

Comment une observation a été faite

EXEMPLE. Rédigée pour une observation réelle de notre propre domaine machinewitness.eu, avec ses paramètres réels, par le même outil que chaque description. Elle est publiée comme exemple et n'est donc pas signée. Une description commandée est rédigée pour l'observation que vous désignez, relue et signée.

1. Objet de la présente description

La présente description expose comment une observation a été faite : l'adresse `https://machinewitness.eu/robots.txt` le jour **2026-09-28** (UTC), récupérée indépendamment par 2 témoins. Elle explique la méthode avec les paramètres réels de cette observation, expose chaque étape de sorte qu'un tiers puisse la répéter sans nous et nomme les objections habituellement soulevées contre la méthode. Elle ne dit rien du contenu récupéré ni d'une quelconque affaire dans laquelle il est utilisé.

Les paramètres ci-dessous sont lus dans les paquets des témoins et recalculés lorsque c'est possible ; rien n'y a été saisi à la main.

WITNESS-1

Témoin	witness-1
Récupéré à (UTC)	2026-09-28T03:12:53+00:00
Requête	GET, sans cookies, redirections suivies, HTTP/1.1
Adresse finale	https://machinewitness.eu/robots.txt
Statut HTTP	200
TLS	TLSv1.3 TLS_AES_256_GCM_SHA384
Certificat, titulaire	CN=machinewitness.eu
Certificat, émetteur	C=US, O=Google Trust Services, CN=WE1
Certificat valide	Sep 20 12:45:20 2026 GMT au Dec 19 13:45:17 2026 GMT
Chaîne de certificats (SHA-256 de chaque DER)	aec098364a0137418a01ed8935ac9d0070fffb370429a16df8b70a8cd73cd5e53 · 1dfc1605fbad358d8bc844f76d15203fac9ca5c1a79fd4857ffaf2864fbeb96 · 76b27b80a58027dc3cf1da68dac17010ed93997d0b603e2fadbe85012493b5a7
Complétude	Conservé intégralement ; aucune limite d'octets ne s'est appliquée à cette observation.
SHA-256 des octets livrés	ae6ef8da7be4397f9d37a57be7b522f3f2b84d2b6af133ba26e8379acab36e32
SHA-256 de la provenance	5819ce2ac282b3651477abf7db916cf1f3afd22a8aa3a0abef9fa9c580dc9c6
Feuille	c6ae3444c00b163a044151ea59f634a6b0b39a4a3e29ca5b57f61abab78ec1ca
Position dans l'arbre du jour	index 44,025 sur 642,761 feuilles, 20 étapes jusqu'à la racine
Racine du jour	f1437269e4708b3dcc32a0c2947bdec58c1dbe084739ff912f14a03cacad48a6
Ancrages de la racine du jour	horodatage RFC 3161 (FreeTSA) · OpenTimestamps (Bitcoin) · horodatage qualifié eIDAS (GLOBALTRUST)
Paquet	machinewitness-extract-witness-1-2026-09-28-d0199b52c7cc.zip, SHA-256 3188c88a114c739d32122f7a89c6f4fa06c96c70eb1105886a2c4710c5633fb7

WITNESS-2

Témoin	witness-2
Récupéré à (UTC)	2026-09-28T03:01:20+00:00
Requête	GET, sans cookies, redirections suivies, HTTP/1.1
Adresse finale	https://machinewitness.eu/robots.txt

Statut HTTP	200
TLS	TLSv1.3 TLS_AES_256_GCM_SHA384
Certificat, titulaire	CN=machinewitness.eu
Certificat, émetteur	C=US, O=Google Trust Services, CN=WE1
Certificat valide	Sep 20 12:45:20 2026 GMT au Dec 19 13:45:17 2026 GMT
Chaîne de certificats (SHA-256 de chaque DER)	aec098364a0137418a01ed8935ac9d0070ffb370429a16df8b70a8cd73cd5e53 · 1dfc1605fbad358d8bc844f76d15203fac9ca5c1a79fd4857ffaf2864fbeb96 · 76b27b80a58027dc3cf1da68dac17010ed93997d0b603e2fadbe85012493b5a7
Complétude	Conservé intégralement ; aucune limite d'octets ne s'est appliquée à cette observation.
SHA-256 des octets livrés	ae6ef8da7be4397f9d37a57be7b522f3f2b84d2b6af133ba26e8379acab36e32
SHA-256 de la provenance	a20e01fd655b9927a077d667fbcf68afe2a2600552863b6ac8ae84297974a730
Feuille	10f22b28b520a9ea35e4e1be81f525f7aa04035157b9d1cb22ced67375f3fd52
Position dans l'arbre du jour	index 24 sur 586,787 feuilles, 20 étapes jusqu'à la racine
Racine du jour	d568805980fcf63d4fbd54959ec16efda605b13fc1cae54b88fb94a7ebdc55d
Ancrages de la racine du jour	horodatage RFC 3161 (FreeTSA) · OpenTimestamps (Bitcoin) · horodatage qualifié eIDAS (GLOBALTRUST)
Paquet	machinewitness-extract-witness-2-2026-09-28-d0199b52c7cc.zip, SHA-256 d69cce6fbdda19d2a951419677ace17a25d2e079ff7799e2fea49ef21e5ed5f6

