
IDENTYFIKUJEMY I BLOKUJEMY OSZUSTWA ORAZ NADUŻYCIA MARKETINGOWE TYPU

NIEPRAWIDLOWE KLIKI I LEADY

# Specyfikacja Techniczna Rozwiązania

# Description of Methodology

www.trafficwatchdog.pl

Spark DigitUP Sp. z o.o.

Plac Wolnica 13 lok. 10

31-060 Kraków

NIP 6762496391

TrafficWatchdog

# 1. System TrafficWatchDog (TwD) – opis realizowanych funkcjonalności

TrafficWatchDog (TwD) – system działający w zakresie wykrywania oszustw oraz nadużyć marketingowych online/mobile dla form reklamowych typu: KLIK oraz LEAD. TwD zbiera i analizuje parametry klika i/lub leada (dane bezosobowe) z poszczególnych płatnych źródeł i na podstawie zebranych parametrów dokonuje oceny klika/leada:

1) CLICK Scanner – identyfikacja 'nieprawidłowych klików' zgodnie ze standardami IAB - Interactive Advertising Bureau Click Measurement Guidelines: "Invalid Clicks arising from suspected “click fraud” are a sub-component of Invalid Clicks and originate from a user, program or automated agent (e.g., Internet robot or spider) that accesses a URL for the purpose of manipulating click measurement activity or click-based advertising payments, having no intention of legitimately browsing site content, making a purchase or performing any other type of legitimate conversion action. Suspected click fraud can arise from both human-initiated and application-initiated automated activity; also, suspected click fraud can arise from invalid Ad Impression activity. Click Fraud also includes situations where a user is unwillingly, or tricked into, accessing information(for example, user “virus” infected activity, or auto-clicking functions)."

2) GOOGLE ADS Scanner – identyfikacja 'nieprawidłowych klików' w kampanii Google Ads, zgodnie ze standardami IAB - Interactive Advertising Bureau Click Measurement Guidelines: "Invalid Clicks arising from suspected “click fraud” are a sub-component of Invalid Clicks and originate from a user, program or automated agent (e.g., Internet robot or spider) that accesses a URL for the purpose of manipulating click measurement activity or click-based advertising payments, having no intention of legitimately browsing site content, making a purchase or performing any other type of legitimate conversion action. Suspected click fraud can arise from both human-initiated and application-initiated automated activity; also, suspected click fraud can arise from invalid Ad Impression activity. Click Fraud also includes situations where a user is unwillingly, or tricked into, accessing information(for example, user “virus” infected activity, or auto-clicking functions)."

   System Google Ads Scanner - dodatkowo pozwala automatycznie blokować wyklikiwanie reklam Google Ads Klienta przez tych samych użytkowników oraz blokować nieprawidłowe kliki w kampaniach Google Ads Klienta.

3) LEAD Scanner – identyfikacja ‘nieprawidłowych leadów’ zgodnie ze standardami IAB - Interactive Advertising Bureau Online Lead Generation: "Lead fraud occurs when leads are submitted with malicious intent or simply for financial gain. These leads should be deemed invalid, and advertisers and agencies should not pay for these leads. Although uncommon, there have been cases when offers are filled out by an artificial, automated system to generate a large quantity of leads. Consumers or companies may also fraudulently fill out offers."

Główne realizowane funkcjonalności:

1. Pełny monitoring 24/7 wszystkich źródeł dostarczających płatne kliki/leady dla Klienta.
2. Automatyczna analiza reklam i klików w Google Ads.
3. Wykrywanie i analiza urządzenia użytkownika – na podstawie tzw. wirtualnego odcisku urządzenia (DEVICE FINGERPRINT).
4. Identyfikacja kraju pochodzenia klika/leada i dostawców IP.
5. Automatyczne blokowanie wyklikiwania reklam w Google Ads przez podejrzane/fruadowe adresy IP.
6. Automatyczne blokowanie wyklikiwania reklam w Google Ads przez podejrzane/fraudowe urządzenia (identyfikacja DEVICE FINGERPRINT).
7. Automatyczne blokowanie wyklikiwania reklam w Google Ads przez podejrzane/fraudowe 'cookie'.
8. Możliwość ustawienia i dopasowania indywidualnych reguł automatycznego blokowania wyklikiwania kampanii Google Ads.
9. Raporty reklamacyjne nieprawidłowych klików oraz leadów dla źródeł dostarczających płatne kliki/leady.
10. Raport reklamacyjny nieprawidłowych klików dla Google Ads.
11. Cykliczne raporty wysyłane na wskazany adres e-mail.
12. Informacje szczegółowe dla każdego zweryfikowanego klika/leada – w tym analiza zachowania potencjalnego użytkownika/bota na monitorowanej stronie.
13. Dostęp online do Panelu Klienta.

