szczęście już wyeliminowanych) skutków uczenia się modelu na danych z Internetu była odpowiedź na pytanie o sposób na lepsze przywieranie sera do pizzy, która cytowała poradę z serwisu Reddit z 2013 roku. Zawierała ona sugestię, aby dodać do sosu ⅛ filiżanki kleju szkolnego (rysunek 179)[129].

Nie da się ukryć, że **bazowanie na danych z sieci skutkuje wynikami pełnymi różnego rodzaju uproszczonych schematów myślenia, uprzedzeń i skrajnych opinii**. Niestety, sposób interakcji z narzędziami AI, w którym na zadane pytanie otrzymujemy pełną, „ludzką" odpowiedź, którą podświadomie traktujemy jako odpowiedź eksperta, obniża motywację do analizowania i podważania uzyskanych rezultatów. Sytuacja ta stanowi istotne zagrożenie w obszarze skutków wykorzystywania modeli językowych.



Rysunek 179. Historyczny wynik wyszukiwania sposobu na lepsze przywieranie sera do pizzy, zawierający prześmiewczą poradę z serwisu Reddit

Halucynacje nie muszą ograniczać się oczywiście jedynie do danych tekstowych. Podobna sytuacja będzie mieć miejsce w przypadku grafik (rysunek 180[130]). Tę niedoskonałość działania narzędzi AI do generowania rzeczywistych obrazów

można jednak przekuć w atut analityka, jeśli jego zadaniem jest weryfikacja prawdziwości analizowanych obrazów.

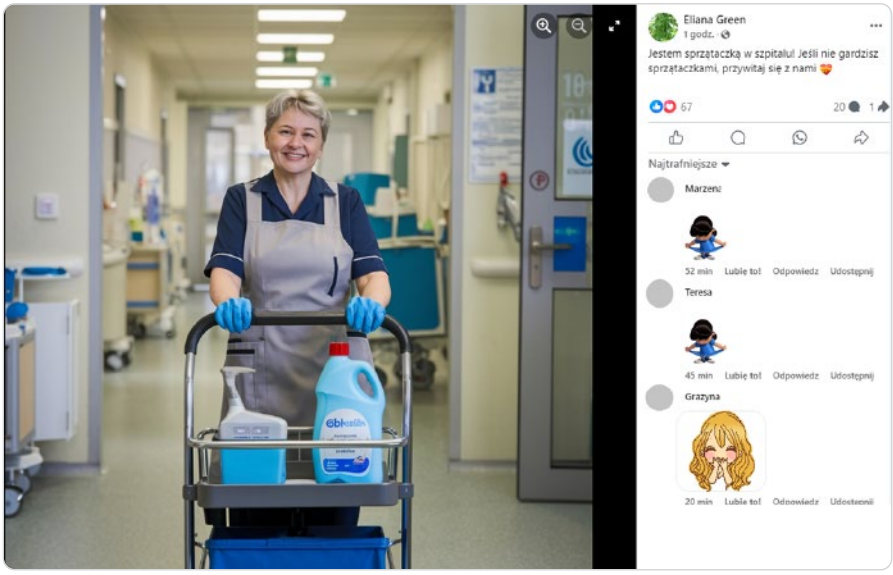
Rysunek 180. Przykład halucynacji narzędzia AI do generowania obrazów

Wyścig między manipulacjami a ich analizą

Techniki analizy i weryfikowania danych cały czas muszą dotrzymywać kroku coraz doskonalszym metodom manipulowania nimi. Zjawisko to można określić istnym „wyścigiem zbrojeń". Sprawa zdaje się coraz trudniejsza, ponie-

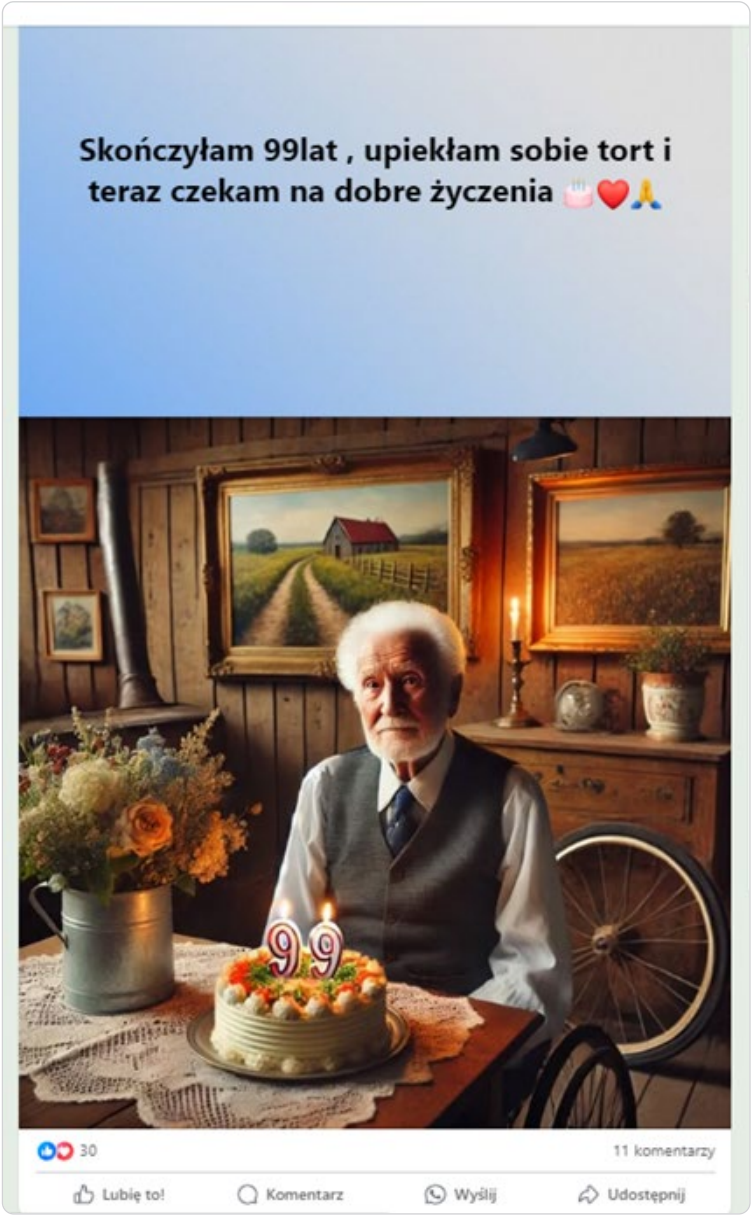
waż generowane obrazy stają się coraz bardziej wiarygodne. Są pozbawione „szóstego palca", „uśmiechu z samych piątek" lub innych, łatwych do wychwycenia niespójności. Jednocześnie osobom wykorzystującym nieprawdziwe obrazy do manipulacji nie zależy na ich dopracowaniu, podobnie jak autorom phishingu nie zależy na poprawności językowej. Duży nakład pracy nie przyniósłby im dużego zysku, a z wykorzystaniem słabych obrazów i tekstów i tak są w stanie oszukać dużą liczbę osób.

Rysunki 181–185 to przykładowe materiały wygenerowane przez AI, zamieszczone w portalu społecznościowym Facebook. Są one publikowane z bardzo dużą częstotliwością, zyskując ogromną popularność*. Co ciekawe, wiele osób reaguje na tego typu „przynętę", upubliczniając swoje dane, jak np. numery telefonów do kontaktu. Zjawisko to jest przerażające, ponieważ dla każdej osoby, która chociaż raz miała do czynienia z analizą sztucznie tworzonych obrazów, zdjęcia te są ewidentnie zmanipulowane. Powtarzają się w nich znane schematy i są one okraszone tendencyjnymi opisami. Może to przypominać trochę zabawę z dzieciństwa w „znajdź różnicę pomiędzy dwoma obrazkami", choć w zamieszczonych poniżej zdjęciach tylko wyćwiczone i wyczulone oko widzi je od razu. No i nie ma oryginału do porównania. Są tylko różnice w stosunku do rzeczywistości.



Rysunek 181. Zdjęcie wygenerowane przez AI w poście zamieszczonym na Facebooku, przedstawiające m.in. opakowania o dziwnej konstrukcji (na wózku, na pierwszym planie)

* Tego typu posty, generujące duży odzew, są często wykorzystywane np. do wprowadzania scamów zamiast „chwytających za serce" treści generowanych przez AI (kiedy post zdobędzie już dużą liczbę lajków i udostępnień) lub do tworzenia konta z dużymi zasięgami, do późniejszej odsprzedaży. Często są to konta udające profile religijne, skierowane do odbiorców cechujących się dużym współczuciem i chęcią pomagania innym, czyli do osób bardziej podatnych np. na oszustwa wykorzystujące przekierowania do fałszywych zbiórek.



Rysunek 182. Na tym zdjęciu pochodzącym z serwisu Facebook również widoczne są łatwe do wychwycenia niespójności: zarówno w opisie do obrazu (odmiana czasownika „skończyć" sugerująca, że autorem fotografii jest kobieta), jak i w widocznych na zdjęciu przedmiotach (niepołączone z niczym elementy wózka inwalidzkiego [?] i komina [?])

Rysunek 183. Podwójne przejście dla pieszych, dziwne znaki oraz sygnalizacja świetlna pozbawiona jakiegokolwiek sensu – to kolejny przykład zdjęcia wygenerowanego przez AI

Rysunek 184. Lewitująca dłoń mężczyzny po lewej, zawiasy na szafkach po stronie klamek, uchwyty łączące drzwi szafki z jej korpusem – czy aby na pewno wszystko jest na swoim miejscu?

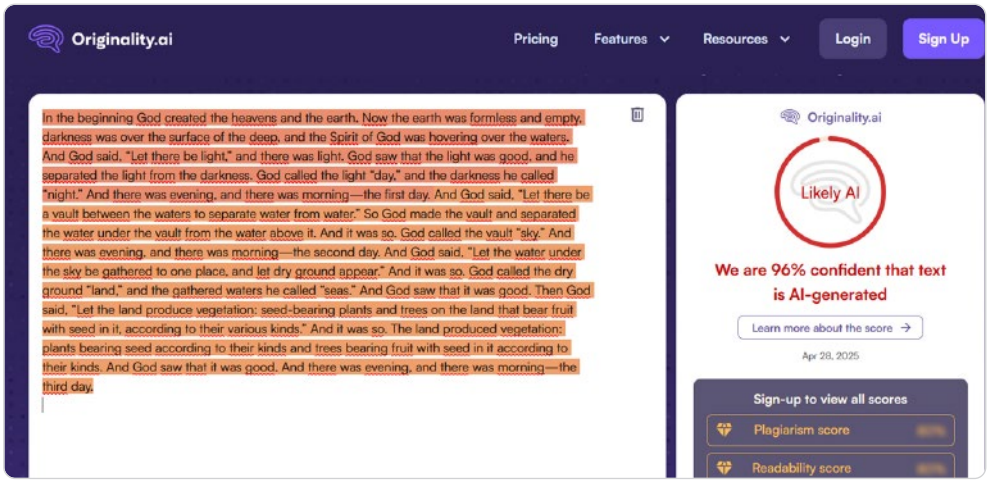
Rysunek 185. Tym razem nietrudno zauważyć dziwną markę ciągnika oraz nietypowy klucz w ręku mężczyzny

Istotny postęp w rozwoju narzędzi obserwujemy również w obszarze **analizy informacji w formie tekstowej**. Algorytmy są cały czas ulepszane w taki sposób, by z jednej strony zwracane wyniki jak najbardziej przypominały dzieło człowieka, a sam fakt, że są wynikiem działania AI, był jak najtrudniejszy do wykrycia. Z drugiej strony, odbywa się też ciągły rozwój narzędzi do wykrywania tekstów generowanych przez AI.

W sieci dostępne są narzędzia do weryfikacji, czy dany tekst nie został wygenerowany przez sztuczną inteligencję. Przykładem takiego rozwiązania, w ograniczonym zakresie bezpłatnego, jest **AI Detector** od Originality.ai[131] (rysunek 186). Niestety, narzędzie to w wielu przypadkach wydaje się bezradne i bardzo omylne.

Jednym z przykładów, na który natknąłem się swego czasu w serwisie Reddit[132], był eksperyment polegający na wklejeniu początku *Księgi Rodzaju* do konkretnego narzędzia. W wyniku analizy wykazano, że tekst ten został w 100% napisany przez AI. W ramach własnych testów próbowałem wklejać różne fragmenty tej księgi – i miałem podobne spostrzeżenia, jednak wyłącznie w przypadku krótszych fragmentów (do około sześciu wersów). Gdy wklejałem dłuższy tekst, wyniki były zgoła inne – kilkanaście wersów było już oznaczane jako w 100% niepochodzące od generatorów AI.

Powyższy przykład pokazuje, że każde narzędzie ma swoje ograniczenia i błędy, które zawsze należy sprawdzić przed jego wykorzystaniem.



Rysunek 186. Wynik weryfikacji oryginalności pierwszych wersów *Księgi Rodzaju* w narzędziu AI Detector

W sierpniu 2024 roku na stronie The Verge ukazał się artykuł[133] wskazujący niebezpieczeństwa związane z rozwojem narzędzi AI służących do poprawiania zdjęć w smartfonach. Opisane w nim narzędzie Reimagine, dostępne na telefonach Google, pozwalało autorom nie tylko na poprawę nieudanego ujęcia (co jest główną funkcjonalnością, wskazywaną w reklamach tego typu aplikacji), ale także **na dodanie na zdjęciach wykonanych w różnych miejscach bardzo realistycznie wyglądających elementów**. Artefakty te zmieniały kontekst zdjęć, tworząc ze zwykłych ujęć ulic i krajobrazów niepokojące sceny wypadków i katastrof, łącznie z ciałami ich ofiar. Ten przykład stał się ostrzeżeniem przed łatwo dostępnym sposobem tworzenia bardzo realistycznych fotografii, służących do manipulacji czy szerzenia dezinformacji. Siłą tego typu techniki manipulacji jest fakt wykorzystania zdjęć przedstawiających realne ujęcia konkretnych miejsc i wydarzeń, co sprawia, że uwierzenie w zmodyfikowaną treść jest o wiele bardziej prawdopodobne. Narzędzie nie było wyposażone w żadne funkcje „bronienia się" przed promptami użytkownika, który zlecał dodawanie elementów wypadków, zwłok i innych elementów wywołujących silne emocje albo wprowadzających w błąd poprzez fałszowanie rzeczywistości.

Zmanipulowane przez narzędzia AI zdjęcia i opisy pojawiają się także coraz częściej w internetowych ogłoszeniach sprzedaży przeróżnych towarów. Aby temu przeciwdziałać, dziennikarka Bellingcat, Kolina Koltai, we współpracy z Evident stworzyła poradnik[134] dotyczący rozpoznawania ogłoszeń, przy tworzeniu których wykorzystana została sztuczna inteligencja.

Warto przeczytać cały ten artykuł, a tu pozwolę sobie przytoczyć jedynie postawione w nim pytania, które pomogą rozpoznać tego typu ogłoszenia:

1. Czy obraz przedmiotu ma w ogóle sens?
2. Czy produkt pokazany jest z wielu ujęć i czy na każdym ujęciu wygląda na ten sam obiekt?
3. Czy w opisie znajduje się informacja bądź inne wskazówki, że obrazy są generowane przez AI?
4. Czy w recenzjach jest informacja o faktycznym wyglądzie produktu?
5. Czy taka oferta nie wydaje się zbyt piękna, aby była prawdziwa?
6. Kto wystawia dany produkt (może też ma zdjęcie wygenerowane przez AI)?

We wskazanym poradniku zamieszczone są także zdjęcia przykładowych produktów, po obejrzeniu których łatwiej będzie uświadomić sobie szczegóły, na które warto zwrócić uwagę podczas analizy ofert sprzedaży *online*.

„Atak klonów", czyli AI w mediach społecznościowych

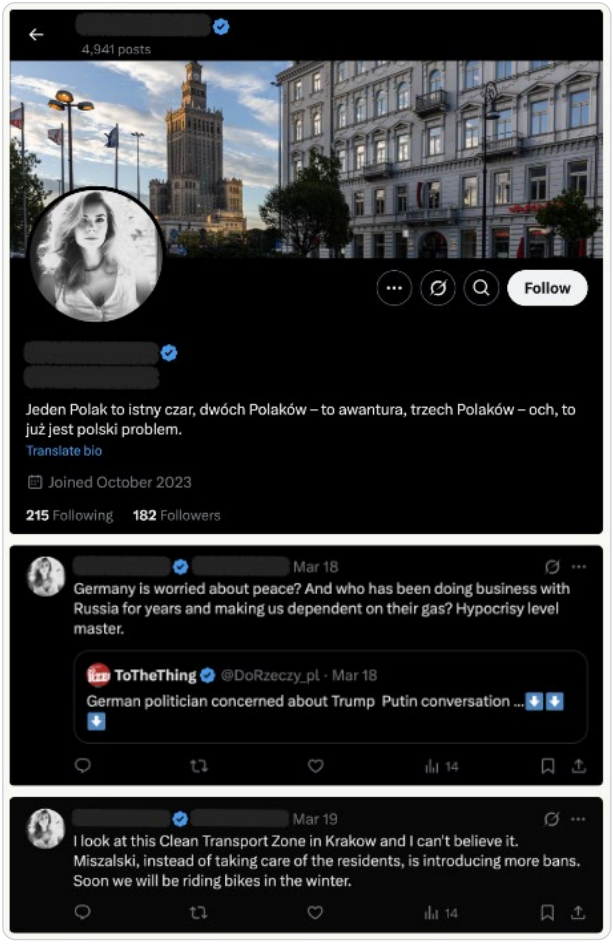
Modele językowe, zaprojektowane po to, aby pomagać ludziom w pracy, dobrze wykonują powierzone im zadania. Z tym jednak zastrzeżeniem, że wśród wspomnianych „ludzi", są także przestępcy i obce służby.

Firma Anthropic, twórca modelu Claude, w swoim raporcie z kwietnia 2025 roku wskazuje, że jej produkt został m.in. wykorzystany do orkiestracji operacji typu *influence-as-a-service* (co można przetłumaczyć jako „wpływ społeczny jako usługa"). Sieć ponad stu fałszywych kont na Facebooku i w serwisie X była kontrolowana z wykorzystaniem modelu Claude w celu szerzenia treści politycznych. Konta te weszły w interakcję z ponad 10 tysiącami innych kont. Ich celem było wspieranie interesów Europy, Iranu, Zjednoczonych Emiratów Arabskich oraz Kenii lub działanie na ich niekorzyść.

Fałszywe konta zostały „zaprogramowane" bardziej na utrzymanie kontaktu z użytkownikami platform społecznościowych niż na zdobycie popularności. Model w tym przypadku został użyty do podejmowania decyzji dotyczących lajkowania, udostępniania, komentowania lub ignorowania postów innych użytkowników, w zależności od zleconego celu i narracji, a także do oceny, czy dany profil powinien wejść w interakcję w konkretnym wątku, oraz do generowania stylu wypowiedzi odpowiadającego profilowi danej „kukiełki" (ang. *sock puppets*).

Co ciekawe, boty zostały skonfigurowane w taki sposób, że jeśli ktoś próbowałby insynuować, że kontrolowane w ramach operacji konta są botami, lub gdyby starał się udowodnić to poprzez prompty, skłaniające je m.in. do

napisania wiersza, miały one odpowiadać na to humorem i sarkazmem*. Oprócz tworzenia wypowiedzi tekstowych model był wykorzystywany również do tworzenia promptów do generowania obrazów za pomocą dwóch innych narzędzi i do oceny, czy są one zgodne z instrukcjami, czy też powinny zostać wygenerowane ponownie. Jedno z kont (rysunek 187) wskazanych w raporcie udawało profil społecznościowy Polki o poglądach prorosyjskich[135].