Les deux témoins ont reçu les mêmes octets : le SHA-256 des octets livrés est identique dans les deux paquets. Leurs feuilles diffèrent, comme il se doit : chaque feuille lie aussi l'heure de récupération propre au témoin et son propre enregistrement de provenance.

2. Récupération

Chaque témoin est une machine distincte chez un fournisseur distinct dans un pays distinct, avec ses propres clés. Aucun ne peut écrire chez l'autre. Chacun récupère l'adresse par une simple requête HTTP GET, en s'identifiant par l'agent utilisateur publié MachineWitnessBot/0.1 (+https://machinewitness.eu/bot; evidence archive; contact: bot@machinewitness.eu), sans envoyer de cookies et en suivant les redirections ; l'adresse qui a finalement répondu est enregistrée comme adresse finale. Le témoin enregistre le statut, tous les en-têtes de réponse, la version et le chiffrement TLS, le certificat du serveur et le SHA-256 de chaque certificat de la chaîne présentée, ainsi que, lorsqu'elles sont enregistrées, sa propre adresse et l'adresse qui a répondu. Il ne se connecte pas, ne clique pas, ne remplit rien et n'exécute pas les scripts de la page. Ce qui est enregistré est donc ce que cette adresse a servi à cette requête à ce moment, et non ce qu'elle a pu montrer à un autre visiteur à un autre moment.

3. Conservation et empreinte

Les octets livrés sont conservés tels que reçus. Leur empreinte SHA-256 est calculée exactement sur ces octets. Le caractère complet des octets conservés est lui-même consigné dans la provenance (truncated), et la ligne de complétude ci-dessus le reprend. L'enregistrement de provenance (adresse finale, en-têtes, données TLS, empreintes des certificats, adresses) est sérialisé en JSON compact à clés triées et reçoit à son tour une empreinte.

4. La feuille

L'observation est réduite à une seule valeur, la feuille :

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

L'octet de préfixe 0x00 distingue les feuilles des nœuds internes de l'arbre, de sorte qu'aucun nœud interne ne puisse être présenté comme une feuille. Pour cette description, la feuille de chaque témoin a été recalculée à partir de ses champs enregistrés et correspond à la feuille du paquet.

5. L'arbre et la racine du jour

Chaque observation qu'un témoin fait au cours d'un jour UTC devient une feuille de l'arbre de Merkle de ce jour. Les nœuds internes sont SHA-256(0x01 || gauche || droite). La valeur unique au sommet, la racine du jour, change si un octet quelconque d'une observation quelconque de ce jour change. Le paquet contient le chemin de cette feuille à la racine : les empreintes sœurs et leur côté. En les repliant dans l'ordre, on retrouve la racine. La racine est publiée dans le registre public de cette archive à une adresse fixe pour le jour.

6. Ancrages

La nuit même, la racine du jour est remise à des tiers extérieurs à cette archive : une autorité d'horodatage RFC 3161, les calendriers OpenTimestamps, qui l'agrègent dans la chaîne de blocs Bitcoin, et, depuis le 31 juillet 2026, GLOBALTRUST (e-commerce monitoring GmbH, Autriche), prestataire de services de confiance qualifié inscrit sur la liste de confiance de l'UE, qui délivre un horodatage électronique qualifié. Chaque ancrage atteste que la racine existait au moment qu'il indique. Dès lors, une racine ne peut plus être remplacée sans que les ancres cessent de correspondre. L'horodatage qualifié est celui qui bénéficie de la présomption prévue à l'article 41, paragraphe 2, du règlement (UE) n° 910/2014 quant à l'exactitude de sa date et de son heure et à l'intégrité des données auxquelles elles se rapportent.