# 2. Architektura techniczna rozwiązania TwD

System składa się z następujących komponentów:

1) Skrypt trackingowy TwD – aplikacja odpowiedzialna za zbieranie parametrów służących ocenie w zakresie klików/leadów.
2) Webservice – aplikacja instalowana na serwerze TwD, do której będą przesyłane dane zebrane przez skrypt
3) Baza danych
4) Serwer
5) AI - sieć neuronowa dokonująca analizy danych
6) Panel Klienta – front Klienta w zakresie prezentacji wyników działania systemu TwD.

# 3. Sposób działania kodów TwD

Działanie dedykowanych kodów trackingowych jest dopasowane do struktury docelowej monitorowanej strony www Klienta - na której implementowane są przygotowane odpowiednie fragmenty kodów HTML zawierające skrypty Javascript oraz pixele, które optymalnie, jeżeli umieszczone będą we wskazanych miejscach docelowych monitorowanego serwisu – bezpośrednio w kodzie monitorowanej strony (tzw. 'body' strony). Skrypty są wykonywane tylko i wyłącznie po stronie usera w jego przeglądarce.

Implementacja przygotowanego kodu trackingowego Javascript/pixeli na docelowej monitorowanej stronie Klienta, może odbywać się również poprzez system GTM (Google Tag Manager). Skrypty są

wykonywane tylko i wyłącznie po stronie usera w jego przeglądarce. W przypadku implementacji kodów TwD za pomocą GTM - wczytanie kodów TwD będzie uzależnione od obsługi przez przeglądarkę usera GTMa (niektóre wersje przeglądarek - blokują GTMa). Może to oznaczać 'straty' w zakresie liczby monitorowanych klików/leadów.

Skrypty i elementy kodu TwD uruchamiają się w trakcie ładowania strony www. Działają również w tle, w trakcie pracy usera na stronie www korzystając z obsługi zdarzeń, generowanych przez elementy strony www. Dane wysyłane przy wysyłaniu wypełnionego formularza (lead) metodą POST lub metodą GET w przypadku zamieszczenia obrazka na stronie.

Dane przesyłane są na docelowy serwer, gdzie poddawane są analizie. Wyniki analizy są dostępne w dedykowanym panelu Klienta serwisu TrafficWatchDog.

# 4. Techniczna implementacja kodów TwD

Na proces wdrożenia i architekturę systemową składają się poniższe elementy:

Po stronie TrafficWatchDog:

1. Dewelopment docelowego kodu TwD (pliku Javascript/pixele) - odpowiedzialnego za zbieranie danych, dopasowanego do specyfikacji monitorowanej strony www
2. Webservice – uruchomienie aplikacji instalowanej na serwerze TrafficWatchDog, do której będą przesyłane za pomocą protokołu HTTPS zebrane informacje przez kod TwD
3. Serwer – zapis zebranych parametrów oceny
4. Siec neuronowa - kalibracja modelu i algorytmów analizy danych i oceny rekordów
5. Wystawienie dedykowanego panelu Klienta - w którym można analizować w trybie online wyniki analizy/tworzyć raporty reklamacyjne dla np. Adwords, itd

Po stronie Klienta – właściciela monitorowanej strony:

1. Wklejenie dedykowanego kodu TwD (Javascript/pixele) na docelową stronę www
2. Do decyzji Klienta pozostaje na które serwisy zostanie zaimplementowany kod TwD - kod może zostać umieszczony tylko i wyłącznie na wybranych stronach/tzw. mikro-site'ach, które mają być analizowane (np. wybrane kampanijne Landing Page – tzw. mikro site'y marketingowe). Strony traktowane specjalnie ze względów bezpieczeństwa, takie jak panel administracyjny Klienta, strony zakupowe lub transakcyjne mogą byc wyłączone z analizy (brak wpiętych kodów TwD).
3. W zależności od decyzji Klienta – korzystanie ze skryptu JavaScript znajdującego się na serwerze TrafficWatchDog lub umieszczenie pliku Javascript na własnym serwerze monitorowanej strony.