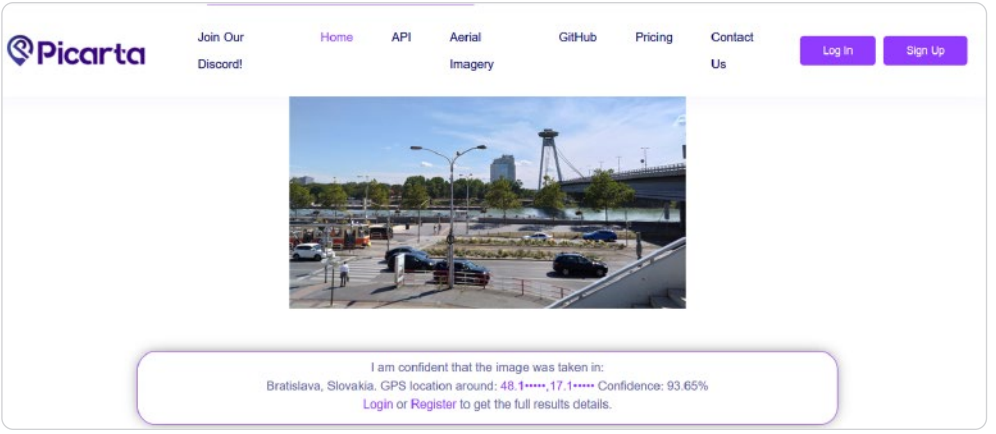
Rysunek 187. Przykład konta kontrolowanego przez model (wpisy zostały przetłumaczone na język angielski na potrzeby raportu firmy Anthropic)

* Tak, modele potrafią już używać sarkazmu. Fanom tego typu tonu wypowiedzi polecam **chatbota Monday**, stworzonego z wykorzystaniem ChatGPT, jednak ostrzegam, że określenie go „Garfieldem wśród modeli językowych" jest wyjątkowo trafne. W razie czego: ostrzegałem.

AI w służbie OSINT-u – geolokalizacja

W rozdziale *Czy geolokalizacja może zrobić się sama?* (s. 181) podałem przykłady narzędzi wspomagających znajdowanie miejsca, w którym zostało wykonane zdjęcie z wykorzystaniem narzędzi AI. Czy od czasu publikacji tego tekstu* coś się zmieniło?

Funkcjonalności tego typu występują również w wielu innych narzędziach. Obecnie możliwe jest przesłanie zdjęcia w ramach rozmowy chociażby z ChatGPT i zapytanie go, gdzie zostało ono wykonane. Narzędzie GeoSpy, opisywane w tamtym rozdziale, zyskało wprawdzie nowe funkcje wyszukiwania na podstawie zdjęć wnętrz, jednak stało się też dużo mniej dostępne. Na szczęście są jeszcze inne narzędzia, które dobrze sobie radzą z geolokalizacją, takie jak chociażby Picarta (rysunek 188)[136].



Rysunek 188. Wyszukiwanie lokalizacji wykonania zdjęcia przy użyciu narzędzia Picarta

Istnieje jeszcze inny sposób geolokalizacji, który być może nie jest tak oczywisty i uniwersalny, jak ten opisany powyżej, jednak warto pamiętać o jego istnieniu. Jest to **tekstowe wyszukiwanie miejsca**. Co zrobić bowiem w przypadku posiadania jedynie papierowej kopii zdjęcia lub dysponowania informacją o miejscu, opierając się jedynie na ludzkiej pamięci? Można poprosić chatbota o pomoc w identyfikacji miejsca na świecie na podstawie jego opisu.

Jest to dość trudne zadanie, ponieważ zachodzi konieczność przekazania posiadanych informacji w taki sposób, aby model miał szansę zidentyfikować daną lokalizację. Z własnego doświadczenia wiem, że czasami warto opisywać nawet z pozoru logiczne dla człowieka elementy, np.: „Tory tramwajowe biegną wzdłuż rzeki, prostopadle do mostu". Podczas rozmowy z drugim człowiekiem

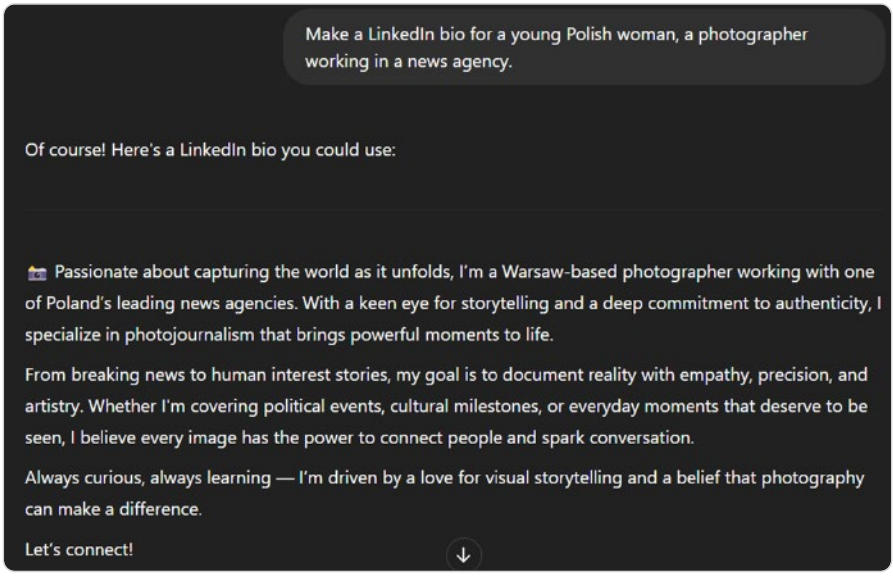
* Niniejsza edycja książki została zaktualizowana mi.in. o treść rozdziału *Więcej AI, OSINT wytrzyma (?)*; od czasu, gdy ukazało się wydanie I, minął ponad rok.

raczej nie jest konieczne takie doprecyzowanie sposobu, w jaki biegną tory (wzdłuż rzeki, są prostopadle do mostu rozpiętego nad nią itd.), jednak dla modeli niekiedy okazuje się to bardzo pomocną informacją.

Przygotowywanie środowiska pracy

Wykorzystanie narzędzi AI do przygotowania kont alternatywnych tożsamości w celu bezpiecznego prowadzenia śledztw OSINT-owych zostało opisane w rozdziale *Jak AI narzędzia zmieniają OSINT* (s. 166-173), jednak od momentu publikacji i tego tekstu działania w tym zakresie stały się dużo prostsze.

Obecnie nie trzeba już wymyślnych promptów, aby skłonić chatbota do wygenerowania danych nieistniejącej osoby, jej biografii (rysunek 189) czy historii nauki i pracy. Firmy rozluźniły nieco swoje zasady i obecnie można prosić wprost o stworzenie całego zestawu danych dla profilu konta OSINT-owego, należącego do fikcyjnej osoby. Niezależnie od tego, czy stoi za tym rozwój możliwości narzędzi, czy też prosta zasada zwiększania swoich możliwości, aby nie odstawać od konkurencji (nawet jeśli wyniki tego zadania dla chata nie są do końca „etyczne"), osoby zajmujące się OSINT-em mają teraz ułatwione zadanie przy tworzeniu kont „kukiełek".



Rysunek 189. Przykład wygenerowanego biogramu dla konta alternatywnej tożsamości z wykorzystaniem narzędzia ChatGPT

Podobnie rzecz ma się z generowaniem zdjęć do tego typu profili. Opcje narzędzi, które umożliwiają wykorzystanie jednego zdjęcia do tworzenia kolejnych, pozwalają sfabrykować całą historię fikcyjnej osoby w formie fotografii, co jeszcze lepiej ukrywa fakt, że ona nie istnieje.

Zagrożenia

Przed użyciem jakichkolwiek narzędzi (nie tylko tych wykorzystujących sztuczną inteligencję) należy zadać sobie pytanie, **w jaki sposób przetwarzane są wprowadzane dane** i **czy mogą one zostać** w ogóle przekazane **do podmiotów zewnętrznych**.

Niestety, od czasu do czasu pojawiają się informacje o wyciekach danych z modeli językowych, które mogą być spowodowane m.in. przez:

- możliwość ekstrakcji danych, na których trenowany był model (np. osobowych lub finansowych);
- brak kontroli nad wykorzystywanym modelem;
- ataki typu *prompt injection*, polegające na skonstruowaniu takiego promptu, który spowoduje zachowanie niepożądane przez jego twórców;
- możliwość utracenia dostępu do logów/wyników generowanych przez modele.

Podczas używania dużych modeli językowych w ramach OSINT-u warto pamiętać o dwóch zasadach:

1. Jeśli model trenowany był na wątpliwej jakości danych (np. zebranych z Internetu i nieprzefiltrowanych), to choćby został najlepiej napisany, będzie działał według zasady: *garbage in – garbage out* (czyli: słaba jakość danych wejściowych oznacza słabą jakość uzyskanych danych wyjściowych).
2. Jeśli operator nie ma świadomości dotyczącej działania danego modelu lub nie jest w stanie dobrze nim sterować, może się okazać, że nawet dysponując bardzo dobrymi danymi jako danymi wejściowymi, otrzyma wyniki o bardzo złej jakości.

Przykładem sytuacji, w której zmiana systemu promptu (czyli podstawowej instrukcji dla określenia m.in. sposobu zachowania i reagowania dla danego modelu) może wpłynąć na generowane przez niego treści, jest chociażby afera z pierwszych dni lipca 2025 roku. Wtedy to, po „usprawnieniu" Groka, czyli chatbota firmy xAI Elona Muska, polskojęzyczną część platformy X zaczęły zalewać jego odpowiedzi pełne wulgaryzmów i obelg, kierowanych głównie pod adresem krajowych polityków. Co prawda twórcy Groka oświadczyli, że został on jedynie przestawiony na tryb nieco mniej powściągliwego języka, aby lepiej wskazywać brutalną prawdę i unikać politycznej poprawności. Wydaje się wszakże, że wynikiem niesubordynacji narzędzia była jedynie jeszcze większa fala obraźliwych tekstów w sieci i wprowadzenie kolejnych emocji do i tak już mocno spolaryzowanych nastrojów społecznych.

Jeszcze rozleglejsze zagrożenia dla OSINT-u w zakresie korzystania z narzędzi AI opisał Nico Dekens (znany w sieci jako Dutch OSINT Guy) w swoim

wpisie *The Slow Collapse of Critical Thinking in OSINT due to AI*[137], opublikowanym w kwietniu 2025 roku na jego osobistym blogu. Zauważył on, że wielu analityków bardzo chętnie sięgnęło po wspomagające ich pracę narzędzia AI, jednak powoli przesuwali oni ciężar pracy właśnie na nie. **Zaczynało się od zlecenia podsumowania tekstu i jego tłumaczenia, a kończyło się na przygotowywaniu raportów przez asystentów AI, co w efekcie może prowadzić do powolnej utraty krytycznego myślenia wśród analityków.**

To właśnie sposób, w jaki działają dostępne modele językowe – dające szybkie, jasne i pewne odpowiedzi – wywołuje w operatorze mylne przeświadczenie, że otrzymana odpowiedź musi być prawdziwa. Zachęcam do przeczytania całego wpisu na blogu Nico. Pozwala on lepiej zrozumieć, co może się stać, jeśli analitycy zaczną zbytnio ufać osądom generowanym przez narzędzie wyłącznie pomocnicze, a nie przez człowieka, doświadczonego i świadomego istnienia pewnych pułapek umysłowych. W pierwszej chwili może wydawać się, że tekst jest zbyt fatalistyczny, jednak przez przerysowanie niektórych zagrożeń stanowi on dobre ostrzeżenie przed ślepym zaufaniem, pokładanym w „inteligentnych" asystentach. Narzędzia te obecnie nie są bowiem w stanie wychwycić i wyciągnąć wniosków z takich obszarów, jak źródła niemainstreamowe, kalki językowe czy słownictwo i różne style językowe. **Pewność siebie emanująca z odpowiedzi chatbotów powoduje mniejszą chęć weryfikacji źródeł i uruchomienia krytycznego myślenia.**

Czy zatem wszystko jest stracone i analitycy powinni przestać korzystać z tego typu asystentów? Absolutnie nie.

Zamiast tego Nico Dekens sugeruje podjęcie następujących kroków:

- testowanie modeli dla różnych promptów, nawet zawierających ewidentnie nieprawdziwe informacje, i obserwacja ich zachowań;
- porównywanie odpowiedzi z różnych modeli;
- porównanie wyników z ręcznym wyszukiwaniem;
- proszenie o kontrargumenty.

Warto także pamiętać o najważniejszej moim zdaniem zasadzie: **traktowaniu AI jak młodszego analityka**.

Podsumowanie

Ogromny skok technologiczny w obszarze sztucznej inteligencji, który dokonał się na przestrzeni ostatnich dwóch–trzech lat, a ponadto udostępnienie w Internecie całej gamy narzędzi wykorzystujących nowe możliwości, zmienił oblicze OSINT-u. Nie da się ukryć, że narzędzia tradycyjne zostały nieco „odsunięte w kąt", a w ich miejsce pojawili się asystenci AI, którzy są w stanie wygenerować dane tekstowe lub graficzne, przetwarzać je, a także w bardzo szybki sposób zebrać i porównać informacje pochodzące z wielu źródeł.

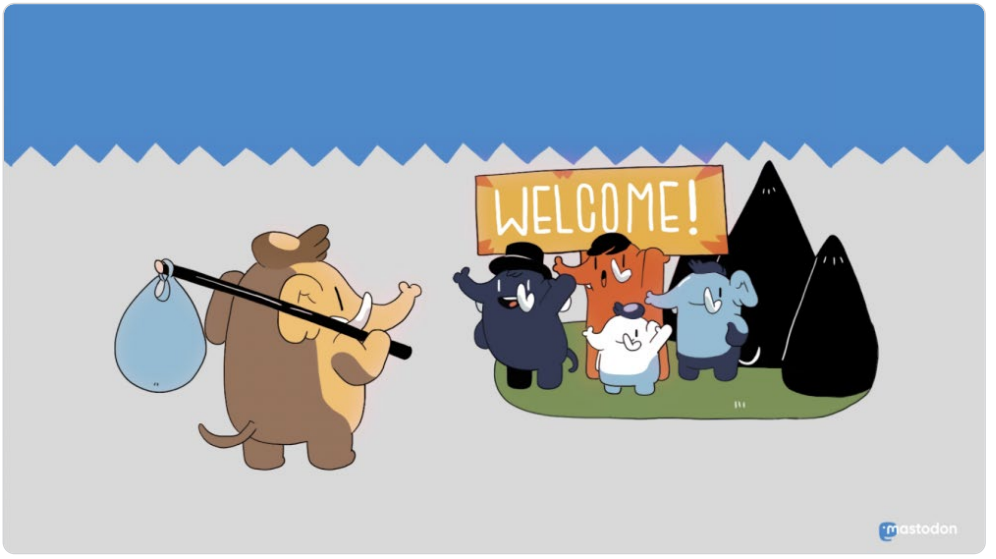
Współczesne narzędzia AI to z jednej strony ogromne ułatwienie dla każdego, nawet niedoświadczonego OSINT-owca, ale z drugiej – wielkie zagrożenie. Dla niewprawionego użytkownika mogą stać się źródłem mylnych osądów i bezpodstawnych oskarżeń. Jak każda potężna broń, także ta wymaga nauki i rozwagi. W rękach osób świadomych ich możliwości, ale przede wszystkim ich ograniczeń, narzędzia potocznie określane mianem AI będą stanowić o sile nowoczesnego OSINT-u.

Nadal jednak najdoskonalszym narzędziem analizy rzeczywistości niech pozostanie nasza własna, prawdziwie ludzka inteligencja.

CZĘŚĆ III: OSINT *HINTS*

R31 MASTODON – OSINT-OWA ANALIZA CORAZ POPULARNIEJSZEJ ALTERNATYWY WOBEC TWITTERA/X

Od kiedy Twitter (obecnie X) został kupiony i przejęty przez Elona Muska*, coraz więcej osób wieszczy jego szybki koniec albo co najmniej ogromną utratę wartości, zaufania i interesujących informacji. Niezależnie od tego, czy jest to prawdą czy nie, na sile przybrała tendencja do zakładania bądź odświeżania kont w alternatywnych mediach społecznościowych. Jednym z nich jest Mastodon – platforma na pierwszy rzut oka bardzo przypominająca Twittera/X. Warto więc na nią zwrócić uwagę z OSINT-owego punktu widzenia (rysunek 190).



Rysunek 190. Czym jest Mastodon?

* Kwiecień–październik 2022 roku.

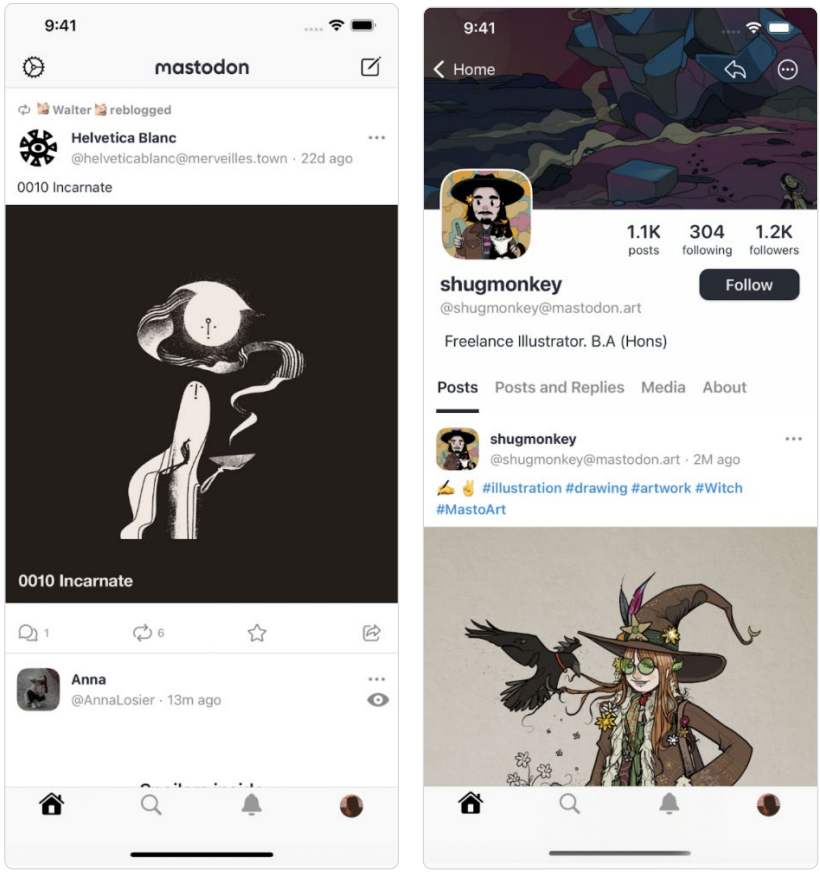
Witaj w fediwersum

Mastodon to sieć rozproszonych serwerów (tzw. instancji), które razem tworzą wspólną platformę, przypominającą nieco wczesnego Twittera. Każdy może uruchomić swój węzeł z oprogramowaniem Mastodon i dołączyć do sieci, dzięki czemu możliwe jest komunikowanie się pomiędzy serwerami, co jest podstawą tzw. fediwersum (ang. *fediverse* – od złożenia słów *federation* i *universe*).

