

Jak powstała jedna obserwacja

PRZYKŁAD. Sporządzony dla prawdziwej obserwacji naszej własnej domeny machinewitness.eu, z jej rzeczywistymi parametrami, tym samym narzędziem co każdy opis. Jest opublikowany jako przykład i dlatego nie jest podpisany. Zamówiony opis sporządzamy dla wskazanej przez Państwa obserwacji, sprawdzamy i podpisujemy.

1. Przedmiot niniejszego opisu

Niniejszy opis przedstawia, jak powstała jedna obserwacja: adres <https://machinewitness.eu/robots.txt> w dniu **2026-09-28** (UTC), pobrany niezależnie przez 2 świadków. Wyjaśnia metodę z rzeczywistymi parametrami tej obserwacji, przedstawia każdy krok tak, by osoba trzecia mogła go powtórzyć bez nas, i wymienia zarzuty zwykle podnoszone wobec metody. Nie mówi nic o pobranej treści ani o żadnej sprawie, w której jest ona wykorzystywana.

Poniższe parametry odczytano z pakietów świadków i tam, gdzie to możliwe, ponownie obliczono; nic nie zostało wpisane ręcznie.

WITNESS-1

Świadek	witness-1
Pobrano o (UTC)	2026-09-28T03:12:53+00:00
Żądanie	GET, bez plików cookie, z podążaniem za przekierowaniami, HTTP/1.1
Adres końcowy	https://machinewitness.eu/robots.txt
Status HTTP	200
TLS	TLSv1.3 TLS_AES_256_GCM_SHA384
Certyfikat, podmiot	CN=machinewitness.eu
Certyfikat, wystawca	C=US, O=Google Trust Services, CN=WE1
Certyfikat ważny	Sep 20 12:45:20 2026 GMT do Dec 19 13:45:17 2026 GMT
Łańcuch certyfikatów (SHA-256 każdego DER)	aec098364a0137418a01ed8935ac9d0070ffb370429a16df8b70a8cd73cd5e53 · 1dfc1605fbad358d8bc844f76d15203fac9ca5c1a79fd4857ffaf2864fbeb96 · 76b27b80a58027dc3cf1da68dac17010ed93997d0b603e2fadbe85012493b5a7
Kompletność	Zachowano w całości; do tej obserwacji nie zastosowano limitu bajtów.
SHA-256 dostarczonych bajtów	ae6ef8da7be4397f9d37a57be7b522f3f2b84d2b6af133ba26e8379acab36e32
SHA-256 danych pochodzenia	5819ce2ac282b3651477abf7db916cf1f3afd222a8aa3a0abef9fa9c580dc9c6
Liść	c6ae3444c00b163a044151ea59f634a6b0b39a4a3e29ca5b57f61abab78ec1ca
Pozycja w drzewie dnia	indeks 44,025 z 642,761 liści, 20 kroków do korzenia
Korzeń dnia	f1437269e4708b3dcc32a0c2947bdec58c1dbe084739ff912f14a03cacad48a6
Zakotwiczenia korzenia dnia	znacznik czasu RFC 3161 (FreeTSA) · OpenTimestamps (Bitcoin) · kwalifikowany znacznik czasu eIDAS (GLOBALTRUST)
Pakiet	machinewitness-extract-witness-1-2026-09-28-d0199b52c7cc.zip, SHA-256 3188c88a114c739d32122f7a89c6f4fa06c96c70eb1105886a2c4710c5633fb7

WITNESS-2

Świadek	witness-2
Pobrano o (UTC)	2026-09-28T03:01:20+00:00
Żądanie	GET, bez plików cookie, z podążaniem za przekierowaniami, HTTP/1.1
Adres końcowy	https://machinewitness.eu/robots.txt