# 5. Wpływ kodów TwD na architekturę monitorowanej strony docelowej

Zaimplementowane kody TwD nie mają wpływu na architekturę docelowej monitorowanej strony www. Skrypty JavaScipt/pixele są wykonywane tylko i wyłącznie po stronie uzytkownika w jego

przeglądarce. Brak wpływu na user experiance w zakresie szybkości ładowania strony/itd. (testy narzędziem: https://developers.google.com/web/tools/lighthouse)

Zamieszczone skrypty w żaden sposób nie mają wpływu na ścieżkę logowania do systemów transakcyjnych Klienta/itd

# 6. Bezpieczeństwo IT

Zamieszczone kody TwD na docelowej stronie www Klienta zbierają parametry, które generowane są podczas korzystania ze strony www. Należy zaznaczyć, że dane są zbierane anonimowo, nie jest możliwe skojarzenie ich z konkretnym użytkownikiem po stronie dostawcy aplikacji TwD.

Wszelkie dane są przekazywane i przechowywane na wewnętrznych serwerach TwD – stosowane są wielopoziomowe zabezpieczenia. Między uruchomionym skryptem w przeglądarce użytkownika a serwerem zbierającym dane, komunikacja odbywa się szyfrowanym kanałem HTTPS ( SSL TLS 1.2 z 2048 bitowym kluczem). Następnie dane są przetwarzane na serwerze aplikacyjnym, który jako jedyny ma bezpośrednie połączenie z publiczną siecią Internet. Jest on zabezpieczony firewallem Stateful Packet Inspection (SPI) z Login/Intrusion Detection i zabezpieczeniem przed atakami typu BruteForce. Po przetworzeniu dane są składowane w wewnętrznej bazie danych, do której jest dostęp wyłącznie z wewnętrznej sieci. Logowanie do wszystkich serwerów jest wyłącznie za pomocą indywidualnych 4096 bitowych kluczy RSA.

Zastosowane standardy wdrożeń w normie dotyczącej technik bezpieczeństwa PN-ISO/IEC 27002:2014-12 w zakresie organizacji bezpieczeństwa informacji, kontroli dostępu, kryptografii oraz bezpieczeństwa komunikacji.

# 7. Analizowane kategorie parametrów

Kategorie analizowanych parametrów:

I. Dane URL
II. Dane wizyty
III. Parametry IP
IV. Parametry przeglądarki + Fingerprint przeglądarki
V. Parametry systemu
VI. Parametry urządzenia + Fingerprint urządzenia
VII. Parametry user bahavioral
VIII. Obsługa skryptu
IX. Parametry Google reCaptcha v.3 (opcjonalnie)
X. Dane sesji

# 8. Analizowane parametry – benchmark

Przykładowe parametry pobierane przez kody monitorujące TwD. W celu zabezpieczenia bezpieczeństwa procesów monitoringu TwD przed naruszeniem lub próbami obejścia – nie jest prezentowana pełna lista monitorowanych parametrów w poszczególnych badanych obszarach.

## Dane url/strony i wizyty

- url strony
- elementy na stronie
- wczytywanie danych strony

- obsługa cookies
- identyfikatory wizyt
- liczba odwiedzin

- czas przesyłania danych
- odświeżanie strony

## Analiza IP

- identyfikacja dostawcy internetu ISP
- geo-lokalizacja
- identyfikacja połączenia – proxy, VPN, sieć TOR, infrastruktura centrum danych
- sieć GSM
- WebRTC z lokalnymi numerami IP

## Parametry przeglądarki

- nazwa przeglądarki
- wersja przeglądarki
- user agent
- silnik przeglądarki

- obsługa błędów
- obsługa funkcji

- rozmiar okna
- zainstalowane wtyczki

## Parametry systemu

- nazwa systemu
- wersja systemu

- rozdzielczość
- ustawienia obrazu
- ustawienia systemu

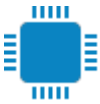
- zestaw czcionek

## Parametry urządzenia

- mikrofon
- głośniki
- karta dźwiękowa

- kamera
- WiFi
- bluetooth

- położenie urządzenia



- procesor
- platforma

- rodzaj ekranu

## Fingerprint urządzenia

- Unikalny identyfikator pozwalające określić unikalność urządzenia

## Fingerprint przeglądarki

- Unikalny identyfikator pozwalające określić unikalność przeglądarki
- Audio context fingerprint
- Canvas Fingerprint