Właśnie idea zdecentralizowanej sieci społecznościowej może być nieco myląca dla osób, które przyzwyczajone są do takich serwisów, jak: Twitter (obecnie X), Facebook czy Instagram. Najprościej rzecz ujmując, można stwierdzić, że sieć instancji Mastodon można przyrównać do serwerów e-mailowych, które – pomimo różnych domen i właścicieli – stanowią sieć umożliwiającą komunikację pomiędzy nimi.

Główną instancją jest mastodon.social, na której aktualnie nie można się już rejestrować z powodu wyczerpania zasobów jego serwerów. Twórcy udostępnili jednak kolejny serwer – mastodon.online, który obecnie umożliwia natychmiastowe założenie i aktywowanie konta. A nie jest to takie oczywiste, jak mogłoby się wydawać, gdyż niektóre instancje umożliwiają zakładanie kont, jednak proces aktywacji wykonywany jest ręcznie przez administratorów. Obecnie istnieją jeszcze dość duże wątpliwości co do idei działania samej platformy, gdyż zgodnie z zasadami tam panującymi wspomnienie kogoś w prywatnej rozmowie dołącza tę osobę do czatu, a wiadomości są przechowywane bez jakiegokolwiek szyfrowania, co pozwala administratorom serwera na łatwy dostęp do nich[138].

Zagłębiając się nieco bardziej w portal Mastodon, należy przyswoić nieco zmienioną nomenklaturę w stosunku do Twittera/X. Wpisy określane są mianem ***toot***, zamiast retweetowania jest podbijanie (ang. ***boost***), a polubienie (ikona z serduszkiem na Twitterze/X) zostało zastąpione dodaniem do ulubionych i **ikoną gwiazdki** (rysunek 191).



Rysunek 191. Interfejs Mastodona (po lewej) na pierwszy rzut oka bardzo przypomina Twittera/X (po prawej)

OSINT w Mastodonie

Warto jednak spojrzeć na ten portal nie od strony funkcjonalnej, a w kontekście możliwości analizy w ramach OSINT-u. Mnogość serwerów oznacza, że równie liczne mogą być konta użytkowników o tej samej nazwie, podobnie jak możliwe są takie same loginy w poczcie np. na Gmailu i Outlooku. Jeśli więc zależy nam na konkretnej nazwie, trzeba poszukać serwera, na którym dany login nie będzie jeszcze zajęty. Jako ciekawostkę można dodać, że swój własny serwer w Mastodonie ma np. niemiecka administracja rządowa.

Z punktu widzenia OSINT-u jest to pewne utrudnienie, gdyż w celu odszukania osoby o danym pseudonimie należy przeanalizować wszystkie serwery. Pomocą w tym zakresie może być narzędzie autorstwa OSINT Tactical – Masto (rysunek 192) pomagające wyszukać użytkownika o danym loginie na różnych instancjach lepiej, niż robi to wyszukiwarka wbudowana w Mastodona.

Rysunek 192. Przykładowe wyszukiwanie w narzędziu Masto

Jedną z instancji w chwili pisania tego tekstu można także przeszukiwać za pomocą narzędzia whatsmyname.app, służącego do znajdowania profili w różnych portalach społecznościowych. Można oczywiście też użyć wyszukiwarki, poszukując adresów na różnych serwerach Mastodon ze znakiem „@", który jest zawsze umieszczany w adresie profilu przed pseudonimem, np. *https://mastodon.online/@SEINT*.

W trakcie prac nad tym rozdziałem powstało jeszcze jedno narzędzie – imagstodon, które stworzyłem, aby móc wyszukiwać obrazki profilowe za pomocą zapytań do różnych instancji Mastodona.

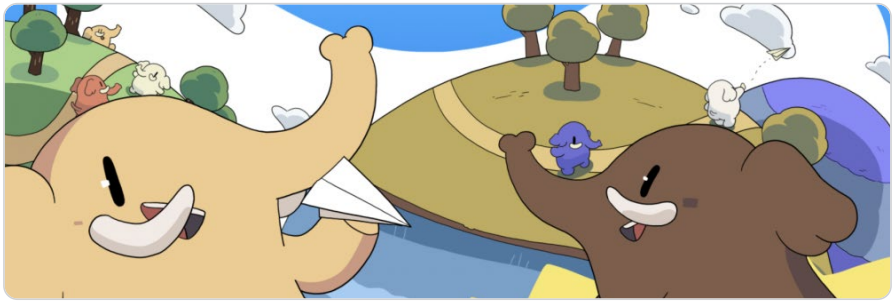
Należy pamiętać, że konto o takim samym loginie, ale na różnych instancjach wcale nie musi należeć do tej samej osoby. Może wystąpić także sytuacja, że pomimo wizualnej zgodności kont pomiędzy instancjami jedno lub więcej z nich będzie podszywało się pod prawdziwego właściciela. Administratorzy starają się jednak wyłapywać tego typu sytuacje, chociaż czasami są w tym nieco nadgorliwi[139].

Plusem zamieszania z Twitterem/X i przechodzenia wielu użytkowników do innych serwisów społecznościowych jest to, że bardzo często informują oni o swoich pseudonimach, pod którymi występują w innych portalach, co w przypadku OSINT-u wykonywanego w stosunku do danej osoby będzie dla

śledczych niezwykle pomocne. Nie zawsze oczywiście takie zachowanie musi być złe – w bardzo wielu przypadkach informacje te przydają się osobom śledzącym dany profil, które mogą go znaleźć w przypadku nagłego krachu np. X.

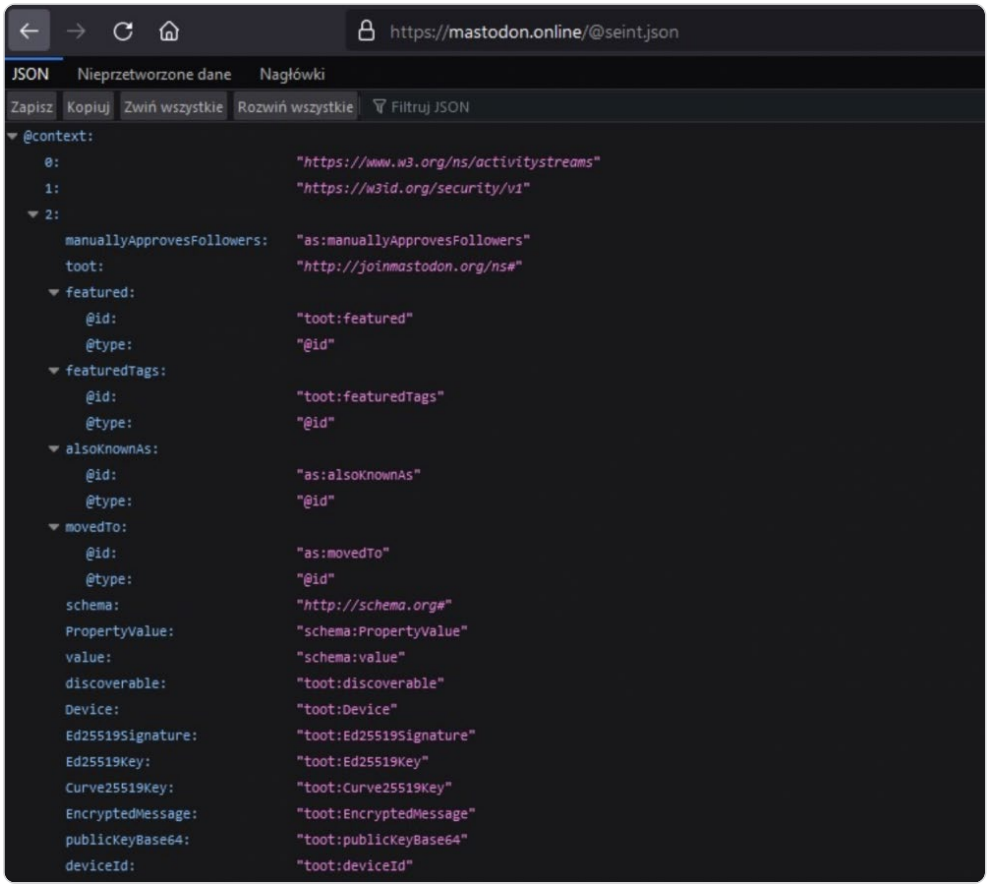
Jednym z trików OSINT-owych, który odkryłem niedawno przez przypadek, jest możliwość obejrzenia obrazka będącego grafiką tła danego profilu na Mastodonie w formie nieprzyciętej. Normalnie na stronie profilu wyświetlany jest obraz o rozmiarze 1500 × 500 pikseli. Nie jest on jednak przycinany podczas wgrywania, a jedynie wyświetlany w części. Wystarczy więc z menu pod prawym klawiszem myszy na obrazku tła profilu wybrać opcję POKAŻ OBRAZ W NOWEJ KARCIE, aby obejrzeć go w całości. Może się okazać, że taki obraz w domyślnie niewidocznych obszarach zawiera jakieś interesujące informacje, które mogą się przydać w ramach śledztwa OSINT-owego (rysunki 193 a i b).

Rysunek 193 a. Sposób wyświetlenia obrazka tła



Rysunek 193 b. Pełny obrazek

Inną ciekawą techniką podzielił się jakiś czas temu Sector035 na Twitterze[140], wskazując, że do adresu profilu na Mastodonie wystarczy dodać końcówkę `.json`, aby otrzymać informacje o danym użytkowniku w formie czytelnie sformatowanego (tu niespodzianka) pliku JSON, co może okazać się ułatwieniem w przypadku automatyzacji poszukiwań (rysunek 194). Taki plik może zresztą zawierać więcej informacji niż te wyświetlane na stronie danego profilu. Ten sam trik działa w wypadku rozszerzenia `.rss`.



Rysunek 194. Widok profilu Mastodon w formatowaniu JSON

Podsumowanie i rady

Mastodon na pewno ma obecnie swoje pięć minut. Niezależnie od tego, czy stanie się konkurentem lub nawet następcą Twittera/X, czy też pozostanie w jego cieniu, warto mieć świadomość, że jest to kolejne miejsce, które należy sprawdzić, prowadząc OSINT-owe poszukiwania.

R32 PRZEKIEROWANIA Z KRÓTKICH LINKÓW I JAK JE ZNALEŹĆ

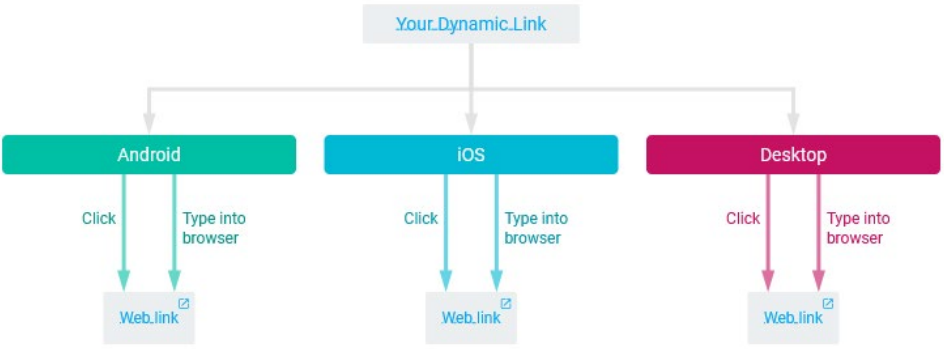
W wielu miejscach w Internecie stosowane są wszelkiego rodzaju skracacze linków – jedne po to, aby zaoszczędzić na liczbie znaków w miejscach, gdzie do dyspozycji jest tylko ich ograniczona liczba, inne w celu śledzenia przejść pod dany adres albo ułatwienia przepisywania lub zapamiętywania ich, a jeszcze inne – w atakach phishingowych, by ukryć docelową domenę, która wzbudziłaby mniejsze zaufanie niż krótki link ze znanego nam serwisu. Co jednak zrobić, aby poznać docelowy adres, pod który operator serwisu skracającego linki będzie chciał nas przenieść, bez przechodzenia tam? Jest na to kilka sposobów.

Modyfikacje linków przekierowujących

Pierwszą techniką jest dodanie konkretnego elementu, specyficznego dla danego serwisu skracającego linki, który pozwoli na wyświetlenie docelowego adresu URL bez przechodzenia do niego.

Google – *goo.gl*

Google, co prawda, wycofało się z tego projektu w 2019 roku (rysunek 195), ale wcześniej utworzone linki nadal działają. Żeby zweryfikować adres docelowy, należy do linka dodać `?d=1`, co wyświetli schemat blokowy przydatny przy debugowaniu linków dynamicznych, ale jednocześnie pokaże także docelowy link. Przykład: *https://goo.gl/l6MS?d=1*.



Rysunek 195. Google – *goo.gl*

Bitly – *bit.ly*

Bitly oferuje możliwość podejrzenia strony z informacją o adresie docelowym po dodaniu znaku plus (+) na końcu krótkiego linku. Przykład: *https://bitly.com/Wn2Xdz+*.

TinyURL

Ten serwis informuje od razu po stworzeniu skróconego linku o możliwości podejrzenia docelowego adresu poprzez dodanie prefiksu (subdomeny) *preview* przed adresem linku. Przykład: *https://preview.tinyurl.com/y53y8oq6* (rysunek 196).

Rysunek 196. TinyURL

Serwis *is.gd*

Tym razem, aby wyświetlić stronę pokazującą nam docelowy URL, należy do krótkiego linku dodać znak minus (-). Przykład: *https://is.gd/dKGELA-*.

Serwis *tiny.cc*

W wypadku tego serwisu konieczne jest z kolei dodanie po krótkim linku znaku równości (=). Przykład: *https://tiny.cc/9i3tvz=*.

Serwisy „wydłużające" linki

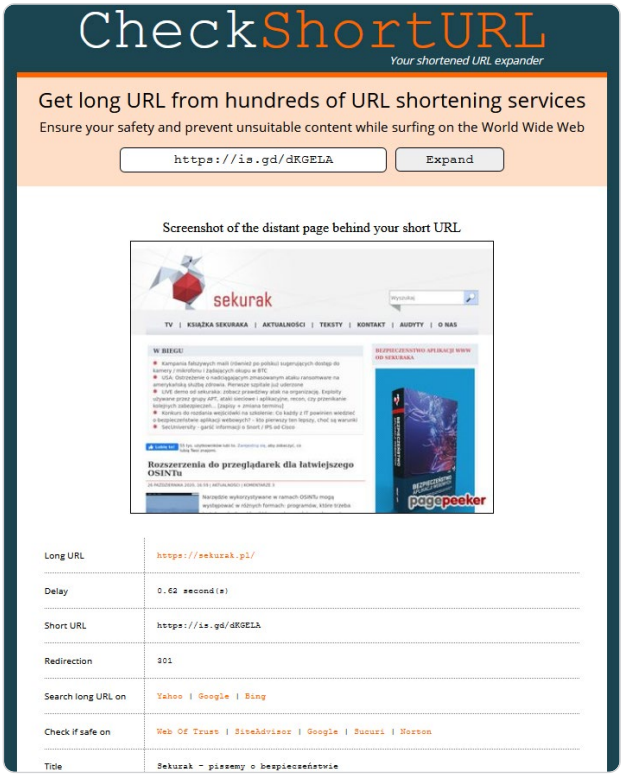
Kolejną techniką jest skorzystanie z narzędzi w sieci. Jest tam oczywiście całe mnóstwo serwisów rozwijających zarówno linki z powyższej listy, jak i wiele innych, np. t.co z Twittera/X czy fb.me z Facebooka. Kilka z popularniejszych stron to:

- Unshorten.It! (rysunek 197),
- GetLinkInfo (rysunek 198),
- Unshorten.me,
- ExpandURL,
- CheckShortURL (rysunek 199),
- URL X-ray.

Rysunek 197. Unshorten.It!

Rysunek 198. GetLinkInfo

Warto tutaj zaznaczyć, że Unshorten.it i CheckShortURL oprócz informacji o stronie docelowej oferują także jej podgląd oraz możliwość weryfikacji strony w Web of Trust. GetLinkInfo i ExpandURL podają za to liczbę przekierowań i ich adresy.



Rysunek 199. CheckShortURL

Rozszerzenia/dodatki do przeglądarek

Wśród rozszerzeń do przeglądarek Firefox, Edge i Opera nie udało mi się znaleźć żadnego dobrze działającego analizatora krótkich linków. Jeśli chodzi o Chrome, to sytuacja wygląda trochę lepiej – działa m.in. Link Unshortener, który po prostu pokazuje docelowy adres po kliknięciu w krótki link.

Zestawienie modyfikatorów adresów URL dla różnych serwisów

W ramach badań serwisów do skracania linków zidentyfikowałem kilkadziesiąt z tych, które udostępniają funkcjonalność informowania użytkownika o adresie docelowym bez przenoszenia go tam, po dodaniu odpowiedniego modyfikatora do linku. Zestawienie serwisów i dostępnych modyfikatorów umieściłem na GitHubie jako *Short links verification cheatsheet*[141].

Podsumowanie i rady

Obecnie stosowanie linków w formie skróconej używane jest w wielu informacjach, ofertach czy reklamach. Przed kliknięciem w nie warto zastanowić się, czy na pewno można ufać dostawcy tych informacji na tyle, żeby bez zastanowienia kliknąć w link i dać się przenieść do nieznanej nam (przed

kliknięciem) strony. Linki takie często pojawiają się w wiadomościach przesyłanych nam na telefony komórkowe, np. w SMS-ach. Jeśli istnieje jakakolwiek wątpliwość, warto taki link najpierw skopiować i dowiedzieć się, gdzie przekierowuje po kliknięciu.

R33 SKRYPTOZAKŁADKI – JAK Z ZAKŁADKI W PRZEGLĄDARCE ZROBIĆ NARZĘDZIE DO OSINT-U

Najprawdopodobniej wszyscy znają mechanizm działania zakładek w przeglądarkach – chcąc zachować odnośnik do jakiejś strony, należy go zapisać jako zakładkę i w każdej chwili można do tej strony przejść za jej pomocą. Czy można jednak zamiast linku rozpoczynającego się np. od `http(s)` lub `ftp(s)` wpisać tam coś innego? Otóż tak – można rozpocząć od `javascript:`, co sprawi, że powstanie właśnie skryptozakładka. Temat znany jest nie od dziś, ale pomimo swojej historii nie należy do zakresu „wiedzy powszechnej" o działaniu przeglądarek.

Skryptozakładki (ang. *bookmarklets*) – osobiście wolę słowo *bookmarklet*, bo „skryptozakładka" brzmi trochę jak „hydrozagadka" – wywołują po prostu funkcję w JavaScript, mogą więc przykładowo modyfikować stronę wyświetloną lokalnie, wywoływać polecenia, które posłużą do analizy strony, lub generować przekierowania na podstawie określonych danych.

Analiza skryptów

Należy jednak podkreślić, że wszelkie skrypty uruchamiane lokalnie w przeglądarce powinny być gruntownie przeanalizowane, niezależnie od tego, czy są pobrane czy przepisane. Innymi słowy – należy być zawsze pewnym, że skrypt robi tylko i wyłącznie to, co powinien. Wykonywanie skryptów, odnośnie do których nie ma pewności co do ich działania, może być równoznaczne z XSS-em, który będzie miał pełny dostęp do danych ze strony i będzie mógł je wysyłać do wszelkiej maści przestępców.