Status HTTP	200
TLS	TLSv1.3 TLS_AES_256_GCM_SHA384
Certyfikat, podmiot	CN=machinewitness.eu
Certyfikat, wystawca	C=US, O=Google Trust Services, CN=WE1
Certyfikat ważny	Sep 20 12:45:20 2026 GMT do Dec 19 13:45:17 2026 GMT
Łańcuch certyfikatów (SHA-256 każdego DER)	aec098364a0137418a01ed8935ac9d0070ffb370429a16df8b70a8cd73cd5e53 · 1dfc1605fbad358d8bc844f76d15203fac9ca5c1a79fd4857ffaf2864fbeb96 · 76b27b80a58027dc3cf1da68dac17010ed93997d0b603e2fadbe85012493b5a7
Kompletność	Zachowano w całości; do tej obserwacji nie zastosowano limitu bajtów.
SHA-256 dostarczonych bajtów	ae6ef8da7be4397f9d37a57be7b522f3f2b84d2b6af133ba26e8379acab36e32
SHA-256 danych pochodzenia	a20e01fd655b9927a077d667fbcf68afe2a2600552863b6ac8ae84297974a730
Liść	10f22b28b520a9ea35e4e1be81f525f7aa04035157b9d1cb22ced67375f3fd52
Pozycja w drzewie dnia	indeks 24 z 586,787 liści, 20 kroków do korzenia
Korzeń dnia	d568805980fc63d4fbd54959ec16efda605b13fc1cae54b88fb94a7ebdc55d
Zakotwiczenia korzenia dnia	znacznik czasu RFC 3161 (FreeTSA) · OpenTimestamps (Bitcoin) · kwalifikowany znacznik czasu eIDAS (GLOBALTRUST)
Pakiet	machinewitness-extract-witness-2-2026-09-28-d0199b52c7cc.zip, SHA-256 d69cce6fbdda19d2a951419677ace17a25d2e079ff7799e2fea49ef21e5ed5f6

Obaj świadkowie otrzymali te same bajty: SHA-256 dostarczonych bajtów jest identyczny w obu pakietach. Ich liście się różnią, jak powinny: każdy liść wiąże także własny czas pobrania świadka i jego własny zapis pochodzenia.

2. Pobranie

Każdy świadek to odrębna maszyna u odrębnego dostawcy w odrębnym kraju, z własnymi kluczami. Żaden nie może zapisywać u drugiego. Każdy pobiera adres zwykłym żądaniem HTTP GET, przedstawiając się opublikowanym identyfikatorem MachineWitnessBot/0.1 (+https://machinewitness.eu/bot; evidence archive; contact: bot@machinewitness.eu), bez wysyłania plików cookie i z podążaniem za przekierowaniami; adres, który ostatecznie odpowiedział, jest zapisywany jako adres końcowy. Świadek zapisuje status, wszystkie nagłówki odpowiedzi, wersję i szyfr TLS, certyfikat serwera i SHA-256 każdego certyfikatu przedstawionego łańcucha oraz, jeśli zostały zapisane, własny adres i adres, który odpowiedział. Nie loguje się, nie klika, niczego nie wypełnia i nie uruchamia skryptów strony. Zapisane jest więc to, co ten adres dostarczył temu żądaniu w tym momencie, a nie to, co mógł pokazać innemu odwiedzającemu w innym momencie.

3. Przechowywanie i odcisk

Dostarczone bajty są przechowywane w postaci, w jakiej je otrzymano. Ich odcisk SHA-256 oblicza się dokładnie na tych bajtach. To, czy przechowywane bajty są kompletne, jest samo zapisane w danych pochodzenia (truncated), a powyższy wiersz o kompletności to powtarza. Zapis pochodzenia (adres końcowy, nagłówki, dane TLS, skróty certyfikatów, adresy) jest serializowany jako zwarty JSON z posortowanymi kluczami i sam otrzymuje odcisk.