## User behavioral analysis

- współrzędne kursora

- scroll

- rodzaj i liczba klawiszy

- czas zdarzeń na stronie
- interakcja z elementami

- czas na polach formularza
- liczba znaków w polach
- obsługa pól

## Obsługa skryptu – site rendering

- sposób pobrania i uruchomienia skryptu
- błędy skryptu

- czas wysyłania danych
- metody wysyłania danych

- punkty kontrolne skryptu

### Google Score

- ocena Google reCaptcha v3

### Dane sesji

- Identyfikacja wizyt na podstawie identyfikatora cookie lub fingerprinta
- Liczba wizyt
- Liczba stron
- Częstotliwość i powtarzalność wizyt

# 9. Metodyka audytu kliknięć

Metodyka przeprowadzania audytu kliknięć przez system TwD - zgodnie z wytycznymi organizacji IAB (dokument „Click Measurement Guidelines", Version 1.0, Final Release May 12, 2009 [1]).

## Opis procesu audytu kliknięć

W celu przeprowadzanego audytu kliknięć oraz leadów – system TwD realizuje usługę CLICK SCANNER, GOGLE ADS SCANNER oraz LEAD SCANNER dokonując weryfikacji oraz oceny każdego odnotowanego przez system TwD klika oraz leada w zakresie potencjalnych nieprawidłowości.

System TwD działa w oparciu o technologie:

1. Analizy parametrów systemowych/przeglądarki - analiza botów/programów/scraperow podszywających się pod różne typy systemów oraz przeglądarek, które po sprawdzeniu nie pasują do atrybutów danego typu systemu lub przeglądarki. Weryfikacja bot-lists.
2. Identyfikacji zaawansowanych narzędzi automatyzacji przeglądarek takich jak Selenium i PhantomJS.
3. Device Fingerprinting – unikalne identyfikatory urządzeń
4. Canvas Fingerprinting – unikalne identyfikatory przeglądarek
5. Machine learning – klasyfikatory oraz algorytmy sztucznej inteligencji.
6. Bot 'honeypots' – 'pułapki' identyfikujące działające na stronie boty.
7. User behavioral analysis (UBA) - analiza behawioralna w celu identyfikacji nienaturalnych wzorców zachowania użytkownika na monitorowanej stronie.
8. Analiza IP - analiza geo-lokalizacji, adresów oraz dostawców IP. Identyfikacja adresów IP generowanych przez centra danych, usługi TOR, VPN, serwery proxy. Identyfikacja adresów IP znajdujących się na IP black lists.

9. Google reCAPTCHA v3 API – identyfikacja zachowania typu bot vs człowiek.
10. Analiza danych wizyt – analiza parametrów URL, plików cookie.
11. Tamper proofing - algorytmy ‘proof of work’ wykonujące zadania, możliwe do zrealizowania w czasie naturalnego korzystania z przeglądarki.
12. Site rendering monitoring - analiza obsługi skryptów JavaScript na monitorowanej stronie w zakresie renderowania docelowej strony.

System TwD mierzy kliknięcia tzw. Resolved Click (patrz pkt. 2.4 [1]) występujące, gdy kliknięcie otrzymane uruchamia docelową stronę internetową Reklamodawcy lub inną stronę mającą na celu zapewnienie Reklamodawcy interakcji handlowej z potencjalnym użytkownikiem.