Zacznijmy jednak od podstawowego, bazowego wyglądu skryptozakładki:

```
javascript:(function(){
// tutaj wpisujemy kod w JavaScript
})();
```

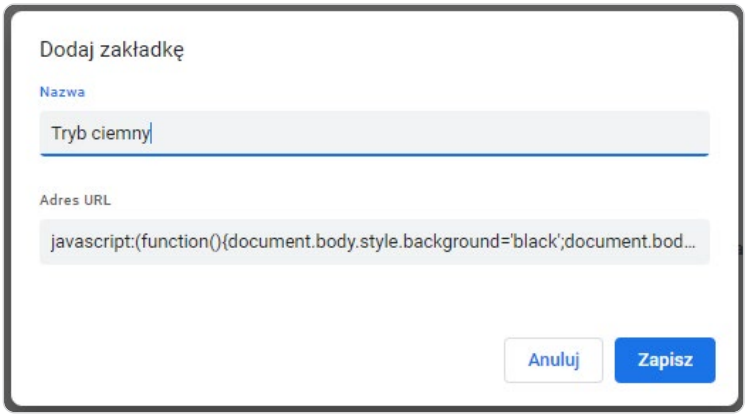
Pomiędzy klamrami muszą znaleźć się polecenia zapisane w języku JavaScript. Można je wstępnie wpisywać linia pod linią, jednak docelowo i tak cały kod będzie zapisany w jednej linii, co nie stanowi problemu dla przeglądarki. Polecenia będą bowiem rozdzielone średnikami, enterów używa się tylko dla lepszej wizualizacji tworzonego kodu.

Tworzenie narzędzi OSINT-owych

Chcąc zmodyfikować wyświetlaną stronę (bo modyfikacje będą miały wpływ jedynie na już pobraną stronę, nie modyfikujemy nic w serwisie hostującym), odwołujemy się do elementów DOM (Document Object Model). Można w ten sposób stworzyć np. narzędzie do przełączania aktualnie oglądanej strony w tryb ciemny (rysunek 200, listing 2).

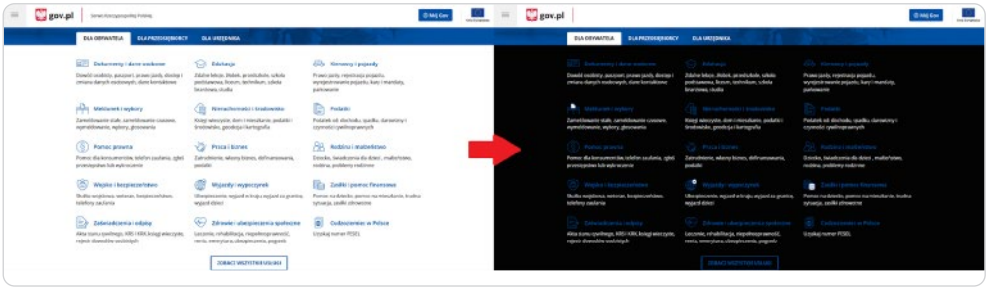
Listing 2. Skryptozakładka powodująca zmianę trybu wyświetlania strony

```
javascript:(function(){
    document.body.style.background='black';
    document.body.style.color='white';
 })();
```



Rysunek 200. Kod skryptozakładki wpisany w polu ADRES URL zakładki w Chrome

W powyższym skrypcie najpierw następuje odwołanie do treści strony i zmiana jej stylu (a konkretnie: koloru) tła na czarny (rysunek 201). Następnie cały tekst na stronie zmieni się na biały. Ten trik oczywiście zadziała tylko na stronach niezawierających w tle obrazków, które mogłyby się nałożyć na czarne tło. Kolory można dobrać dowolnie, nie tylko z zakresu kolorów nazwanych w HTML, ale także podając ich składowe w dowolnej akceptowanej przez HTML postaci, np. `#0000FF` będzie odpowiednikiem niebieskiego (`#RRGGBB`, gdzie `RR` – czerwony, `GG` – zielony, `BB` – niebieski, każde podawane w zakresie `00-FF`, szesnastkowo). Może się oczywiście okazać, że na stronach, które chcemy „przełączać", stosowane są elementy, na które skrypt nie będzie działał. Należy wtedy zajrzeć do źródła strony i sprawdzić, w jakich fragmentach strony są one wyświetlane – i te konkretne elementy zmieniać.



Rysunek 201. Portal *gov.pl* w wersji domyślnej i po zastosowaniu narzędzia zmiany kolorów

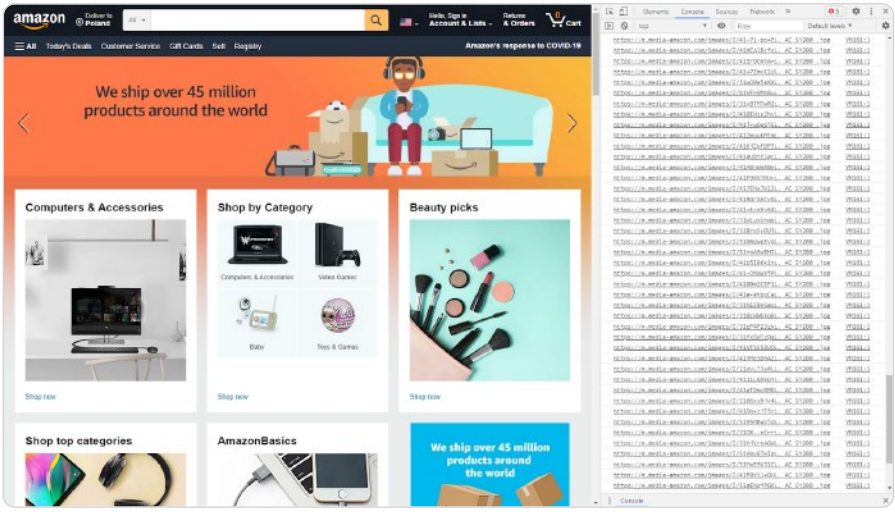
A jeśli chcemy stworzyć narzędzie nieco bardziej skomplikowane niż „zmieniacz kolorów"?

Ciekawe przykłady wykorzystania skryptozakładek do OSINT-u zaproponował na SANS Summit 2021 Chris Poulter z australijskiego OSINT Combine. Jedno z zaoferowanych przez niego zastosowań posłużyć może do listowania URL-i wszystkich obrazków na danej stronie. Kod wykonujący to zadanie przedstawiony jest na listingu 3.

Listing 3. Skryptozakładka listująca wszystkie obrazki z danej strony

```
javascript:(function(){
    var items = document.getElementsByTagName("img");
 for ( i = 0; i < items.length ; i++) {
    console.log(items[i].src);
 }
 })();
```

W powyższym przykładzie zapisujemy najpierw do zmiennej element typu `img`, czyli obrazki. Następnie, iterując po wszystkich znalezionych elementach, wpisujemy do konsoli zawartości pola `src`, czyli, najprościej mówiąc, linki do tych obrazków. Żeby zobaczyć, co pojawiło się w konsoli (rysunek 202), musimy zajrzeć do narzędzi deweloperskich – bezpośredni skrót do konsoli w Chrome: COMMAND+OPTION+J (Mac) / CONTROL+SHIFT+J (Windows/Linux), a w Firefoksie: COMMAND+OPTION+K (Mac) / CONTROL+SHIFT+K (Windows/Linux).



Rysunek 202. Widok konsoli po wykonaniu skryptu wyszukującego obrazki na otwartej stronie (Amazon)

Jeśli strona zawiera nie tylko obrazki statyczne, ale także wczytywane przez CSS-y, można do zmiennej `items` wczytać wartości w sposób zaprezentowany na listingu 4 i następnie, iterując, wyszukiwać w otrzymanych wynikach pola `name`, a nie `src`.

Listing 4. Kod skryptozakładki wyszukującej obrazki wczytywane przez CSS

```
javascript:(function(){
 var items = performance.getEntriesByType('resource'). ⤶
filter(resource=>resource.initiatorType == 'img');
 for ( i = 0; i < items.length ; i++) {
    console.log(items[i].name);
 }
 })();
```

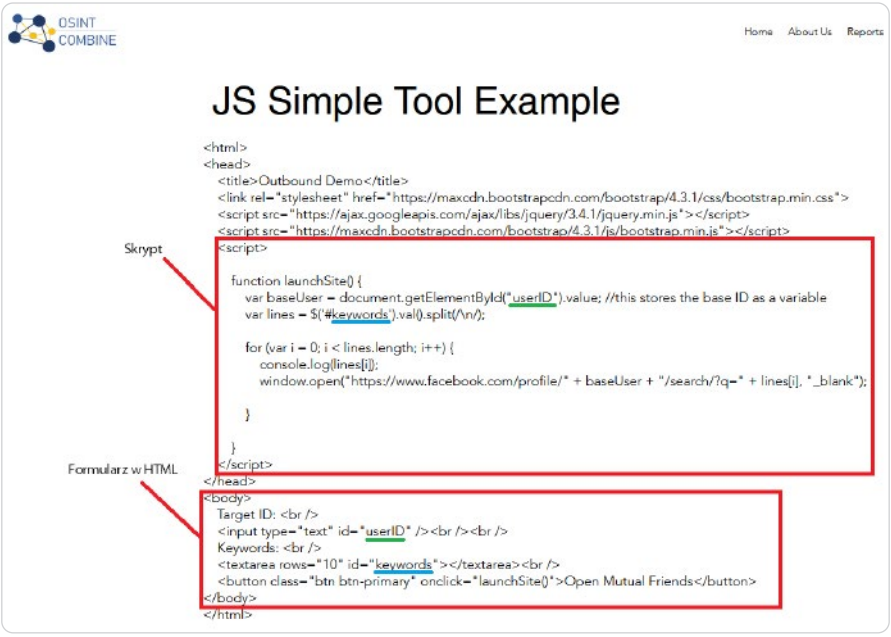
Oczywiście można tworzyć takie narzędzia, jakie będą potrzebne, ograniczeniem są jedynie możliwości języka JavaScript. Chcąc automatycznie wyszukiwać zaznaczony tekst w wielu serwisach, można np. posłużyć się kodem dla skryptozakładki zaprezentowanym na listingu 5.

Listing 5. Skryptozakładka wyszukująca zaznaczony tekst w wielu serwisach *online*

```
javascript:(function(){
    var szu = window.getSelection().toString();
    var google = "https://www.google.pl/search?q=";
    var bing = "https://www.bing.com/search?q=";
```

```
    var duck = "https://duckduckgo.com/?q=";
    window.open(google.concat(szu),'_blank');
    window.open(bing.concat(szu),'_blank');
    window.open(duck.concat(szu),'_blank');
})();
```

To jednak jeszcze nie wszystkie sposoby na tworzenie nowych narzędzi OSINT-owych. Idąc krok dalej, warto zerknąć na *URL Launcher* od OSINT Combine (rysunek 203[142]). To prosta strona w HTML + JavaScript, w której najpierw należy wpisać do formularza ID użytkownika Facebooka oraz słowa kluczowe, jakie powinny zostać wyszukane w jego profilu. Pozwala to znacznie skrócić proces przeczesywania profili w poszukiwaniu informacji, które mogą się tam znaleźć.



Rysunek 203. Przykład kodu strony z narzędzia od OSINT Combine do wyszukiwania fraz na profilu facebookowym – zaznaczenia i opisy własne

Ten skrypt, po niewielkiej modyfikacji linku facebookowego, można wykorzystać do przeszukiwania np. wspólnych znajomych badanej osoby (`userID`) i dowolnej liczby innych osób, których identyfikatory można wpisać w drugim polu (`keywords`). Wystarczy zamienić tylko kod otwierający nowe zakładki na: `window.open("www.facebook.com/browse/mutual_friends/?uid="+baseUser+"&node="+lines[i], "_blank");`

Podsumowanie i rady

Zaprezentowałem tutaj jeden sposób pozwalający na dowolne dostosowywanie skryptów do aktualnych potrzeb. Możliwe jest automatyczne wyszukiwanie informacji na zadany temat w określonych serwisach informacyjnych, znajdowanie kombinacji nazw użytkownika i wybranych domen w wyszukiwarkach, tworzenie adresów e-mailowych lub też pozyskiwanie ze stron pożądanych informacji i wyświetlanie ich w postaci wygodnej do późniejszej obróbki.

Za pomocą skryptozakładek można także wyciągać z kodu strony linki do zdjęć profilowych, materiałów wideo czy innych interesujących informacji. Przykłady kodu służącego do ekstrakcji informacji z różnych serwisów można znaleźć również na GitHubie u użytkownika Sinwindie, który w artykule *Make Your Own Custom OSINT Bookmarklets (p1)*[143] opisał m.in. sposoby na wyodrębnianie linków z kodu strony i prezentowanie ich następnie w przeglądarce.

R34 KOLEKCJONOWANIE DOWODÓW: RECON A ZRZUTY EKRANOWE STRON W SIECI

Popularne stwierdzenie „screenshot or it didn't happen" (czyli „pokaż mi zrzut ekranu albo to nie miało miejsca") staje się jeszcze bardziej adekwatne w momencie, kiedy zdamy sobie sprawę, że odwiedzana kiedyś strona już nie istnieje, w archiwum typu The Wayback Machine nie została zarchiwizowana, a my akurat zapomnieliśmy zrobić zrzuty ekranu lub już nie jesteśmy w stanie przypomnieć sobie, jak doszliśmy do aktualnie otwartej jednej z kilkudziesięciu zakładek w przeglądarce. Sam proces tworzenia zrzutów ekranu potrafi także zajmować dużo cennego czasu i uwagi. Dlaczego więc go nie zautomatyzować?

WMN_screenshooter

W rozdziale *Sherlock i doktor Whatsmyname – wyszukiwanie profili po nazwie użytkownika* (s. 50–52) pisałem o narzędziu, które służy do wyszukiwania profili o konkretnym loginie na ponad 280 serwisach: w mediach społecznościowych, na popularnych forach internetowych czy innych stronach – WhatsMyName (autorstwa WebBreachera). Jeśli ktoś chce dodatkowo mieć widoki wszystkich stron, na których znaleziono użytkownika o poszukiwanej nazwie, może skorzystać z bazującego na WhatsMyName skryptu autorstwa swedishmike'a – WMN_screenshooter (rysunek 204). Instalacja sprowadza się standardowo do pobrania repozytorium z serwisu GitHub i zainstalowania zależności. Dodatkowo należy wskazać bazę stron do przeszukiwania z narzędzia WhatsMyName (w pliku JSON), przy czym potrzebny jest nam tylko ten jeden plik, a nie całe narzędzie.

```
  $ python3 ./WMN_screenshooter.py -c /home/osint/WMN_screenshooter/web_accounts_list.json -u jankowalski -t 20
 *  Skipping Gab - Marked as not valid.
[+] Found user at https://www.eyeem.com/u/jankowalski
[+] Found user at https://audiojungle.net/user/jankowalski
[+] Found user at https://issuu.com/jankowalski
[+] Found user at https://fancy.com/jankowalski
[+] Found user at https://www.cnet.com/profiles/jankowalski/

Trying to capture screenshot(s) from the identified site(s) now.
The screenshots will be stored in /home/osint/WMN_screenshooter/2021-02-05_123718_jankowalski
Capturing: https://www.eyeem.com/u/jankowalski
Capturing: https://audiojungle.net/user/jankowalski
Capturing: https://issuu.com/jankowalski
Capturing: https://fancy.com/jankowalski
Capturing: https://www.cnet.com/profiles/jankowalski/
```

Rysunek 204. Efekt pracy narzędzia WMN_screenshooter

Po znalezieniu stron, na których istnieje konto poszukiwanego użytkownika, skrypt robi zrzuty ekranów i wrzuca je do katalogu dedykowanego danemu wyszukiwaniu.

Minusem tego rozwiązania jest jego niska stabilność, bo niestety w przypadku pewnej liczby przeszukiwanych serwisów pojawiają się błędy, które często uniemożliwiają przeprowadzenie pełnego skanowania. Ratunkiem w moim przypadku była jedynie ręczna modyfikacja pliku JSON i usuwanie wpisów powodujących błędne działanie.

EyeWitness

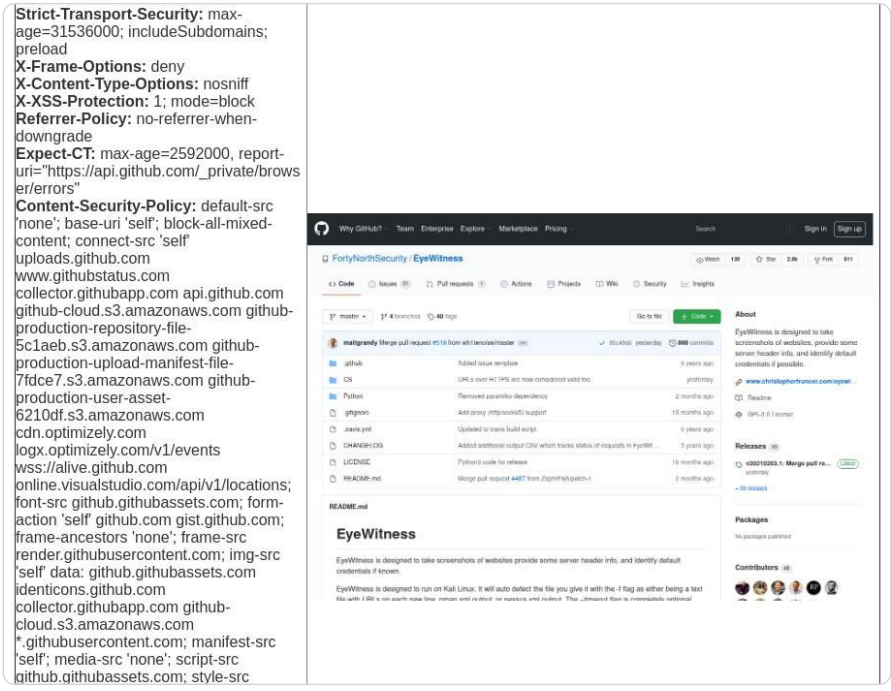
Drugim z narzędzi, które można „zaprzęgnąć” do robienia zrzutów ekranu podczas rekonesansu, jest EyeWitness (rysunek 205), przy czym jego możliwości wykraczają znacznie poza zrzuty ekranu. Zasilony danymi z pliku tekstowego z listą adresów (po jednym na linię) lub pliku XML wygenerowanego za pomocą narzędzia Nmap czy skanera podatności Nessus, wykonuje weryfikację możliwości połączenia, zrzuca aktualny wygląd strony i podstawowe informacje o hoście, przy czym bada nie tylko strony (http/https), ale i dostęp po RDP czy VNC (w tym drugim przypadku tylko w ustawieniu bez uwierzytelnienia).

```
################################################################################
#                                 EyeWitness                                   #
################################################################################
#           FortyNorth Security - https://www.fortynorthsecurity.com           #
################################################################################

Starting Web Requests (3 Hosts)
Attempting to screenshot https://github.com/FortyNorthSecurity/EyeWitness
Attempting to screenshot https://sekurak.pl
Attempting to screenshot https://securitum.com
Finished in 59.53115797042847 seconds

[*] Done! Report written in the /home/osint/screenshots folder!
Would you like to open the report now? [Y/n]
```

Rysunek 205. EyeWitness to przydatne narzędzie do wykonywania zrzutów ekranu podczas rekonesansu

Dodatkowo Eyewitness może wykonywać swoje zadania poprzez proxy, zmieniać rodzaj urządzenia/oprogramowania, które próbuje się łączyć (manipulacja nagłówkiem `User-Agent`), a także wykonywać próby logowania w celu wykrycia danych logowania. Należy również dodać, że narzędzie jest dostępne nie tylko dla systemów linuksowych (Kali/Debian 7+), ale także w wersji do samodzielnej kompilacji pod Windows – otrzymywany jest wtedy ten sam program w formie pliku EXE.