7. Deux témoins

Le second témoin fait sa propre récupération, construit son propre arbre et prend ses propres ancres. Les deux racines ne sont pas identiques et ne sont pas censées l'être : chaque témoin observe selon son propre calendrier et enregistre sa propre heure de récupération. Ce qu'elles permettent, c'est une comparaison : pour la même adresse le même jour, le paquet de chaque témoin montre ce que ce témoin a reçu, et les deux peuvent être confrontés. Les deux témoins ont reçu les mêmes octets : le SHA-256 des octets livrés est identique dans les deux paquets. Leurs feuilles diffèrent, comme il se doit : chaque feuille lie aussi l'heure de récupération propre au témoin et son propre enregistrement de provenance.

8. Répéter les étapes sans nous

1. **Octets.** sha256sum payload-<id>.bin donne la valeur figurant dans leaf-<id>.json sous payload_sha256.
2. **Provenance.** sha256sum provenance-<id>.json, le fichier tel quel, donne provenance_sha256.
3. **Feuille.** La formule de la section 4, avec les cinq champs de leaf-<id>.json, donne leaf. Tout outil calculant SHA-256 convient.
4. **Racine.** Replier le chemin de proof-<id>.json comme décrit à la section 5 ; le résultat est la racine de <jour>.root.txt et du registre public.
5. **Ancrages.** openssl ts -verify pour les deux jetons RFC 3161 contre les chaînes de certificats des émetteurs ; ots verify pour la preuve OpenTimestamps.

Chaque paquet contient ces étapes dans un fichier VERIFY.txt. Aucune ne nécessite de logiciel de cette archive.

9. Objections habituelles et réponse technique

L'exploitant aurait pu modifier l'enregistrement après coup.

La modification d'un octet quelconque modifie la feuille, la racine et les ancres du jour. Les ancres ont été délivrés la nuit où le jour a été scellé et sont détenus par des tiers. Un enregistrement modifié ne leur correspond plus, et cela se vérifie sans nous (section 8, étapes 4 et 5).

L'enregistrement montre ce que le témoin a choisi de conserver, non ce que le serveur a envoyé.

Les octets sont conservés tels que reçus et reçoivent leur empreinte avant toute autre opération. La complétude est consignée comme champ scellé, et non affirmée après coup. Lorsqu'une limite d'octets s'est appliquée, l'enregistrement l'indique pour cette observation.

Le serveur a pu montrer autre chose à d'autres visiteurs.

C'est exact et c'est dit, non caché : l'enregistrement couvre ce que cette adresse a servi à cette requête, identifiée par l'agent utilisateur publié, au moment indiqué. Il n'affirme rien sur d'autres requêtes.

L'heure de récupération repose sur l'horloge du témoin.

L'heure de récupération est consignée par le témoin. Les ancres fixent indépendamment le moment au plus tard auquel le jour entier, cette observation comprise, existait. L'horodatage qualifié indique son heure sous la supervision décrite à la section 6.

Une seule machine pourrait se tromper.

Il y en a deux, chez des fournisseurs différents, avec des clés distinctes, et aucune ne peut écrire chez l'autre (section 7).

10. Ce que la présente description n'est pas

Elle ne contient aucune déclaration sur une affaire, aucune appréciation du comportement de quiconque et aucun avis sur les chances d'une procédure. Elle décrit une procédure et les paramètres d'une observation. Les conséquences à en tirer relèvent des parties et du tribunal.

Partie B · Réponses techniques écrites, série 1

Questions reçues par écrit sur l'observation ci-dessus, avec réponses écrites. Les réponses s'appuient sur la méthode publiée et ne disent rien de l'affaire.

L'extrait donne deux racines du jour différentes pour le 28 septembre 2026, une par témoin. Laquelle des deux est la bonne ?

Les deux. Chaque témoin construit son propre arbre sur ses propres observations de ce jour et ancre sa propre racine ; les deux arbres contiennent des ensembles différents de feuilles, enregistrées à des moments différents, de sorte que leurs racines diffèrent par construction. Une racine se vérifie par rapport au registre et aux ancrages du témoin qui l'a produite. Ce que les deux témoins ont en commun n'est pas la racine, mais l'observation : pour cette adresse, les deux paquets portent le même SHA-256 des octets livrés.

Comment vérifier que le robots.txt n'a pas été modifié après sa conservation ?

En recalculant, sans nous : le SHA-256 de payload-<id>.bin doit être égal à payload_sha256 dans le fichier de la feuille ; la feuille doit se recalculer à partir de ses cinq champs (section 4) ; le chemin de proof-<id>.json doit se replier jusqu'à la racine du jour ; et la racine du jour doit correspondre aux ancrages délivrés la nuit même (section 8). Si un seul octet avait été modifié après le 28 septembre 2026, l'une de ces quatre vérifications échouerait.

Lieu, date

Martin Schenk, pour MachineWitness (Martin Schenk S.L., Madrid)

EXEMPLE, non signé.