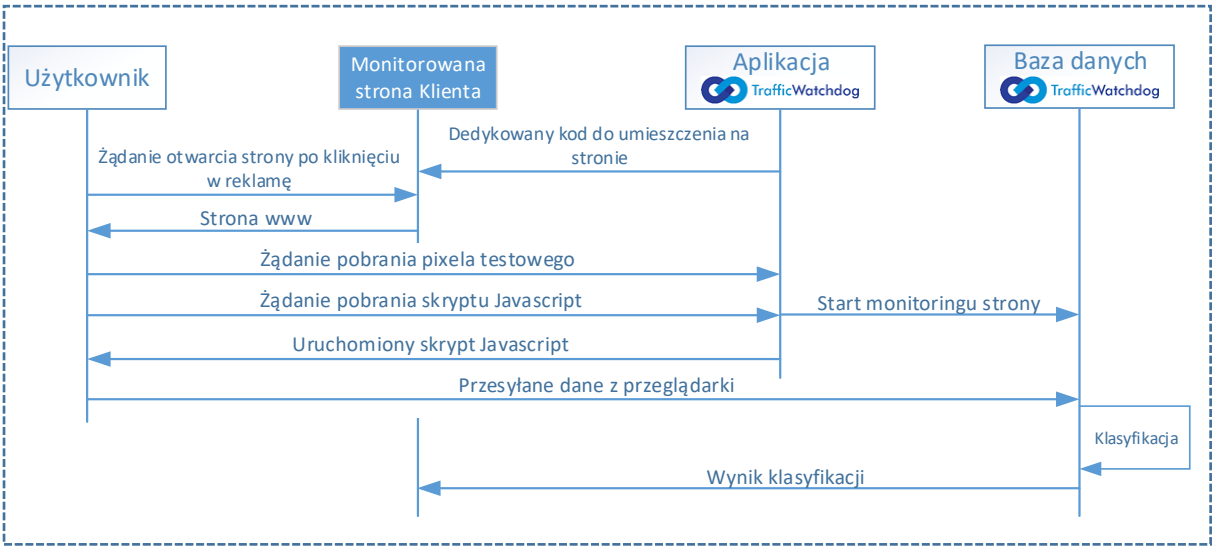
W audycie kliknięć nie są zbierane żadne dane osobowe - nie są zbierane informacje o znakach wpisywanych w formularzach zamieszczonych na stronie, itd. Nie jest analizowana treść przeglądanej przez użytkownika strony. Zebrane dane są wykorzystywane jedynie dla potrzeb klasyfikacji kliknięcia i w żaden sposób nie są łączone z konkretnym użytkownikiem (np. w celu tworzenia profilu użytkownika dla potrzeb marketingowych lub innych).

## Metodologia pomiaru klików

Kliknięcia audytowane przez system TwD obejmują jedynie wejścia ze zdefiniowanych źródeł. Zgodnie z wytycznymi zawartymi w [1] jako podstawowa metodologia liczenia przyjęta została metoda opisana jako One-Click-Per-Impression Method. Rejestracja pojedynczych kliknięć ze źródeł daje elastyczność w momencie rozliczenia pomiędzy Reklamodawca a Wydawcą. Raporty mogą być korygowane o odpowiednie przedziały czasowe liczonych kliknięć w celu uniknięcia na przykład naliczania powtórzeń w pewnych przedziałach czasowych.
Schemat przepływu danych oraz kolejno wykonywanych sekwencji od momentu przekierowania po kliknięciu zaprezentowano na wykresie poniżej:

1. Kliknięcie mierzone jest od momentu pobrania pixela testowego i pobrania skryptu JavaScript zamieszczonego na monitorowanej stronie.
2. W kolejnych krokach skrypt wykonuje się w przeglądarce użytkownika, nawiązuje połączenie z serwerem aplikacji TrafficWatchDog i zaczyna się pobieranie kolejnych danych.
3. Każda z wymienionych czynności wraz z otrzymanymi danymi jest zapisywana w bazie danych.

**Diagram przepływ danych - TwD**




Na proces pobierania i przetwarzania danych składają się następujące elementy:

1. Plik Javascript, którego zadaniem jest zbieranie danych. Skrypt jest umieszczany na monitorowanej stronie Klienta. Wcześniej jest odpowiednio dopasowany do specyfikacji monitorowanej strony www.
2. Webservice, usługa która pobiera zaszyfrowane dane zebrane przez kod Javascript umieszczony na stronie Klienta.
3. Baza danych, której zadaniem jest przechowywanie danych zgromadzonych na stronie Klienta,
4. Algorytmy klasyfikacji kliknięcia oraz AI, działają jako procesy na bieżąco analizujące i oceniające spływające dane.
4. Panel Klienta umożliwia analizę w trybie online wyniki klasyfikacji i ma możliwość generowania raportów reklamacyjnych.