Fragment raportu z Eyewitness ze zrzutem strony i z danymi o hoście został przedstawiony na rysunku 206.



Rysunek 206. Fragment raportu z EyeWitness ze zrzutem strony i z danymi o hoście

Dodatki

Jeśli już jesteśmy przy archiwizacji stanu przeglądanych stron internetowych, warto wspomnieć też o wtyczkach do przeglądarek. Jednym z lepiej działających dodatków/wtyczek/rozszerzeń jest, moim zdaniem, FireShot (wersje dla przeglądarek: Firefox[144], Chrome[145], Edge[146], a także innych), który nawet w darmowej wersji pozwala na przechwycenie całej strony jednym skrótem klawiszowym (przy okazji – warto pamiętać, żeby nie ufać dodatkom do przeglądarek i weryfikować ich pochodzenie przed instalacją). Dużo opcji oferuje także dodatek Nimbus (dla przeglądarek Firefox[147] i Chrome[148]).

Co ciekawe, funkcje zapisu całych stron do obrazka czy PDF-a powoli stają się częścią samych przeglądarek – Firefox ma od jakiegoś czasu opcję WYKONAJ ZRZUT EKRANU w menu kontekstowym, a w Edge pod skrótem CTRL+SHIFT+S jest opcja (dostępna także z menu) PRZECHWYCENIE SIECI WEB, która, wbrew nazwie, służy jedynie do wykonywania zrzutu ekranu i umożliwia dodawanie późniejszych adnotacji i zapisywanie go jako obrazka, podobnie do funkcji WYCINEK I SZKIC w Windowsie.

Przeglądarkowe, darmowe narzędzia wymagają niestety interakcji użytkownika – chcąc mieć narzędzie, które będzie podążało za działaniami w sieci, warto pomyśleć o opcjach płatnych, jak np. Hunchly, które jest jednym z najpopularniejszych narzędzi do wspomagania i archiwizacji śledztw OSINT-owych (chociaż trzeba zaznaczyć, że nie współpracuje z Firefoksem).

Na koniec jeszcze kilka słów o zapisywaniu ekranu w formie nieco bardziej dynamicznej – do tworzenia filmików z przebiegu działań OSINT-owych warto użyć Screenity[149], rozszerzenia do przeglądarki Chrome, które nagrywa ekran, pozwala wprowadzać dodatkowe opisy i rysować na ekranie, wskazywać kliknięcia, dodawać dźwięk oraz eksportować filmy.

Podsumowanie i rady

Zapisywanie informacji znalezionych w trakcie internetowego śledztwa to bardzo ważny element OSINT-u. Z jednej strony, pomaga to poradzić sobie z niedoskonałościami natury ludzkiej, czyli zwykłym zapomnieniem, gdzie znalazło się daną informację i jak ona dokładnie brzmiała, a z drugiej – ratuje w przypadku niedostępności danego źródła w Internecie przy próbie powrotu, aby ją ponownie znaleźć. Analiza zrzutów ekranowych może także pomóc odtworzyć linię czasową dotarcia do danego miejsca w sieci.

CZĘŚĆ IV: OSINT W BIZNESIE

R35 JAK WYKORZYSTAĆ OSINT DO OCHRONY BIZNESU?

Duże firmy i organizacje najczęściej dysponują własnymi zespołami bezpieczeństwa, dbającymi o to, aby nieproszeni goście nie dostali się do wewnętrznej sieci i budynków, a potem przede wszystkim do danych. W mniejszych firmach jest to temat trudniejszy, gdyż niejednokrotnie nie mają one wystarczających kadr, aby wyznaczyć chociażby jedną osobę, która będzie sprawować tego typu funkcję. Niezależnie od wielkości i zaawansowania ochrony cyberbezpieczeństwa w danym podmiocie możliwe jest wykorzystanie technik OSINT-owych, które wskażą, jakie dane firmowe udostępniane są w Internecie, w jaki sposób i którędy może dojść do próby ataku, oraz uzmysłowią, co należy poprawić, aby do takiego ataku nie doszło.

Pierwszym krokiem do zapewnienia bezpieczeństwa jest sama świadomość możliwości ataku. Jeżeli pracownicy firmy, a w szczególności kierownictwo, będą świadomi zagrożeń, będą też w stanie skuteczniej się bronić przed ewentualnymi próbami wykorzystania niedoskonałości zabezpieczeń. **OSINT jest też jednym z pierwszych etapów ataków, zarówno w dziedzinie informatycznej, jak i socjotechnicznej.** Atakującym nie opłaca się atakować, jeśli nie wiedzą, jakie systemy napotkają po drugiej stronie. Zdarzają się oczywiście ataki „na ślepo", jednak jeśli dana grupa lub osoba poważnie podchodzi do tematu ataków, najpierw przeprowadzi rekonesans, aby określić możliwości powodzenia ataku oraz techniki i narzędzia, jakich należy użyć. Z tego powodu, **aby skutecznie się obronić, takiego samego rekonesansu powinny dokonywać same firmy**.

W tym rozdziale chciałbym zwrócić uwagę na kilka aspektów, które warto wziąć pod uwagę, przeprowadzając OSINT własnej firmy.

Dokumenty

W mojej pracy bardzo często poszukuję przeróżnych dokumentów w Internecie. Przez lata nauczyłem się kilku zasad.

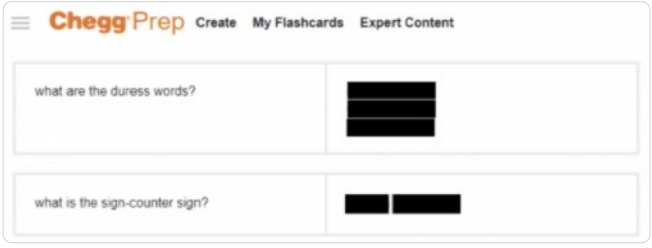
Po pierwsze: **nawet jeśli danego dokumentu nie ma prawa być w sieci, warto go jednak poszukać**. Niestety, wiele organizacji udostępnia dokumenty w formie zarówno skanów, jak i plików edytowalnych, chociaż nie wolno im tego robić. Pliki te najczęściej mają dopiski „do użytku wewnętrznego" lub „zakaz kopiowania i rozpowszechniania", a mimo to w wielu zespołach znajdzie się ktoś, kto takie dokumenty udostępni. Tak było m.in. w przypadku umieszczenia w jednym z narzędzi ArcGIS danych 20 tysięcy policjantów[150] czy bazy prawie wszystkich obywateli Austrii[151].

Po drugie: **brak bezpośredniego linkowania do plików nie zabezpiecza przed dostępem do nich**. Zdarzało mi się uzyskiwać dostęp do dokumentów, do których linki łatwo było odgadnąć, ponieważ zawierały np. kolejne numery lub były tworzone w przewidywalny sposób na podstawie informacji, które nietrudno było pozyskać.

Po trzecie: **zabezpieczenia plików**, a w szczególności PDF-ów, w postaci zaciemnienia niektórych elementów, są czasami wykonane w mało efektywny sposób i umożliwiają dostęp do „zamazanych" danych (zabezpieczanie plików PDF zostało opisane w rozdziale *Metadane – Święty Graal czy ślepy zaułek?*, s. 89–94).

Weryfikację obecności plików firmowych można sprawdzić przez wyszukiwanie fraz, które się w nich znajdują, a są unikalne dla danej firmy. Może to być jej nazwa, adres, numer telefonu, adresy e-mail lub indywidualne hasła reklamowe.

Jednym z przykładów mało odpowiedzialnego publikowania danych wewnętrznych w Internecie jest przypadek wykorzystywania serwisu do nauki za pomocą fiszek do niezamierzonego upublicznienia przez żołnierzy m.in. rozmieszczenia broni nuklearnej NATO w Europie (rysunek 207[152]).

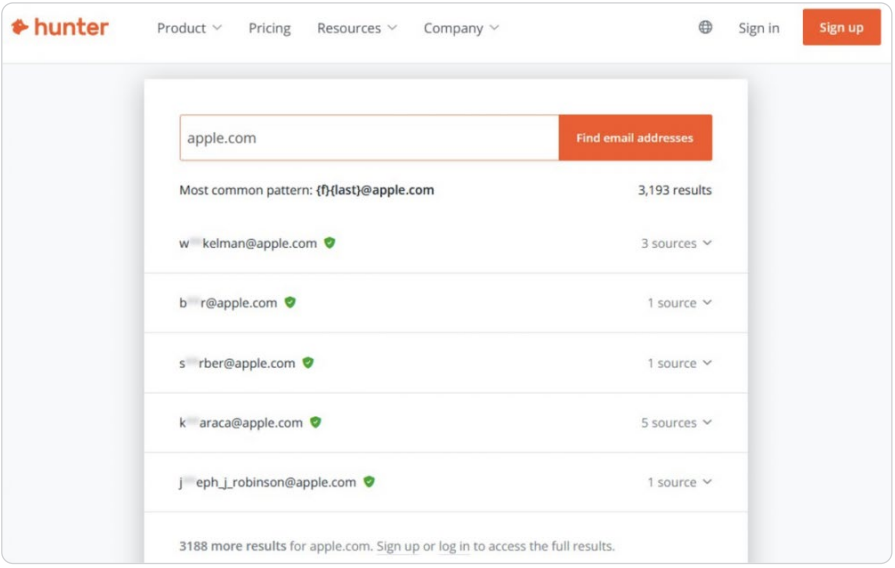


Rysunek 207. Przykład fiszki zawierającej informacje o bazach wojskowych NATO w Europie

Adresy e-mail

Skoro wspomniałem wyszukiwanie za pomocą adresów e-mail, warto także powiedzieć parę słów o wyszukiwaniu ich samych. Identyfikacja adresów, które są dostępne w sieci, może pomóc wskazać te konta, które mogą być bardziej narażone na atak, np. phishingowy. Adresy e-mail można wyszukać nie tylko na stronie firmowej, ale także m.in. w dokumentach dostępnych w Internecie, agregatorach danych (jak np. *hunter.io*, rysunek 208) oraz w wyciekach

danych, przy czym jeśli chodzi o te ostatnie, to w najprostszym scenariuszu nie jest konieczne poszukiwanie w bazach pozyskiwanych z forów w darknecie, a wystarczy sprawdzenie np. na portalu *haveibeenpwned.com*, czy dany adres e-mail nie znajduje się na tej liście.



Rysunek 208. Przykład wyszukania informacji o znalezionych adresach e-mail z domeny *apple.com* wraz z ich wzorcem

Portal *hunter.io* udostępnia jeszcze jeden zestaw interesujących informacji, a mianowicie wzorce tworzenia adresów e-mail w danej domenie. Przykładowo, jeśli obecne w Internecie adresy będą wskazywały, że tworzone są według wzorca: `imię.nazwisko`, to zostanie to przedstawione w formie wzorca `{first}.{last}`. Jeśli wzorzec będzie wskazywał na obecność jedynie pierwszej litery imienia przed nazwiskiem, będzie to: `{f}{last}` itd.

Media społecznościowe – firmowe i prywatne

Firmy lubią chwalić się swoimi osiągnięciami w mediach społecznościowych i nie ma w tym nic złego – w końcu do tego one służą. Warto jednak zwrócić uwagę, jakie informacje są udostępniane. Czy przed publikacją nowego wpisu ktoś weryfikuje, czy na pewno wszystkie dane powinny się w nim znaleźć? Czy nie są podawane nadmiarowe informacje, być może nie wprost, lecz w sposób znacznie ułatwiający zdobycie wiedzy o zabezpieczeniach? Jeśli np. firma publikuje informację o swoim nowym, tajnym projekcie, ale podaje tak dużo danych, że wywnioskowanie pozostałych jest jedynie kwestią połączenia faktów, to ten temat nie jest już tajny. Nabiera to szczególnego znaczenia, jeśli dotyczy informacji policji, wojska lub innych służb.

Warto także zwracać uwagę pracownikom na to, by nie publikowali na swoich prywatnych kontach w mediach społecznościowych informacji służbowych, które mogą mieć wpływ na obniżenie poziomu bezpieczeństwa firmy. Osobiście wychodzę z założenia, że wszystkie informacje, które są oficjalnie dostępne na stronie firmowej, mogą być dalej upubliczniane, a jeśli czegoś nie widać na stronie lub w mediach firmowych – lepiej tego nie podawać dalej.

W przypadku konieczności zachowania poufności konkretnych informacji warto także uczulić pracowników, aby porozmawiali ze swoimi rodzinami o niepublikowaniu informacji, które mogą mieć wpływ na przypadkowe upublicznienie poufnych danych. Mam tu w szczególności na myśli tematy ruchów wojsk. Zdarzało się bowiem, że rodziny żołnierzy dzieliły się informacjami, gdzie udają się ich bliscy. Ich teoretycznie nie obowiązuje tajemnica, ale dobrze jest zabezpieczyć także ten obszar.

Zdjęcia

Mając pewność, że na zdjęciach wykonanych wewnątrz firmy nie widać niczego niepokojącego, tzn. nie zostały upublicznione szczegóły zabezpieczeń fizycznych oraz elektronicznych, jak np. hasła do Wi-Fi napisane na tablicy (rysunek 209[153]), warto sprawdzić też zdjęcia w serwisie Google StreetView. Może się bowiem okazać, że przejeżdżający samochód Google uchwycił moment, gdy można było zobaczyć elementy wewnątrz terenu lub pomieszczeń firmy, których nie powinno być widać.

Rysunek 209. Słynne zdjęcie księcia Williama, na którym uchwycono także login i hasło do jednego z wojskowych systemów, widoczne na kartce przyklejonej do ściany

Kluczowe osoby

Jednym z niedocenianych elementów OSINT-u firmy jest skupienie się na kluczowych osobach i wykonanie rozpoznania tego, jaki ślad w Internecie zostawiają. Pod pojęciem kluczowych osób nie mam na myśli jedynie ścisłego kierownictwa, ale także np. administratorów i wszelkie osoby mające dostęp do wartościowych informacji. To one będą obiektem ataku, jeśli okaże się, że zdobycie cennych danych jest niemożliwe w bezpośredni sposób. OSINT tego typu osób może znacznie pomóc w uprzedzeniu ich, że mogą stać się obiektem konkretnego typu ataku oraz że powinny np. ograniczyć ekspozycję w zakresie publikowanych danych o swoich podróżach służbowych lub planowanych wyjazdach.

Podsumowanie i rady

Powyższe zagadnienia zostały opisane z perspektywy zabezpieczenia interesów firmowych. Nic nie stoi jednak na przeszkodzie, aby użyć ich przy zapewnieniu bezpieczeństwa swojej rodzinie i bliskim. Wdrożenie zabezpieczeń przed atakami będzie niekiedy trudniejsze niż w firmie, w której można przeforsować politykę zakazującą umieszczania w Internecie dokumentów służbowych, ze względu na brak wpływu na wszystkich członków rodziny, mających własne poglądy na to, czy naprawdę trzeba wstawiać dziesiątki zdjęć z każdych wakacji na bieżąco oraz czy trzymanie skanu swojego dowodu na ogólnodostępnym serwisie do udostępniania dokumentów jest bezpieczne. Uprzedzając pytania: moim zdaniem „nie trzeba, a nawet nie należy" oraz „zdecydowanie nie jest bezpieczne". Niekiedy pomaga pokazanie, jak za pomocą jedynie prostych technik OSINT-owych można dowiedzieć się, co wujek jadł wczoraj na śniadanie oraz że ciocia urodziła się jednak pięć lat wcześniej, niż twierdzi.

Jeśli w firmie nie były prowadzone opisywane tutaj OSINT-owe sprawdzenia poziomu udostępniania danych, warto o tym pomyśleć i zainwestować w tego typu umiejętności. Lepiej jest bowiem odnaleźć i spróbować usunąć nadmiarowo upublicznione informacje, zanim staną się one przyczyną wpadki wizerunkowej lub, co gorsza, przedmiotem ataku.

R36 PODSTAWY OBRONY PRZED ATAKAMI SOCJOTECHNICZNYMI

Projektując lub analizując zabezpieczenia systemów teleinformatycznych, należy wziąć pod uwagę, oprócz całej gamy zabezpieczeń „cyfrowych", także fakt, że **jednym z elementów każdego systemu jest jego interakcja z człowiekiem go obsługującym**. Niestety, niemalże w każdym przypadku jest to najsłabsze ogniwo tegoż systemu.

Człowiek jest z jednej strony najmniej przewidywalny, a z drugiej – najbardziej podatny na wpływy osób chcących złamać zabezpieczenia i pozyskać interesujące je dane. Ataki na systemy informatyczne przy użyciu technik wpływu na użytkowników nazywane są atakami socjotechnicznymi i bazują na podatnościach nie sprzętu czy oprogramowania, ale na skłonności człowieka do ulegania bezwiednie wpływom osób, które chcą przez to zdestabilizować pracę systemu (a co za tym idzie, osoby lub organizacji) lub uzyskać dostęp do pożądanych informacji, takich jak: dane dostępowe do konta bankowego, numer PIN lub CVC karty kredytowej, szczegółowe dane osobowe, czy też innej informacji, która w danym momencie jest dla nich niezbędna do wykonania „misji" przestępcy (np. wyczyszczenie konta, zaciągnięcie kredytów w naszym imieniu itp.). Ataki mogą być wymierzone nie w konkretną osobę, ale w całą firmę czy organizację, a celem atakującego będzie przeniknięcie w jej głąb, poznanie struktury i enumeracja podatności, a w końcu zaszkodzenie jej lub uzyskanie pożądanych informacji.

W całym rozdziale często pojawiają się stwierdzenia „na przykład", „między innymi" czy „i tym podobne". Bierze się to z faktu, że niniejszy tekst omawia jedynie mały wycinek możliwości i technik wykonania ataku socjotechnicznego. Przestępcy dostosowują atak do ofiary i sytuacji, często mieszając techniki wpływu społecznego i wykorzystując dodatkowo różnego rodzaju „zasłony dymne". Poniższe informacje i przykłady należy traktować jedynie jako wskazówki do dalszego zastanowienia się nad przebiegiem potencjalnego ataku.

Budując obronę przed atakami socjotechnicznymi, należy przede wszystkim poznać i, co najważniejsze (a jednocześnie najtrudniejsze), nauczyć się kilku podstawowych **technik wpływu na zachowanie drugiego człowieka**, aby w momencie, kiedy następuje atak, zauważyć ten fakt i zdążyć się przed nim obronić. Największy problem polega jednak na tym, że techniki te trzeba sobie tak głęboko przyswoić, żeby nawet podczas ataku, w chwili nagłego stresu powodowanego celowo, aby wywołać dezorientację, zauważyć, że trwa atak i należy zacząć się bronić.

Niestety, brak informacji, kiedy następuje atak, wykorzystywanie słabości (być może pozyskanych z wcześniejszych ataków socjotechnicznych), mnogość typów ataków oraz przede wszystkim sprytne ukrycie ich w interakcji powoduje, że nawet wybitni specjaliści z zakresu psychologii społecznej raz na jakiś czas dają się złapać na przynętę atakującego. Niemniej jednak znajomość narzędzi wpływu społecznego jest podstawą obrony przed napastnikiem. Tak jak wiele szkół walki uczy chwytów, które mogą służyć do wyrządzenia przeciwnikowi krzywdy, lecz jednocześnie wpaja zasadę, że te techniki powinny służyć tylko do obrony, tak samo **specjaliści od wpływu społecznego, chcąc uodpornić daną osobę na ataki socjotechniczne, uczą ją metod wpływania na drugiego człowieka, jednocześnie przestrzegając, by stosować je tylko**

i wyłącznie do obrony. Analogicznie sprawa ma się w przypadku trenerów cyberbezpieczeństwa i metod obrony przed atakami typowo informatycznymi.