4. Liść

Obserwacja zostaje sprowadzona do jednej wartości, liścia:

```
leaf = SHA-256( 0x00 || "mwleaf-v1|" url "|" observed_at "|" payload_sha256 "|" status "|"
provenance_sha256 )
```

Bajt przedrostka `0x00` oddziela liście od węzłów wewnętrznych drzewa, tak aby żadnego węzła wewnętrznego nie można było przedstawić jako liścia. Na potrzeby tego opisu liść każdego świadka ponownie obliczono z jego zapisanych pól i zgadza się on z liściem w pakiecie.

5. Drzewo i korzeń dnia

Każda obserwacja, którą świadek wykonuje w danym dniu UTC, staje się liściem drzewa Merkle tego dnia. Węzły wewnętrzne to `SHA-256(0x01 || lewy || prawy)`. Jedyna wartość na szczycie, korzeń dnia, zmienia się, gdy zmieni się jakikolwiek bajt jakiegokolwiek obserwacji tego dnia. Pakiet zawiera ścieżkę od tego liścia do korzenia: skróty węzłów sąsiednich i ich stronę. Złożenie ich po kolei odtwarza korzeń. Korzeń jest publikowany w publicznym rejestrze tego archiwum pod stałym adresem dla danego dnia.

6. Zakotwiczenia

Jeszcze tej samej nocy korzeń dnia zostaje przekazany podmiotom spoza tego archiwum: organowi znakowania czasem RFC 3161, kalendarzom OpenTimestamps, które włączają go do łańcucha bloków Bitcoin, oraz, od 31 lipca 2026 r., GLOBALTRUST (e-commerce monitoring GmbH, Austria), kwalifikowanemu dostawcy usług zaufania z unijnej listy zaufanych podmiotów, który wydaje kwalifikowany elektroniczny znacznik czasu. Każde zakotwiczenie poświadcza, że korzeń istniał w momencie, który wskazuje. Od tej chwili korzenia nie można podmienić bez utraty zgodności z zakotwiczeniami. To kwalifikowany znacznik czasu korzysta z domniemania, o którym mowa w art. 41 ust. 2 rozporządzenia (UE) nr 910/2014, co do dokładności wskazanej daty i czasu oraz integralności danych, z którymi są one powiązane.

7. Dwóch świadków

Drugi świadek wykonuje własne pobranie, buduje własne drzewo i uzyskuje własne zakotwiczenia. Oba korzenie nie są identyczne i nie mają takie być: każdy świadek obserwuje według własnego harmonogramu i zapisuje własny czas pobrania. Umożliwiają one porównanie: dla tego samego adresu w tym samym dniu pakiet każdego świadka pokazuje, co ten świadek otrzymał, i oba można ze sobą zestawiać. Obaj świadkowie otrzymali te same bajty: `SHA-256` dostarczonych bajtów jest identyczny w obu pakietach. Ich liście się różnią, jak powinny: każdy liść wiąże także własny czas pobrania świadka i jego własny zapis pochodzenia.

8. Powtórzenie kroków bez nas

1. **Bajty.** `sha256sum payload-<id>.bin` daje wartość zapisaną w `leaf-<id>.json` jako `payload_sha256`.
2. **Pochodzenie.** `sha256sum provenance-<id>.json`, plik dokładnie w obecnej postaci, daje `provenance_sha256`.
3. **Liść.** Wzór z sekcji 4 z pięcioma polami z `leaf-<id>.json` daje `leaf`. Wystarczy dowolne narzędzie obliczające `SHA-256`.
4. **Korzeń.** Złożyć ścieżkę z `proof-<id>.json` zgodnie z sekcją 5; wynikiem jest korzeń z `<dzień>.root.txt` i z publicznego rejestru.
5. **Zakotwiczenia.** `openssl ts -verify` dla obu tokenów RFC 3161 wobec łańcuchów certyfikatów wystawców; `ots verify` dla dowodu OpenTimestamps.

Każdy pakiet zawiera te kroki w pliku `VERIFY.txt`. Żaden nie wymaga oprogramowania tego archiwum.