Dane z monitorowanej strony klienta zbierane są na bieżąco. Kod umieszczany jest wyłącznie na wybranych przez Klientach stronach, które mają być docelowo monitorowane.
Mierzenie kolejnych odwiedzin użytkownika dokonywane jest za pomocą dwóch, niezależnych mechanizmów: informacji zawartej w pliku cookie i/lub unikalnego identyfikatora device Fingerprint [2]. Pierwsze rozwiązanie, jeżeli tylko nie zostanie wyłączone, daje możliwości bezpośredniego śledzenia obecności użytkownika. Drugie rozwiązanie stosowane jest w momencie, gdy pliki cookie z jakiś względów są wyłączone lub usuwane z przeglądarki (na przykład w celu usunięcia śladów obecności).

# Metodologia klasyfikacji klików

System TrafficWatchDog stosuje techniki klasyfikacji kliknięć bazujące na identyfikatorach, badaniu aktywności użytkownika i opracowanych wzorcach danych pobranych w trakcie aktywności użytkownika na stronie internetowej Klienta. Stosowana klasyfikacja ma na celu identyfikację nieprawidłowego kliknięcia (zgodnie z definicją stosowaną w dokumencie [1]) polegającego na uzyskaniu dostępu do adresu URL w celu manipulowania działaniami związanymi z pomiarem kliknięć lub płatnościami reklamowymi opartymi na kliknięciach, bez zasadnego zamiaru przeglądania zawartości witryny, zakupu lub wykonania innego rodzaju zasadnej konwersji. Klasyfikacja obejmuje również nadużycia związane z kliknięciem w sytuacjach, w których użytkownik nieświadomie lub w

wyniku oszustwa uzyskuje dostęp do informacji (na przykład aktywność spowodowana przez zainfekowanie wirusem lub funkcje automatycznego klikania).

Parametry monitorowane i pobierane podczas audytu kliknięcia podzielone zostały na 10 głównych obszarów podlegających poszczególnym ocenom – i składających się na finalną ocenę klika.
Lista audytowanych obszarów:

1. Sposób renderowania strony – do tego obszaru zaliczana jest analiza poprawności obsługi skryptów JavaScript oraz testowych pixeli zaimplementowanych na monitorowanej stronie. W skrypcie zastawione są również tzw. honeypots czyli 'pułapki' identyfikujące działające na stronie boty. W przypadku wykrycia nieprawidłowości w zakresie wczytywania docelowej strony Klienta – obszar zostanie sklasyfikowany jako nieprawidłowy.
2. Parametry systemowe – zbiór danych identyfikujących system operacyjny pobieranych w trakcie wykonywania skryptu JavaScript. Pobierane są również dane pozyskane z nagłówków HTTP, w szczególności z User-agent. W przypadku wykrycia niestandardowych parametrów systemowych – obszar zostanie sklasyfikowany jako nieprawidłowy.
3. Parametry przeglądarki – dane pobrane przez API JavaScript charakterystyczne dla danej wizyty na stronie internetowej. Parametry wchodzą w skład generowanego Fingerprint przeglądarki. Służą weryfikacji poprawności wpisu User-agent i możliwość jego celowej podmiany. Niestandardowe wartości parametrów lub znaczniki bota - pozwalają identyfikować boty, w tym również boty korzystające z tzw. interfejsu webdriver, czyli mechanizmu sterowania przeglądarką implementowanym m.in. w bibliotekach Selenium czy PhantomJS. Dodatkowo realizowane jest zadanie typu 'proof of work', które wykonuje zadania pozwalające zidentyfikować prawdziwą przeglądarkę.
4. User behavioral – zestaw danych zbieranych w skończonym przedziale czasu pozwalający na określenie zachowania człowieka na stronie internetowej. Analizowane są dane dostarczone z urządzeń peryferyjnych: myszy oraz klawiatury w przypadku komputerów stacjonarnych lub dotyku w przypadku ekranów dotykowych urządzeń mobilnych. Mierzone są również interwały czasowe pomiędzy wykonywanymi akcjami oraz miejsca aktywności na stronie. Zebrane parametry umożliwiają identyfikację nienaturalnego zachowania i wykluczenia człowieka jako użytkownika przeglądarki – lub potwierdzenie braku aktywności potencjalnego użytkownika na monitorowanej stronie Klienta. W przypadku wykrycia nienaturalnych wzorców zachowań potencjalnego użytkownika, braku aktywności użytkownika na monitorowanej stronie Klienta – obszar zostanie sklasyfikowany jako nieprawidłowy.
5. Parametry urządzenia – w ramach zebranych wartości parametrów dokonywane są między innymi testy związane z interfejsami canvas oraz WebGL udostępnionych w HTML 5, a także tzw. audio context i WebRTC. Część tych parametrów wpływa następnie na generowany Fingerprint urządzenia oraz wykorzystywana jest podczas analizy adresu IP.
6. Analiza adresu IP. Korzystając z zewnętrznych baz danych numerów IP identyfikowanych jest szereg danych związanych z numerem IP użytkownika przeglądarki takich jak: nazwa dostawcy internetowego czy geo-lokalizacja. Sprawdzane są również informacje związane z korzystaniem przez potencjalnego użytkownika z sieci TOR, połączenia VPN czy serwera proxy. Pozwala to na wykrycie potencjalnych nadużyć oraz zmian numerów IP w celu ukrycia śladów nadużyć.
7. Fingerprint urządzenia jest charakterystycznym identyfikatorem urządzenia generowanym z wybranych parametrów urządzenia. Dzięki unikalnej wartości pozwala na zastąpienie cookie w celu identyfikacji użytkownika. Składają się na niego m.in. Fingerprint wygenerowane w oparciu o canvas, webgl oraz audio context. W przypadku wykrycia nieprawidłowości w zakresie generowania Fingerprint urządzenia – obszar zostanie sklasyfikowany jako nieprawidłowy.
8. Fingerprint przeglądarki to unikalny odcisk palca przeglądarki wygenerowany z parametrów dostarczonych przez API przeglądarki. Wraz z Fingerprint urządzenia pozwala zastąpienie cookie i identyfikację powtarzających się kliknięć. W przypadku wykrycia nieprawidłowości w zakresie generowania fingerprinta przeglądarki – obszar zostanie sklasyfikowany jako nieprawidłowy.
9. Ocena Google Score. Wykorzystywane jest zewnętrze narzędzie Google reCAPTCHA v3 API, które pozwalają na identyfikację zachowania typu bot vs człowiek (przyjęta jest skala oceny: null – 100).