Przygotowanie i przeprowadzenie ataku

W celu odpowiedniego przygotowania się do ataku w pierwszej kolejności poszukuje się informacji, które są dostępne bez konieczności interakcji z daną osobą lub z pracownikami danej organizacji, które mają być celem ataku socjotechnicznego. Wykonuje się wtedy tzw. ***footprinting***, **czyli wstępne rozpoznanie celu**. Elementem tegoż może być m.in. „nurkowanie w śmietniku" (ang. *dumpster diving*), czyli poszukiwanie porzuconych informacji, które pomogą nam później odpowiednio sprofilować ataki socjotechniczne. Atak na osobę prywatną może być więc poprzedzony przejrzeniem jej kont w mediach społecznościowych. W przypadku ataków na firmę poszukiwane są informacje o jej strukturze, adresy e-mail, nazwiska i stanowiska, numery telefonów czy nawet zużyte elementy wyposażenia informatycznego, które mogą zawierać przydatne dla atakującego dane.

Aby atak socjotechniczny miał większe prawdopodobieństwo powodzenia, osoba będąca jego celem w większości przypadków jest najpierw odpowiednio „urabiana", by łatwiej było nią manipulować. Do tego typu działań zaliczają się m.in. dwa zupełnie odmienne zachowania – **wprowadzenie ofiary w stan pełnego zaufania i komfortu lub w stan mocnego stresu**.

Pierwsze charakteryzuje się działaniami mającymi uśpić czujność ofiary, sprawić, by czuła się dobrze i bezpiecznie, aby w momencie, kiedy najmniej spodziewa się zagrożenia, którego może nawet nie zauważyć, przypuścić atak. W drugim z wymienionych zachowań atakujący wprowadza chaos w otoczeniu ofiary, aby poczuła się ona zagrożona lub zdezorientowana mnogością informacji i przez to działała w sposób jak najbardziej automatyczny. Związane jest to z jednym z podstawowych zasad funkcjonowania ludzkiej psychiki, która odwołuje się do ewolucji gatunku ludzkiego i rozwoju mózgu człowieka. Najstarszą, z ewolucyjnego punktu widzenia, częścią centralnego ośrodka nerwowego jest pień mózgu. Jest on odpowiedzialny za automatyczne działanie naszego ciała, co wydaje się dość sensowne, biorąc pod uwagę fakt, że nasi przodkowie musieli raczej martwić się o to, jak upolować zwierzynę lub jak przed nią uciec, zaś kontemplowanie piękna otaczającego krajobrazu i kreatywne myślenie przyszło nieco później, kiedy podstawowe potrzeby takie jak pożywienie i bezpieczeństwo były już zapewnione. Jaki to ma związek z atakami socjotechnicznymi? Otóż **mózg w momencie nagłego stresu przełącza się na podstawowe sterowanie, wraca do prymitywnych zachowań, aby nas przede wszystkim chronić**. Przetwarzanie informacji odbywa się głównie w pniu mózgu, co skutkuje niezwykle dużą automatyką zachowań. I tu właśnie przydaje się nam bardzo dobre wyuczenie technik wpływu społecznego.

Im bardziej są one przyswojone, tym większa jest szansa, że mózg będzie brał je pod uwagę w momencie nagłej potrzeby szybkiego działania. Należy sobie wyrobić odruch warunkowy (niczym psy Pawłowa reagujące na dzwonek na kolację) i wprowadzić do „rdzenia" systemu dowodzenia odpowiednie mechanizmy obronne.

Najczęstsze rodzaje ataków

Święta nie tylko od święta

Jednym z najprostszych sposobów na atak z użyciem socjotechniki (choć można by się kłócić, czy jej stopień zastosowania tutaj jest na tyle duży, aby kategoryzować ten typ ataku jako socjotechniczny) jest przekazanie ofierze prezentu w formie np. spreparowanego pendrive'a zawierającego złośliwe oprogramowanie, które wykradnie dane. Może to być prezent w zamian za wypełnienie ankiety (fikcyjnej oczywiście, służącej jedynie zyskaniu podstaw do dania nam prezentu) lub podarunek od potencjalnego kontrahenta na poczet przyszłej współpracy. Niemalże każdy lubi być obdarowywany, więc po otrzymaniu takiego prezentu **rzadko podejrzewa się osobę, która była miła** (dała nam przecież prezent, więc na pewno nie ma wobec nas złych zamiarów), o próbę kradzieży. Na przykładowym pendrivie może znajdować się choćby rozbudowany keylogger, który przechwyci i wyśle do atakującego informacje np. o wybranym banku czy loginie i haśle. W połączeniu z przejęciem kontroli nad posiadanym telefonem lub kartą SIM przestępca może w spokoju wyczyścić nam konto. Na temat tego, czy możliwe jest zabezpieczenie się w pełni przed kradzieżą pieniędzy z konta z wykorzystaniem przechwyconych danych dostępowych do konta bankowego i zduplikowanej karty SIM lub zhackowanego telefonu komórkowego, trwają ożywione dyskusje w Internecie, więc na razie ograniczymy się do najbardziej podstawowych i „zgrubnych" metod uodparniania się na tego typu ataki. Na szczęście (?) w polskiej rzeczywistości często spotyka się też przejawy większej podejrzliwości („Aha, dał/dała mi coś, więc na pewno czegoś chce!"), które w tym wypadku mogą uratować przed bezrefleksyjnym przyjmowaniem podarków i używaniem ich w domu czy w pracy.

Swego czasu głośno było o chińskich firmach dających swoim zachodnim kontrahentom pendrive'y[154], na których znajdowało się wyżej opisane oprogramowanie. W tym przypadku nie chodziło jednak o okradzenie konta bankowego, a o wejście w posiadanie informacji o znaczeniu strategicznym dla prowadzonych biznesów.

Prezent może być także niematerialny – może być to wizja wygrania dużej nagrody, przesłana e-mailem wraz z linkiem do strony, na której będzie się znajdowało szkodliwe oprogramowanie.

Ludzie tacy jak my

Wspomniany przed chwilą sposób uśpienia czujności ofiary przez podarunek może też przyjąć postać rozmowy poprowadzonej w taki sposób, aby osoba atakowana poczuła więź z atakującym i przez to pozbyła się oporów przed wyjawieniem mu poufnych danych lub nawet podaniem ich z chęcią „na tacy". Działanie takie opiera się na **psychologicznej regule sympatii**.

Im bardziej jakaś osoba podobna jest do nas, nosi chociażby podobne imię czy nazwisko, podobnie się ubiera, wyznaje zbieżne z naszymi poglądy polityczne itp., tym bardziej jesteśmy skłonni uznać ją za osobę godną zaufania i automatycznie traktujemy ją lepiej. Wynikiem takiego automatycznego przyporządkowania jest brak lub znaczne ograniczenie zahamowań przed wyjawieniem informacji. Może nam się wydawać, że jesteśmy odporni na tego typu sposoby podejścia nas. Przestępcy używający socjotechniki to jednak w ogromnej większości osoby świadome takich automatycznych zachowań i wystarczy im jedynie drobna nieuwaga z naszej strony, aby przeprowadzić skuteczny atak. Atakujący może prowadzić z nami długą rozmowę, opowiadając o rzeczach, które nas łączą, udając osobę wybierającą się w tym samym kierunku lub cierpiącą z tego samego powodu. Może też wykorzystać część informacji zdobytych wcześniej od nas lub o nas, aby stworzyć wrażenie posiadania wspólnego wroga albo udawać, że zna kogoś ze znajomych, aby wkraść się do grona osób najbliższych, tj. godnych zaufania. W tym celu atakujący może wykorzystywać ujawnione podczas rozmowy informacje, „podczepiając się" pod nasze słowa („Tak, tak, znam go/ją od lat!") albo wykorzystać dane z wcześniejszego rekonesansu, np. odwiedzając profil w portalu społecznościowym. W dzisiejszych czasach bardzo wiele osób dzieli się chętnie w sieci informacjami o tym, kogo znają, z kim się spotkały i co jadły, gdzie spędziły wakacje itp. To wszystko ułatwia atak wymierzony w konkretną osobę (ang. *spear-phishing*) i może być użyte w celu zwiększenia podatności nań.

Zresztą nie tylko ludzie starają się sprawić, abyśmy poczuli się, jakbyśmy ich znali, a co za tym idzie – bezpiecznie. Strony internetowe starają się wyglądać tak, jak dobrze nam znane ekrany logowania do banku, poczty czy choćby Facebooka. Osoba widząca dobrze znaną kolorystykę i layout nie pomyśli, że jest właśnie atakowana, i poda przestępcy swoje dane dostępowe. A jeśli ten trafi na osobę mniej obeznaną w bezpieczeństwie IT lub procedurach bankowych, to jest szansa, że uda się wydobyć od ofiary także kody potwierdzeń dla przelewów lub inne informacje, które później można wykorzystać do kradzieży pieniędzy z konta. Dlatego banki coraz częściej informują, że nigdy nie wymagają od swoich klientów podania dodatkowych danych podczas procesu logowania lub w korespondencji e-mailowej.

Przysługa za przysługę

Kolejnym sposobem przygotowania ofiary do wyjawienia informacji lub spełnienia prośby atakującego jest wykorzystanie **reguły wzajemności**. Ten prosty mechanizm każe nam odwdzięczyć się za wyświadczoną nam przysługę, czy jej potrzebowaliśmy, czy nie. Przestępca wykorzystujący socjotechnikę będzie się zatem starał stworzyć taką sytuację, abyśmy poczuli obowiązek wyświadczenia mu przysługi.

Jeśli przestępca przeniknie do firmy, może np. pomóc ofierze pozbierać przypadkiem rozrzucone dokumenty (samemu tworząc wcześniej przypadkowe potrącenie) lub skorzystać z faksu czy drukarki. Kiedy pomoc zostanie już wyświadczona, przychodzi czas na rewanż – i tu pojawia się prośba o ujawnienie informacji bądź np. wpuszczenie do zamkniętej części firmy, do której ofiara ma dostęp, a w efekcie – przeniknięcie jeszcze głębiej i zdobycie dodatkowych informacji. Atakujący może także poprosić o przysługę mało prawdopodobną do spełnienia, a kiedy mu odmówimy, wyjść z prośbą o wyświadczenie dużo mniejszej i prostszej. Kiedy ofiara odmówiła pomocy za pierwszym razem, będzie czuła odpowiedzialność, aby tę sytuację naprawić – i będzie miała większą motywację, aby spełnić drugą prośbę.

Uratuj mój świat

Innym sposobem przekonania potencjalnej ofiary do wykonania prośby atakującego jest sprawienie, aby sądziła ona, że **to, co robi, jest wartościowe i potrzebne**. Prosto rzecz ujmując, można stwierdzić, że jest to stwarzanie poczucia bycia superbohaterem, wybawicielem innych. Wbrew pozorom na ataki „na wnuczka" wcale nie są narażone tylko osoby starsze. W przypadku cyberataku zamieniamy jedynie wypadek krewnego na awarię systemu, policjanta na administratora sieci, a pieniądze na dane logowania – mechanizm działania przestępcy jest dokładnie ten sam.

Technika ta jest często stosowana łącznie ze stwarzaniem wrażenia pośpiechu i dezorientowaniem osoby będącej celem ataku. Może to być wykorzystane zarówno w rozmowie telefonicznej („Nastąpiła awaria serwerów, prosimy o podanie kodu dostępu do serwerowni, musimy szybko usunąć awarię"), korespondencji e-mailowej („Tu administrator, wykryliśmy atak na Pana/Pani komputer, proszę podać login i hasło do swojego komputera/poczty, abyśmy mogli zweryfikować sprawcę. Prosimy nie rozpowszechniać tej informacji, aby nie spłoszyć włamywacza"), jak i w interakcji bezpośredniej. Prośby te są często nieracjonalne, jeśli się nad nimi dłużej zastanowić, ale fakt wykonywania operacji w pośpiechu i świadomości, że od konkretnej akcji zależy np. odzyskanie danych firmowych, skłania nas do pójścia drogą wskazaną przez atakującego. Przez pośpiech nie weryfikujemy, czy strona, na której się logujemy, nie jest stroną podstawioną przez przestępcę lub czy osoba dzwoniąca do nas

naprawdę jest tym, za kogo się podaje, a dodatkowa prośba o nierozpowszechnianie informacji z jednej strony zapewni atakującemu czas na dalsze działania, a z drugiej – sprawi, że będziemy postrzegać siebie jako istotny element ważnej misji ratunkowej.

Może się także zdarzyć, że atakujący np. zadzwoni z informacją o urlopie, na którym właśnie powinniśmy przebywać. Kiedy odpowiemy, że nie przebywamy na urlopie, atakujący uda zdziwienie i zakłopotanie sytuacją, że do systemu wkradła się pomyłka. W tym momencie sam stwarza sytuację, w której możemy okazać się dla niego wybawieniem, jeśli podamy mu kilka danych w celu naprawienia problemu („A kiedy idziesz na urlop? A może ktoś z Twojego działu jest dzisiaj na urlopie? Jaki masz login w systemie?").

Czy jest na sali jakiś lekarz?

W ramach wyrabiania w osobie atakowanej poczucia bezpieczeństwa stosowana jest też bardzo często **reguła autorytetu**. Atakujący udaje kogoś, co do kogo nie mamy podejrzeń, ponieważ dana osoba posiada uniform lub inne atrybuty jednego z typowych i znanych nam zawodów. Przestępca przebiera się zatem za lekarza, policjanta, strażaka (czyli osobę, której ubiór świadczy o wykonywanym zawodzie) lub serwisanta sprzętu IT (którego nie obowiązuje ubiór roboczy, ale np. może być rozpoznawalny przez koszulkę firmową firmy serwisującej sprzęt, identyfikator oraz narzędzia). Badania pokazały, że „przebraniem" nie musi być nawet mundur policyjny ani kitel lekarski – wystarczy ubranie robocze choćby przedsiębiorstwa wywożącego odpady, aby nikt nawet nie pytał o zasadność wykonania polecenia „przebierańca". W ogromnej liczbie zdarzeń takie osoby nie miały najmniejszego problemu z przeniknięciem do danej instytucji i nakłonieniem pracowników do wykonania pożądanych przez atakującego czynności. Co więcej, spotkały się nawet z nadmiernym zaufaniem i zebrały większe „żniwa", niż się spodziewały.

Nawet bez odpowiedniego ubioru służbowego można jednak przeniknąć do wnętrza firmy lub innej organizacji. W niektórych przypadkach wystarczyło wejście na tzw. bezczelnego – póki wyglądasz, jakbyś wiedział, co robisz, to na pewno to robisz. W tym kontekście może zostać także użyta technika wejścia „przy okazji" (ang. *tailgating*), kiedy atakujący korzysta z faktu, że ktoś, kto ma dostęp do danego budynku/obszaru, wchodzi do niego, i wchodzi tam razem z nim, jak gdyby nigdy nic.

Oczywiście nie tylko ludzie mogą być fałszywymi autorytetami. Jeśli otrzymujemy e-mail z załącznikiem, to dużo chętniej go otworzymy, jeśli w treści wiadomości będzie zawarta regułka „Załączniki przeskanowane pomyślnie przez oprogramowanie antywirusowe X".

Owczy pęd

Jeszcze innym mechanizmem wpływu na człowieka jest **reguła społecznego dowodu słuszności**. Ludzie mają tendencję do wykonywania czynności tylko dlatego, że inni tak robią. Takie zachowanie może być wykorzystane przez przestępcę do uzyskania dostępu do informacji, jeśli przekona ofiarę, np. poprzez wiadomość e-mail, że jest ona ostatnią osobą, która jeszcze nie podała swoich danych dostępowych do poczty firmowej do (fikcyjnego oczywiście) administratora, który tego wymagał. Wcześniejszej prośby mogło nawet nie być, ale świadomość, że inni już to wykonali, przynajmniej na chwilę zbije atakowanego z tropu i być może umożliwi przestępcy zdobycie interesujących go danych. Atakujący może także wyrobić w atakowanym przeświadczenie, że powinien wykonać jakieś działania, poprzez przesłanie kopii sfałszowanej korespondencji, z której wynika, że kilka osób wypowiedziało się już w jakiejś kwestii i wykonało określone działanie. Ofiara ataku dostaje wiadomość dopiero na pewnym etapie i widząc działania innych, także stara się podążyć za grupą.

Powiedziałeś A, powiedziałeś B...

Reguła konsekwencji to kolejne narzędzie, które jest wykorzystywane w atakach z użyciem socjotechniki. Zaangażowanie i konsekwencja każą, by nie wycofywać się z przedstawianych przed chwilą opinii. Jedną z konkretnych technik w ramach tej reguły jest „stopa w drzwiach" (ang. FITD – *foot-in-the-door*). Mówi ona, że po zgodzie na pierwszą, małą prośbę jesteśmy bardziej skłonni spełnić drugą, większą i nawet niezwiązaną w żaden sposób z pierwszą.

Ludzie mają także tendencję do **podążania utartymi i znanymi szlakami**, więc jeśli np. na przełomie miesiąca w firmie pojawiają się w skrzynce e-mailowej duże liczby faktur, istnieje dużo większe prawdopodobieństwo, że pracownik nie będzie weryfikował załącznika, ale od razu go otworzy. Załącznik oczywiście będzie spreparowany przez przestępcę, podszywającego się pod kontrahenta, i w najlepszym przypadku skończy się to ostrzeżeniem w oprogramowaniu antywirusowym, a w najgorszym – zaszyfrowaniem całego dysku (lub jeszcze gorzej: wraz z podłączonym akurat w tym momencie dyskiem z kopiami zapasowymi) i żądaniem okupu.

Już tylko pięć minut do końca promocji

Reguła niedostępności może być używana do zmuszenia osób do wykonania jakiejś akcji tylko dlatego, że jeśli nie zrobią tego teraz, stracą niepowtarzalną szansę na odniesienie korzyści. Dlatego w fałszywych e-mailach mogą się pojawiać sformułowania typu: „To jest ostatnia wiadomość przed usunięciem twojej skrzynki e-mailowej. Zaloguj się na nowej stronie [tutaj link do strony-pułapki], aby zachować wszystkie swoje wiadomości i kontakty!",

„Twoje hasło wygasło i musisz je natychmiast zmienić" lub „Na twoim komputerze wykryto groźnego wirusa! Pobierz szybko oprogramowanie antywirusowe!". Dodatkowo e-mail może być wysłany w piątek po godzinach pracy – tak, by osoba atakowana po przyjściu do pracy w poniedziałek pomyślała, że musi działać szybko, bo w innym wypadku straci swoje dane. Jako element potęgujący stres mogą być użyte rozpoznawalne nazwy i/lub znaki graficzne, np. instytucji skarbowych lub policji.

Nieodpowiedzialni odpowiedzialni

Stres jest złym doradcą – te słowa słyszał chyba każdy co najmniej raz w życiu. I to właśnie stres jest sprzymierzeńcem przestępców, ponieważ daje im o wiele większą pewność, że ich zamierzenia zostaną wykonane przez ofiarę. **Generując sztucznie sytuację „kryzysową"** wokół atakowanego, gdy decyzje muszą być podejmowane automatycznie, bez możliwości zastanowienia się, a dodatkowo bombardując dużą ilością dodatkowych informacji, przestępcy powodują dezorientację danej osoby. Dlatego jeśli atakujący chce wydobyć informacje np. przez telefon, będzie starał się narzucić tempo rozmowy podyktowane nagłą i niespodziewaną sytuacją, mówiąc np.: „Mamy ogień w korytarzu, czy może Pan/Pani podać kod do otwarcia drzwi do biura dyrektora X? Musimy sprawdzić, czy nikogo tam nie ma!". Nagły skok adrenaliny spowodowany informacją o pożarze, połączony jeszcze z odpowiedzialnością za gabinet szefa lub jego samego, może skłonić do podania tego kodu bez wahania.