9. Zwykle podnoszone zarzuty i odpowiedź techniczna

Operator mógł później zmienić zapis.

Zmiana dowolnego bajtu zmienia liść, korzeń i zakotwiczenia dnia. Zakotwiczenia wydano w nocy, w której dzień zapieczętowano, i znajdują się w rękach osób trzecich. Zmieniony zapis przestaje z nimi się zgadzać, co można sprawdzić bez nas (sekcja 8, kroki 4 i 5).

Zapis pokazuje to, co świadek postanowił przechować, a nie to, co wysłał serwer.

Bajty są przechowywane w postaci otrzymanej i otrzymują odcisk, zanim cokolwiek innego się z nimi stanie. Kompletność jest zapisana jako zapieczętowane pole, a nie deklarowana później. Jeśli zastosowano limit bajtów, zapis podaje to dla tej obserwacji.

Serwer mógł pokazać innym odwiedzającym coś innego.

To prawda i jest to powiedziane, a nie ukryte: zapis obejmuje to, co ten adres dostarczył temu żądaniu, identyfikowanemu opublikowanym identyfikatorem, we wskazanym momencie. Nie stwierdza niczego o innych żądaniach.

Czas pobrania opiera się na zegarze samego świadka.

Czas pobrania zapisuje świadek. Zakotwiczenia niezależnie ustalają najpóźniejszy moment, w którym istniał cały dzień, łącznie z tą obserwacją. Kwalifikowany znacznik czasu podaje swój czas pod nadzorem opisanym w sekcji 6.

Jedna maszyna mogłaby się mylić.

Są dwie, u różnych dostawców, z oddzielnymi kluczami, i żadna nie może zapisywać u drugiej (sekcja 7).

10. Czym niniejszy opis nie jest

Nie zawiera żadnego stwierdzenia dotyczącego jakiegokolwiek sprawy, żadnej oceny czyjegokolwiek postępowania ani żadnej opinii o szansach postępowania. Opisuje procedurę i parametry jednej obserwacji. To, co z niego wynika, rozstrzygają strony i sąd.

Część B · Pisemne odpowiedzi techniczne, runda 1

Pytania otrzymane na piśmie w sprawie powyższej obserwacji, z odpowiedziami na piśmie. Odpowiedzi odwołują się do opublikowanej metody i nie mówią nic o sprawie.

Wyciąg podaje dla 28 września 2026 r. dwa różne korzenie dnia, po jednym na świadka. Który z nich jest właściwy?

Oba. Każdy świadek buduje własne drzewo z własnych obserwacji tego dnia i zakotwicza własny korzeń; oba drzewa zawierają różne zbiory liści, zapisane w różnych momentach, dlatego ich korzenie różnią się z samej konstrukcji. Korzeń sprawdza się wobec rejestru i zakotwiczeń świadka, który go utworzył. Wspólny dla obu świadków nie jest korzeń, lecz obserwacja: dla tego adresu oba pakiety zawierają ten sam SHA-256 dostarczonych bajtów.

Jak sprawdzić, że plik robots.txt nie został zmieniony po zapisaniu?

Przez ponowne obliczenie, bez nas: SHA-256 pliku payload-<id>.bin musi być równy payload_sha256 w pliku liścia; liść musi dać się ponownie obliczyć z jego pięciu pól (sekcja 4); ścieżka z proof-<id>.json musi złożyć się do korzenia dnia; a korzeń dnia musi zgadzać się z zakotwiczeniami wydanymi tej samej nocy (sekcja 8). Gdyby po 28 września 2026 r. zmieniono choćby jeden bajt, jedna z tych czterech kontroli zakończyłaby się niepowodzeniem.

Miejscowość, data

Martin Schenk, w imieniu MachineWitness
(Martin Schenk S.L., Madryt)

PRZYKŁAD, niepodpisany.