Oceny Google wskazujące na nieprawidłowy traffic – klasyfikują dany obszar oceny klika jako nieprawidłowy

10. Dane sesji. Weryfikacja poszczególnych wizyt, ich liczby, odwiedzonych stron i częstotliwości odwiedzin. W przypadku wykrycia nieprawidłowości w zakresie danych sesji – obszar zostanie sklasyfikowany jako nieprawidłowy.

W przypadku wykrycia nieprawidłowości w minimum w jednym z analizowanych 10 obszarów oceny klika - klik może zostać zakwalifikowany jako klik nieprawidłowy ze wskazaniem obszarów w którym zostały namierzone nieprawidłowe parametry.

## Raportowanie oceny klików

System TrafficWatchDog udostępnia panel administracyjny Klienta, gdzie Klient może w czasie rzeczywistym śledzić monitoring oraz oceny klików/leadów prowadzony na jego monitorowanej stronie. Parametry dostępne do podglądu oraz możliwe do uwzględnienia w wygenerowanym raporcie mogą zawierać następujące informacje:

1. Informację o klasyfikacji kliknięcia oraz wartości poszczególnych składowych składających się na ostateczny wynik.
2. Czas wejścia na stronę Klienta.
3. Numer IP, lokalizacje użytkownika, informacje o dostawcy ISP
4. Unikalny device oraz canvas Fingerprint
5. Wizualizacje user behaviorala w zakresie zachowaniu potencjalnego użytkownika na stronie.
6. Raporty klików/leadów (z obecnego dnia, zakresu dat, miesięczne itp.) z podziałem na źródła,
7. Informację o przeglądarce, systemie operacyjnym, urządzeniu
8. Wynik oceny Google Score.

W celach raportowych oraz reklamacyjnych dane są dopasowywane i przekazywane Klientom w zależności od ich potrzeb (struktura i zakres raportów TwD). Strony Klientów mogą być dodatkowo monitorowane w zakresie poprawności wywołań po kliknięciu w docelowy link do strony Klienta - znajdujący się na stronie wydawców. Kliki testowe zostaną oznaczone jako kliki nieprawidłowe w raportach dla Klienta. Dane gromadzone podczas monitoringu kliknięć przechowywane są min. przez 3 miesiące wliczając w to badany miesiąc.

## Materiały dodatkowe

[1] Interactive Advertising Bureau, “Click Measurement Guidelines”, Version 1.0 - Final Release May 12, 2009