Metody obrony

Jedno proste pytanie

Obrona przed atakami socjotechnicznymi, podobnie jak same ataki, to tematyka bardzo rozległa i mogąca być kombinacją kilku technik. Jednak w każdym przypadku ataku socjotechnicznego, od najprostszego otrzymania „prezentu" – konia trojańskiego, poprzez próbę zawarcia z nami przyjaźni lub udawania kogoś godnego zaufania, aż po usiłowanie destabilizacji otoczenia wokół nas i oczekiwanie od nas podjęcia odpowiedzialnej decyzji, **można wstępnie zweryfikować zasadność własnych działań i ich następstw**, zadając sobie jedno proste pytanie. Pytanie to znalazło się w jednej z reklam radiowych, które najczęściej zostają w naszych głowach w formie ich dziwnych melodyjek lub rymowanych haseł reklamowych. W tym przypadku głos w reklamie nakazywał: „**Zawsze pytaj: Dlaczego?**".

To z pozoru banalne pytanie potrafi w jednej chwili otrzeźwić, kiedy zdamy sobie sprawę, że tak naprawdę nie ma racjonalnego powodu, dla którego mielibyśmy wykonać jakąś czynność (lub nawet wręcz nie wolno nam jej wykonać), albo też okaże się, że atakujący zostanie zbity z tropu pytaniem, na które nie jest przygotowany. Może się oczywiście okazać, że oponent przemyślał

możliwe ścieżki przebiegu ataku, ale ten krok może być punktem zaczepienia w toku obrony przed atakiem socjologicznym.

Tak samo jak w interakcji z ludźmi, tak też w przypadku otrzymywania e-maili powinniśmy dać sobie chwilę do namysłu. Czy na pewno powinienem/powinnam otworzyć tę fakturę/informację o przesyłce, skoro nic nie zamawiałem/zamawiałam? Czy na pewno jest możliwe, aby była taka atrakcyjna oferta specjalnie dla mnie?

Kontrola – najwyższą formą zaufania

W ramach obrony przed próbą wywarcia wpływu poprzez sugerowanie, że powinniśmy zaufać atakującemu, ponieważ jest osobą na to zasługującą (niezależnie od rodzaju użytej przez niego techniki), można wprowadzić świadomie do rozmowy element, który będziemy kontrolowali, a który pozwoli sprawdzić rozmówcę.

Jeśli ktoś podaje się za osobę z kręgu naszych znajomych lub rodziny, nie możemy sprawdzać go pytaniami w rodzaju: „Czy to ty, Stefan?" (w przypadku rozmowy telefonicznej – kiedy nie widzimy osoby po drugiej stronie) lub „Znasz Kasię?", ponieważ jedyne, co może odpowiedzieć przestępca w tym momencie, to: „Tak, oczywiście!". Nie przyzna się przecież, że jest tymże przestępcą, ale będzie kontynuował wątek, upewniając nas, że jest osobą godną zaufania („No pewnie, że tu Stefan!", „No pewnie, że znam Kasię!"). W interesie atakującego jest podanie jak najmniejszej ilości informacji o sobie, aby nie wzbudzić niepotrzebnych podejrzeń, ale jednocześnie na tyle dużo, żeby zostać uznanym za konkretną osobę, którą znamy.

Aby sprawdzić potencjalnego fałszywego znajomego, trzeba użyć zdania twierdzącego, które jest nieprawdziwe na tyle, że prawdziwy rozmówca zdziwiłby się i zaprzeczył. W tym momencie przestępca powinien dać się „złowić" na przynętę (jeśli nie jest na poziomie, na którym jest odporny na takie sztuczki, lub ma tak dokładne informacje o nas, że nie da się nabrać). Można zatem powiedzieć np.: „Twój brat się ostatnio mocno zestarzał, nie?" (zakładając, że dana osoba podaje się za kogoś, o kim wiemy, że nie ma brata) lub: „Twój dyrektor/kierownik/manager ma nową żonę, nie?" (jeśli przestępca podaje się za kogoś, kto pracuje także w tej samej firmie w dziale, o którym wiemy, że jest kierowany przez kobietę). Jeśli druga osoba zignoruje zdanie lub wyda się zmieszana, to znaczy, że być może rozmówca nie przewidział tego przebiegu zdarzeń. Jeśli zaś odpowie nam twierdząco na fałszywe zdanie, będzie to jasnym znakiem, że jesteśmy właśnie atakowani.

Czy aby na pewno wiesz, gdzie jesteś?

W przypadku kiedy przestępca próbuje uśpić czujność za pomocą wyświetlenia strony, którą dobrze znamy i na której przecież tyle razy bezpiecznie się logowaliśmy, warto upewnić się, że znajdujemy się tam, gdzie chcemy się zalogować, a nie na stronie-pułapce. Dużym ułatwieniem są tutaj dodatki do przeglądarek współpracujące z menedżerami haseł, które na sfałszowanych stronach nie podpowiedzą nam danych logowania, gdyż adres nie będzie zgodny z wprowadzonym do menedżera.

Należy zweryfikować, czy na pewno adres danej strony w przeglądarce odpowiada adresowi, który powinien się tam znajdować*. W przypadku linków znajdujących się na stronach lub w przysłanych wiadomościach e-mail należy nie tylko sprawdzić, jaki adres jest pokazany jako link (np. podkreślony), ale także, dokąd prowadzi – po najechaniu na dany link u dołu przeglądarki powinien wyświetlić się faktyczny adres, pod który kieruje odnośnik. Jeśli jest to inny adres niż w nazwie linku lub jeżeli wydaje się on podejrzany, może to oznaczać próbę ataku. W przypadku telefonów komórkowych sprawa podglądu linków jest nieco trudniejsza, ponieważ w interfejsie dotykowym nie ma jak najechać na link przysłany e-mailem bez klikania w niego (można oczywiście zaznaczyć i skopiować odnośnik lub wyświetlić pełny tekst wiadomości i tak zweryfikować, jak skonstruowany jest link). Warto też sprawdzać, czy w adresie (w linku lub już na stronie, na którą się przenieśliśmy) nie ma literówki lub nie zostały użyte znaki jedynie przypominające litery, których byśmy się w danym adresie spodziewali. Wspomniane wcześniej dodatki do menedżerów haseł, np. KeePassXC, zrobią to za nas, nie podpowiadając danych logowania na fałszywej stronie. Taki sposób zakamuflowania prawdziwego adresu strony jest ostatnio dość często spotykany.

Aktualizacje i backupy to podstawa

Ważnym elementem ochrony ogólnie, nie tylko przed socjotechniką, jest aktualizacja oprogramowania, zarówno jeśli chodzi o system operacyjny, zwykłe oprogramowanie, jak i oczywiście oprogramowanie antywirusowe. Jeśli atak będzie polegał na wyłudzeniu informacji drogą elektroniczną (a nie ustnie lub fizycznie), będzie to na pewno utrudnienie dla atakującego. Kiedy jednak antywirus nie zadziała lub stracimy dane poprzez lukę w innym oprogramowaniu, warto mieć kopię zapasową, którą należy wykonywać na tyle często, aby ewentualna utrata nie była zbyt bolesna. Nośnik z kopią zapasową powinien być tylko do odczytu (CD/DVD/BluRay) lub podłączany do komputera tylko w momencie, kiedy wiemy, że jest bezpiecznie, i jak najszybciej odłączany. Warto też choćby raz wykonać odtworzenie danych z kopii zapasowej,

* Zob. też: M. Sajdak, *Czy zielona kłódka w przeglądarce chroni przed czymkolwiek?*, sekurak.pl, 2 lutego 2022.

bo wiadomo, że ludzie dzielą się na trzy grupy: tych, którzy nie robią kopii bezpieczeństwa, tych, którzy robią, oraz tych, którzy robią i wiedzą, że są w stanie odtworzyć dane z kopii. Podczas tworzenia kopii należy postępować zgodnie z zasadą 3–2–1, tj. tworzyć trzy kopie zapasowe, na dwoch rodzajach nośników, przy czym jedna w odrębnej lokalizacji niż pozostałe. Pozwoli to zminimalizować prawdopodobieństwo utraty kopii zapasowej.

To samo hasło wszędzie to drzwi do raju dla przestępcy

Może się jednak okazać, że damy się nabrać na sztuczki przestępców i podamy dane dostępowe na spreparowanej stronie-pułapce. Ważne staje się wtedy, czy stosujemy wszędzie to samo hasło czy nie. Jeśli atakujący pozna nasz adres e-mail i (nawet superbezpieczne pod kątem złożoności) hasło i okaże się, że tego samego hasła używaliśmy nie tylko do poczty, ale także do logowania się wszędzie indziej (lub używamy czytelnego klucza, jak „nazwa-banku123", „allegro1" itd.), to możemy stracić dużo więcej niż wiadomości e-mail. Warto zatem stosować inne hasła do poczty i każdego innego logowania, a także tam, gdzie to możliwe, stosować uwierzytelnianie wieloskładnikowe, z użyciem aplikacji lub urządzeń wspomagających takie działanie.

Nawet najlepsze hasła nie pomogą, jeśli leżą na biurku

Osobną kwestią jest temat przechowywania haseł. Warto skorzystać z oprogramowania do przechowywania haseł, zabezpieczonego mocnym hasłem głównym. Jeśli już chcemy przechowywać hasła w formie papierowej, należy zadbać o ich odpowiednie fizyczne zabezpieczenie. Trzymanie haseł (jak również innych kluczowych informacji) w wersji papierowej na biurku, obudowie komputera, monitorze czy tablicy przy biurku może prowadzić do tego, że nawet nie będziemy wiedzieli, kiedy ktoś tylko zajrzał do naszego miejsca pracy i zapamiętał/zrobił zdjęcie/zapisał sobie nasze hasła.

Taki strój można kupić w każdym sklepie

Pamiętajmy, że nie każdy, kto nosi biały kitel, musi być lekarzem. W dzisiejszych czasach można dostać w sklepach wszelką odzież specjalistyczną, od strojów lekarskich, ratowniczych i pielęgniarskich (takich standardowych, chociaż atak przy użyciu kusego stroju pielęgniarskiego też w dużej mierze opierałby się na zastosowaniu socjotechniki), poprzez stroje policji i straży pożarnej, na sutannach skończywszy. Każdy także może sobie wyrobić dowolny identyfikator, pieczątkę, a nawet dowód osobisty! Warto zatem przed powierzeniem ważnych informacji lub pieniędzy zweryfikować tożsamość danej osoby, np. pytając o nią obsługę danego budynku lub szukając informacji o konkretnym człowieku w Internecie.

Szkolenie z przykładami, czyli pokaż mi, czego nie potrafię

Niektóre organizacje wykonują specjalne szkolenia dla swoich pracowników, przygotowane na podstawie wcześniej przeprowadzonych ataków (można by je nazwać „szczepionkami", chociaż w kontekście n-tej wojny szczepionkowej w Internecie boję się użyć tego słowa). Pracownicy są zaznajamiani z sytuacjami, które mogą się im przydarzyć, aby, kiedy już one nastąpią, łatwiej je było rozpoznawać. Na takich spotkaniach przedstawia się m.in. listy pytań, które mogą być zadane, a które powinny nas zaalarmować. Najprościej jest to przedstawić na zasadzie **listy „zielony–pomarańczowy–czerwony"**.

W sekcji zielonej są pytania, które normalnie mogą paść z ust nieznajomej osoby i nie wydają się alarmujące, np.: „Dojeżdżasz do pracy na rowerze?", wypowiedziane w holu firmy, gdy widać, że jesteśmy ubrani „na rower" i aktualnie czekamy np. na kogoś innego. Takie zachowanie może być podyktowane chęcią zapytania o najlepszą trasę dojazdu, czas, warunki lub po prostu próbą zaczepienia nas przez osobę nami zainteresowaną (w pozytywnym tego słowa znaczeniu). Nasza odpowiedź twierdząca nie wyjawi żadnych informacji poza tymi, które pytający już ma (skoro mamy ubiór rowerowy, to raczej przyjechaliśmy rowerem).

Jeśli jednak rozmowa toczy się dalej i pytający drąży głębiej („A w którym miejscu trzymasz rower?"), powinna nam się zapalić „pomarańczowa lampka", ponieważ takie pytanie już może stanowić wstęp do pozyskania informacji, które pytający niekoniecznie musi zdobyć. Oczywiście może to być pytanie niewinne, absolutnie niebędące częścią ataku (nie popadajmy w paranoję!), stąd kolor pomarańczowy.

Kiedy jednak padnie pytanie: „A gdzie u was jest gabinet szefa/serwerownia/archiwum?", zapala się lampka czerwona. Takie informacje mogą już służyć do przeprowadzenia ataku i nie powinniśmy udzielać ich osobom, o których nie wiemy, kim są i czy mogą taką wiedzę otrzymać. Jeśli wydaje nam się, że mogliśmy stać się obiektem ataku, wtedy o próbie pozyskania informacji przez podejrzane osoby warto też powiadomić osoby odpowiedzialne za ochronę danych (administrator IT, inspektor bezpieczeństwa itp.). Przed podaniem naprawdę ważnych informacji warto też poinformować swojego zwierzchnika o tym, kto pyta, i upewnić się, czy możemy takich informacji udzielić. Jeżeli byliśmy obiektem ataku, istnieje bardzo duża szansa, że w tym momencie się obronimy.

Bardzo ważnym elementem jest **szkolenie personelu, nie tylko z technik ataków, tak aby kadra była przygotowana na różne próby przechwycenia informacji lub destabilizacji otoczenia i umiała je rozpoznawać, ale również z technik postępowania w przypadku, kiedy pracownicy znajdą się już w takiej sytuacji**.

Podczas szkoleń istotnym elementem jest uświadamianie, że niekoniecznie to, co jest ważne dla organizacji, musi być ważne dla potencjalnego przestępcy – i na odwrót, to, co może się wydawać mało ważne z punktu widzenia biznesu w firmie, jest też mało istotne dla włamywacza. Warto pokazywać, jak ktoś może próbować od nas wyciągnąć pewne dane, udając naszego przyjaciela. Najlepsze będą w tym wypadku przykłady udanych ataków z przeszłości. Istotne jest jasne określenie, że atakujący działa w celu wykradzenia informacji i/lub zaszkodzenia organizacji, a co za tym idzie, utrudnienia pracy lub nawet finalnie pozbawienia jej potencjalnych atakowanych osób. Takie postawienie sprawy często przyczynia się do tego, że ludzie stają się odporniejsi na próby wyłudzenia informacji i destabilizacji środowiska. Oczywiście, **szkolenia muszą być cykliczne, żeby wiedza była cały czas aktualizowana i utrwalana**. Aby jednak sprawić, że pracownicy będą wiedzieli, jak bardzo są narażeni na atak, warto przed szkoleniem lub już w jego trakcie poddać ich testowi, który wykaże, ile informacji są w stanie zdradzić potencjalnemu przestępcy. Dopiero kiedy faktycznie staniemy się ofiarą ataku (choćby ćwiczebnego), zdamy sobie sprawę, że nie jesteśmy tak sprytni i odporni, jak się nam wydaje.

Graj zgodnie z regułami gry

Innym z ważnych elementów, których wprowadzenie może uodpornić organizację (a także poszczególnych ludzi) na ataki socjotechniczne, są **procedury**. Procedury określają, jak postępować: jakie są wymagania odnośnie do złożoności hasła, jak przekazywać informacje, jak niszczyć dokumenty, jakie uprawnienia mogą mieć goście z zewnątrz, kto może mieć dostęp do naszego sprzętu, kogo informować w danej sytuacji itp. W dobie dużych organizacji ważne jest także, aby była co najmniej jedna osoba na określony obszar, która wie, jakie osoby mogą się znajdować wewnątrz tegoż obszaru i kto nie powinien się tam znaleźć. Pozwala to wychwycić intruzów, którzy dostali się tam, wykorzystując luki w tym właśnie zakresie.

Podsumowanie i rady

Powyższe informacje na temat najczęściej spotykanych metod ataków i obrony przed nimi to jedynie mały skrawek wiedzy, która łączy elementy wiedzy o sterowaniu zachowaniem ludzi z elementami wiedzy typowo informatycznej, pozwalającej na przygotowanie narzędzi ataku. Jak każdy inny atak, zależy on w głównej mierze od wiedzy i zdolności przestępcy do jej wykorzystania. Nie można oczywiście dać się zwariować i podejrzewać każdego, ponieważ w normalnym życiu i pracy nie ma po prostu na to czasu, a czasami może być to wręcz niewłaściwie odebrane przez otoczenie. Niemniej jednak znajomość tego tematu staje się istotnym elementem spokojnego życia i pracy.

ZAKOŃCZENIE

Dziękuję Ci, droga Czytelniczko, drogi Czytelniku, że dotarliście do końca tej książki. Mam szczerą nadzieję, że tematy przeze mnie w niej poruszane Was zaciekawiły, być może zdziwiły albo (co chyba najważniejsze) skłoniły do zajrzenia głębiej w tematykę wywiadu otwartoźródłowego, czyli OSINT-u. Jest to tematyka bardzo rozległa i zmieniająca się tak szybko, jak szybko zmienia się środowisko w Internecie. Codziennie powstają nowe strony i narzędzia, wymyślane są nowe techniki poszukiwania informacji w sieci, ale także znikają strony i wyłączane są dostępy do serwisów, co stale zmusza nas do wysiłku i poszukiwania nowych rozwiązań.

Chyba najczęstszym pytaniem, z jakim się spotykam w związku ze szkoleniami, które prowadzę, jest pytanie „Czy znajomość OSINT-u jest aktualnie ważną umiejętnością?". Odpowiedź będzie oczywiście twierdząca, nie tylko dlatego, że osobiście uważam ten obszar wiedzy za ciekawy, ale także dlatego, że widzę jego użyteczność w codziennym życiu, zarówno zawodowym, jak i osobistym. Niezależnie od tego, czy poszukujemy mieszkania lub domu i chcemy dowiedzieć się, gdzie nieruchomość ta jest zlokalizowana wyłącznie na podstawie zdjęć, czy pragniemy zapewnić sobie większy komfort działań w Internecie poprzez weryfikację „śladu", jaki zostawiamy w sieci, czy też chcemy przeprowadzić rozpoznanie internetowe w pracy w ramach zabezpieczania infrastruktury IT albo działań biznesowych, to zawsze OSINT będzie jednym z podstawowych elementów naszego działania.

Rynek pracy dla osób posiadających umiejętności OSINT-owe stale się zwiększa i z każdym rokiem takie umiejętności będą coraz bardziej pożądane przez pracodawców.

Umiejętność rozpoznawania i weryfikowania prawdziwości informacji, które w coraz większej mierze przekazywane są przez Internet, staje się elementem naszego codziennego życia – i w tym aspekcie także zdolność do krytycznego myślenia i znajomość technik analizy danych będzie nam pomagać w budowaniu pełnego obrazu otaczającego nas świata.

OSINT to także ogromna możliwość ćwiczenia swoich „szarych komórek" poprzez różnego rodzaju quizy i konkursy, co może spowodować, że pasja do tego rodzaju działań będzie łączyła się z miłym spędzaniem czasu.

Chciałbym na koniec podziękować wszystkim, którzy przyczynili się do powstania zarówno tekstów źródłowych (inspirując mnie do pisania, podrzucając pomysł oraz sprawdzając moje teksty), jak i całej tej książki, która także wymagała nie lada wysiłku od wielu osób. Dziękuję również Czytelnikom portalu *sekurak.pl*, którzy czytali moje artykuły i reagowali na nie. Jesteście wszyscy inspiracją dla mnie do dalszej pracy.

Do „zobaczenia" w kolejnych publikacjach!

1 C-SPAN, *Director Comey Remarks at Intelligence and National Security Alliance Dinner*, March 29, 2017.
2 Feinberg A., *This Is Almost Certainly James Comey's Twitter Account*, Gizmodo, March 30, 2017.
3 Wosiński K., *Jak wyszukiwarki radzą sobie z analizą zawartości obrazów – OSINT hints*, sekurak.pl, 8 marca 2021.
4 Techjournalist, *Finding people with their faces*, Medium, March 5, 2024.
5 Google for Developers, *Rozmiar obrazu*, ostatnia aktualizacja: 6 sierpnia 2024.
6 Sector035, *Getting a Grasp on GoogleID's*, Medium, December 3, 2019.
7 Cymbor P., *Ukrainiec nie mierzył z broni do przechodniów we Wrocławiu*, FakeNews.pl, 27 listopada 2023.
8 InVid, *InVID Verification Plugin.*
9 Sherlock Projekt, *Sherlock,* GitHub.
10 Hoffman N. (WebBreacher), *WhatsMyName.*
11 Euronews, *Lithuania opens doors of alleged former CIA secret prison*, January 10, 2022.
12 GCHQ, *GCHQ Reveals Secret London Site*, April 5, 2019.
13 Wittmann L., *Bundesservice Telekommunikation – wie ich versehentlich eine Tarnbehörde in der Bundesverwaltung fand*, Medium, 12. Januar 2022.
14 Źródło: The Wayback Machine.
15 Wittmann L., *Hmm. Ob der "Bundesservice Telekommunikation"…*, Twitter, 5. November 2021.
16 The Wayback Machine, Adressen der Bundesverwaltung.
17 The Wayback Machine, Bundesservice Telekommunikation (BST).
18 Wittmann L., *Bundesservice Telekommunikation – enttarnt: Dieser Geheimdienst steckt dahinter*, Medium, 24. Januar 2022.
19 RIPE Database, RIPE Database Query.
20 Jung T., *Nach Recherchen von @LilithWittmann ist der "Bundesservice Telekommunikation" eine ominöse Behörde…*, Twitter, 17. Januar 2022.
21 Wosiński K., *YouTuber wysłał lokalizator Apple AirTag do króla Niderlandów*, sekurak.pl, 18 października 2021.
22 Państwowy Instytut Medyczny MSWiA, *Oświadczenie CSK MSWiA w związku z publikacją zamieszczoną na stronie onet.pl pt. „Jacek Kurski miał koronawirusa. Mimo to poleciał na Eurowizję Junior"*, gov.pl, 24 grudnia 2021.
23 *Caso Djokovic, desde el punto de vista OSINT*, Parekh A., 12 enero 2022 [strona dostępna już jedynie w archiwum Internetu].
24 Institute of Public Health of Serbia "Dr Milan Jovanovic Batut", Covid-19 Validation, Novak Djoković, Confirmation code 7320919-259039, December 12, 2021.
25 Institute of Public Health of Serbia "Dr Milan Jovanovic Batut", Covid-19 Validation, Novak Djoković, Confirmation code 7371999-259039, December 16, 2021.
26 Hoppenstedt M., Meyn J., *New Inconsistencies in the Novak Djoković Case. Were the Results of a Positive PCR Test Manipulated?*, „Der Spiegel", January 11, 2022.
27 Źródło: pcr.euprava.gov.rs, za: „Der Spiegel" [zasób już niedostępny – przyp. red.].
28 Źródło: pcr.euprava.gov.rs [zasób już niedostępny – przyp. red.].
29 grujicd, *This is very sad…*, Hacker News, January 11, 2022.
30 *Affidavit of Novak Djokovic* sworn on 10 January 2022 [zasób już niedostępny – przyp. red.].
31 *Affidavit of Natalie Bannister* filed 8 January 2022 [zasób już niedostępny – przyp. red.].
32 Djokovic N., *An honor to receive…*, Twitter, December 17, 2021.
33 Post of Serbia, Postage stamp for the best one – Novak Đoković, December 16, 2021.
34 Trace Labs, *Crowdsourced OSINT to Find Missing Persons*.
35 Australian Centre to Counter Child Exploitation, *Stop Child Abuse – Trace An Object*.
36 Bellingcat, *New MH17 Photograph Geolocated to Donetsk*, October 20, 2017.
37 Aidarbekova A., *Launching an Open Source Flight Database for Kazakhstan in Wake of Protests*, Bellingcat, January 8, 2022.
38 Sajdak M., *Włoski boss mafii aresztowany po ~20 latach ukrywania się. Zdradziło go zdjęcie na Google Street View…*, sekurak.pl, 6 stycznia 2022.
39 BBC, *Google Maps shows sunken car where missing man's body was found*, September 12, 2019.
40 Giuffrida A., *Mafia fugitive caught after posting YouTube cooking video*, „The Guardian", March 29, 2021.
41 Renaud J., *Missouri teachers' Social Security numbers at risk on state agency's website*, „St. Louis Post-Dispatch", October 14, 2021.
42 NU.nl, *Website die verkiezingsuitslagen in gemeenten toonde offline gehaald*, 17 maart 2021.
43 Cronjé J., *Exclusive: Indian IT guru linked to fake WMC sites*, News24, July 26, 2017.
44 NOAASatellites, *Tongan Eruption Ripples Around the Globe, YouTube*, January 26, 2022.

45 Guardian News, *Tsunami From Volcanic Eruption Damages Harbor In Santa Cruz*, YouTube, January 18, 2022.
46 Human Rights Watch, *Burma: Scores of Rohingya Villages Bulldozed. New Satellite Images Show Destruction Indicating Obstruction of Justice*, February 23, 2018.
47 Blanton T., Willard E., *Srebrenica Conference Documents Detail Path to Genocide from 1993 to 1995*, The National Security Archives, July 1, 2015.
48 Źródło: ICTY; U.S. National Geospatial Intelligence Agency/National Security Archives.
49 Myanmar Witness, *Arms being sent to Myanmar from Russia*, January 24, 2022.
50 Stockholm International Peace Research Institute (SIPRI), *SIPRI Arms Transfers Database*.
51 Britton B., Mulligan M., *Search for clues about Putin's Ukraine plans turns to unlikely source: TikTok*, NBC News, January 28, 2022.
52 Castel B., *How to VERIFY a VIDEO? | #1 Worm in eye*, YouTube, November 11, 2021.
53 0xjomo, *#OSINT / #OPSEC tip: Photos in PDFs are quite often just JPEGs embedded*, Twitter, February 6, 2022.
54 LuganskInformTsentr Z, *Zayavleniye glavy LNR Leonida Pasechnika*, Telegram, 18 fewrala 2022.
55 Pushilin D.W., Telegram.
56 Toler A., *Head of the LNR posted a video…*, Twitter, February 18, 2022.
57 Higgins E., *Metadata shows pro-Russian separatists filmed evacuation video…*, Twitter, February 18, 2022.
58 Wosiński K. (seintpl), *Camera filename patterns*, GitHub.
59 Strick B., *A good reminder…*, Twitter, December 19, 2022.
60 *Legality* [w:] *China, Wikipedia, the Free Encyclopedia*.
61 *System odniesienia WGS 84* [w:] *Wikipedia, wolna encyklopedia*.
62 Tate A., *Hello @GretaThunberg…*, Twitter, December 27, 2022.
63 Thunberg G., *Yes, please do enlighten me…*, Twitter, December 28, 2022.
64 Tate A., *Thank you…*, Twitter, December 28, 2022.
65 Caraballo A., *Romanian authorities…*, Twitter, December 29, 2022.
66 Cymbor P., *Pudełko po pizzy nie przyczyniło się do aresztowania Andrew Tate'a*, fakenews.pl, 1 stycznia 2023.
67 Tate A., *Romania*, Twitter, December 25, 2022.
68 Conspirador Norteño, *It's 2023…*, Twitter, January 11, 2023.
69 X Help Center, *About profile labels and checkmarks on X*.
70 Makowski M., *Ciekawy przypadek porwania domeny perl.com*, sekurak.pl, 16 lutego 2021.
71 Richardson T., *Microsoft forgets to renew hotmail.co.uk domain*, The Register, November 6, 2023.
72 Źródło: Right Said Fred, *Bots 'R' Us*, Twitter, July 27, 2021.
73 Castel B., *Be aware of SCAM-accounts…*, Twitter, February 8, 2023.
74 Vox Ukraine, FAKE: *Video of the destruction of Russian military equipment near Kharkiv*, May 20, 2022.
75 Marchant de Abreu C., *Video game clip falsely shared as NATO military convoy being destroyed in Ukraine*, France 24, October 24, 2022.
76 Bohemia Interactive, *Arma 3 footage being used as Fake News*, YouTube, November 28, 2022.
77 Info ou Intox – France 24, *Pologne…*, Twitter, February 9, 2023.
78 Behr M., *DuckDuckGo Ends Microsoft Tracking Agreement*, Digit News, August 8, 2022.
79 Dekens N., *10 Minute Tip: Viewing LinkedIn Profiles Anonymously*, YouTube, February 7, 2022.
80 Sangwan S., *Using Shadows & Sun's Position for OSINT*, Medium [strona dostępna już jedynie w archiwum Internetu.].
81 walnut, *OSINT challenge*, Medium, February 5, 2024.
82 Harris S. (Nixintel), *Using Flight Tracking For Geolocation – Quiztime 30th October 2019*, nixintel.info.
83 Grozev Ch., *The Remote Control Killers Behind Russia's Cruise Missile Strikes on Ukraine*, Bellingcat, October 24, 2022.
84 Toler A., *How we Geolocated a Photo of a Russian Missile Programming Team*, Bellingcat, October 28, 2022.
85 Strick B., *Reflection-assisted geolocation…*, Twitter, January 4, 2023.
86 Jenkins R., Kerr C, *Identifiable Images of Bystanders Extracted from Corneal Reflections*, ResearchGate, December 2013; zob. też: Long Y. i in., *Private Eye: On the Limits of Textual Screen Peeking via Eyeglass Reflections in Video Conferencing*, arXiv:2205.03971, v3 [cs.CR], January 16, 2023.
87 Wosiński K. (seintpl/SEINT_pl), *Geolocation Analysis Diagram Outside clues*, GitHub.
88 Źródło: materiały własne Autora: Wosiński K. (seintpl/SEINT_pl), *Useful OSINT hints and links*, GitHub.
89 Ludwig, *I Forced the Best Geoguessr Player in the World to Play Blind*, YouTube, June 21, 2022.
90 Sements V. (vitaliysements), *Thanks to technology…*, Instagram, April 14, 2022.
91 Wosiński K., *YouTuber wysłał lokalizator Apple AirTag do króla Niderlandów*, sekurak.pl, 18 października 2021.

92 Motolko.Help, *Hajun Project published the data of Russian marauder soldiers, who may be involved in crimes on the territory of Ukraine*, April 4, 2022.
93 Smol W., *Shodan, czyli Google dla urządzeń sieciowych*, sekurak.pl, 18 lutego 2013.
94 Sajdak M., *Shodan dostępny dożywotnio za $1 – można kupić przez najbliższe ~24h*, sekurak.pl, 23 listopada 2019.
95 Mr Ghostly, *The numerous routes of fitness…*, Twitter, January 29, 2018.
96 Cox J., *AllTrails Data Exposes Precise Movements of Former Top Biden Official*, Vice, March 8, 2023.
97 Źródło: Twitter, Offensive OSINT.
98 Thompson S.A., Warzel Ch., *How to Track President Trump*, „The New York Times", December 20, 2019.
99 Reddit, *FindBostonBombers*, The Wayback Machine.
100 La Razón, *@larazon_es publicó ayer por error una foto de @Veeren_Jubbal confundiéndole…*, Twitter, 15 de noviembre de 2015.
101 Sluzhba bezpeky Ukrayiny, *Peredawajte informaciju pro okupantiw, a ne publikujte dani pro zsu czy rezul'taty worożych obstriliw*, Facebook, 21 bereznia 2022 r.
102 Federal Bureau of Investigation, *U.S. Capitol Violence*.
103 Federal Bureau of Investigation, *Pipe Bombs in Washington*, D.C., January 5, 2021.
104 FirefighterNation, *Retired Chicago Firefighter Wrongly Accused of Participating in Capitol Violence*, January 18, 2021.
105 SekurakTV, *Radio SDR – podstawy i zastosowania*, YouTube, 17 kwietnia 2020.
106 jetvision, *RTL1090 Installation and Operating Manual*, last revised: May 19, 2013.
107 mxrch, *GHunt*, GitHub.
108 Bewarder M., Flade F., Milling P., *Mutmaßlicher Verrat beim BND. Spione und Diamanten*, tagesschau, 2. Februar 2023.
109 Fake PhD Investigator, *1/x Great use…*, Twitter, February 2, 2023.
110 Zob. np. Wnękowicz M., *Rekonesans infrastruktury IT – część 1 (google hacking)*, sekurak.pl, 17 lipca 2018.
111 Niseki M. (ninoseki), *Mitaka*, GitHub.
112 Takahashi D. (HASH1da1), *Gotanda*, GitHub.
113 OpenAI, *Introducing ChatGPT*, November 30, 2022.
114 Zob. Clark E., *The 10 Best AI Content Detector Tools*, "Forbes", December 14, 2023; Undetectable AI: *Advanced AI Detector and Humanizer*.
115 SANS Cyber Defense, *The New OSINT Cheat Code: ChatGPT*, YouTube, April 6, 2023.
116 Quiztime, *Verif!cation Quiz Bot*, Twitter, August 10, 2018.
117 Wyszukiwarka Google, *Szybsze i prostsze znajdowanie informacji dzięki przeglądowi od AI w wyszukiwarce Google*, https://support.google.com/websearch/answer/14901683
118 Cylect, https://cylect.io
119 Phind, https://www.phind.com
120 Perplexity, https://www.perplexity.ai
121 Microsoft, Copilot, https://copilot.microsoft.com
122 ChatGPT, https://chatgpt.com
123 DeepSeek, https://chat.deepseek.com
124 AI, OSINT, https://chatgpt.com/g/g-aZQ1x6vqB-ai-osint
125 Zubic E., Intel Assistant, https://chatgpt.com/g/g-LEs2Ed8aV-intel-assistant
126 CQCore, *AI-Resources*, GitHub, https://github.com/The-Osint-Toolbox/AI-Resources
127 Google, Notebook LM, https://notebooklm.google
128 BlipCuy, AI Video Translator, https://videotranslator.blipcut.com
129 Reddit, *My cheese slides off the pizza too easily*, https://www.reddit.com/r/Pizza/comments/1a19s0/my_cheese_slides_off_the_pizza_too_easily/
130 Źódł: Sutton G., *Please don't get your campsite setup ideas from AI…*, Facebook, July 2, 2024, https://www.facebook.com/groups/vwcampervanownersclub/posts/1535152057079114/
131 Originality.ai, AI Detector, https://originality.ai/ai-checker
132 r/exchristian, *Book of Genesis written by an artificial intelligence according to AI detection tools, I found this both hilarious and intriguing*, Reddit, 2023, https://www.reddit.com/r/exchristian/comments/13plh5t/book_of_genesis_written_by_an_artificial/
133 Johnson A., *Google's AI 'Reimagine'tool helped us add wrecks, disasters, and corpses to our photos*, The Verge, August 21, 2024, https://www.theverge.com/2024/8/21/24224084/google-pixel-9-reimagine-ai-photos – dostę 30.06.2025 r.
134 Koltai K., *Don't Get Scammed! Tips For Spotting AI-Generated Fake Products Online*, Bellingcat, March 2025, 2025, https://www.bellingcat.com/resources/2025/03/25/detecting-ai-products/

135 Anthropic, *Operating Multi-Client Influence Networks Across Platforms*, April 2025, https://cdn.sanity.io/files/4zrzovbb/website/45bc6adf039848841ed9e47051fb1209d6bb2b26.pdf

136 Picarta, https://picarta.ai

137 Dekens N. (Dutch OSINT Guy), *The Slow Collapse of Critical Thinking in OSINT due to AI*, dutchosintguy.com, April 2, 2025, updated: April 9, 2025, https://www.dutchosintguy.com/post/the-slow-collapse-of-critical-thinking-in-osint-due-to-ai

138 Cluley G., Mastodon: *What you need to know for your security and privacy*, grahamcluley.com, November 8, 2022.

139 Krebs B. (briankrebs), *Welp, that didn't last long…*, Twitter, November 8, 2022.

140 Sector035, *Extra Mastodon #OSINT tip for today!*, Twitter, November 7, 2022.

141 Wosiński K. (SEINT_pl), *Short links verification cheatsheet*, GitHub.

142 Źródło: *OSINT Combine*.

143 Sinwindie, *Make Your Own Custom OSINT Bookmarklets (p1)*, secjuice, Feb 16, 2020.

144 Suslikov E. (susbox), *FireShot: Full Web Page Screenshots*, Mozilla.

145 Chrome Web Store, *Zrób pełny, całkowity zrzut ekranu strony internetowej – FireShot*.

146 Microsoft, *Dodatki do przeglądarki Edge*.

147 Mozilla, *Nimbus Screen Capture: Screenshot, Edit, Annotate*.

148 Chrome Web Store, *Nimbus Screenshot & Screen Video Recorder*.

149 Chrome Web Store, *Screenity – Nagrywarka & Edytor adnotacji*.

150 *[AKTUALIZACJA #6] Wyciekły dane osobowe ponad 20 000 policjantów, strażaków, celników, pograniczników i innych*, Niebezpiecznik, 20 kwietnia 2021.

151 Sajdak M., *Znalazł publicznie dostępną bazę z danymi prawie wszystkich obywateli Austrii. Służyła do namierzania osób uchylających się od płacenia abonamentu RTV*, sekurak.pl, 26 stycznia 2023.

152 Źródło: Postma F., *US Soldiers Expose Nuclear Weapons Secrets Via Flashcard Apps*, Bellingcat, May 28, 2021.

153 Źródło: Davies C., *Prince William photos offer insight into RAF working life*, The Guardian, November 20, 2012.

154 Leppard D., *China bugs and burgles Britain*, "The Sunday Times", January 31, 2010.

securitum WYDAWNICTWO

Książki **Securitum** to owoc 15 lat doświadczeń w branży szkoleń i pentestów

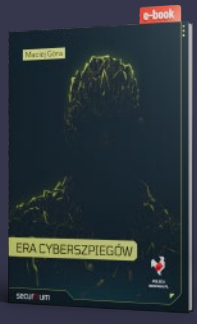
- wiedza, którą dzielą się polscy specjaliści
- spojrzenie na omawiane zagadnienia okiem praktyka
- problemy z codziennej pracy wyjaśniane przez fachowców
- prosty przekaz, dla każdego zainteresowanego bezpieczeństwem IT

e-booki

Adam Samson
Bezpieczeństwo domowego routera Wi-Fi. Wprowadzenie

Krzysztof Wosiński
OSINT: nowy wymiar poszukiwań w sieci

Maciej Góra
Era cyberszpiegów



Robert (ProXy) Kruczek
Socjotechnika w praktyce. Triki i kruczki hackowania ludzi

wydawnictwo.securitum.pl