

Come è stata fatta un’osservazione

ESEMPIO. Redatta per un’osservazione reale del nostro stesso dominio machinewitness.eu, con i suoi parametri effettivi, con lo stesso strumento di ogni descrizione. È pubblicata come esempio e perciò non è firmata. La descrizione che Lei ordina viene redatta per l’osservazione che indica, riletta e firmata.

1. Oggetto della presente descrizione

La presente descrizione espone come è stata fatta un’osservazione: l’indirizzo `https://machinewitness.eu/robots.txt` nel giorno **2026-09-28** (UTC), prelevato in modo indipendente da 2 testimoni. Spiega il metodo con i parametri effettivi di quell’osservazione, espone ogni passaggio in modo che un terzo possa ripeterlo senza di noi e indica le obiezioni sollevate di solito contro il metodo. Non dice nulla sul contenuto prelevato né su alcuna vicenda in cui venga usato.

I parametri qui sotto sono letti dai pacchetti dei testimoni e ricalcolati dove possibile; nulla è stato digitato a mano.

WITNESS-1

Testimone	witness-1
Prelevato alle (UTC)	2026-09-28T03:12:53+00:00
Richiesta	GET, nessun cookie, reindirizzamenti seguiti, HTTP/1.1
Indirizzo finale	https://machinewitness.eu/robots.txt
Stato HTTP	200
TLS	TLSv1.3 TLS_AES_256_GCM_SHA384
Certificato, titolare	CN=machinewitness.eu
Certificato, emittente	C=US, O=Google Trust Services, CN=WE1
Certificato valido	Sep 20 12:45:20 2026 GMT al Dec 19 13:45:17 2026 GMT
Catena dei certificati (SHA-256 di ogni DER)	aec098364a0137418a01ed8935ac9d0070ffb370429a16df8b70a8cd73cd5e53 · 1dfc1605fbad358d8bc844f76d15203fac9ca5c1a79fd4857ffaf2864fbeb96 · 76b27b80a58027dc3cf1da68dac17010ed93997d0b603e2fadbe85012493b5a7
Completezza	Conservato per intero; a questa osservazione non si è applicato alcun limite di byte.
SHA-256 dei byte consegnati	ae6ef8da7be4397f9d37a57be7b522f3f2b84d2b6af133ba26e8379acab36e32
SHA-256 della provenienza	5819ce2ac282b3651477abf7db916cf1f3afd222a8aa3a0abef9fa9c580dc9c6
Foglia	c6ae3444c00b163a044151ea59f634a6b0b39a4a3e29ca5b57f61abab78ec1ca
Posizione nell’albero del giorno	indice 44,025 di 642,761 foglie, 20 passaggi fino alla radice
Radice del giorno	f1437269e4708b3dcc32a0c2947bdec58c1dbe084739ff912f14a03cacad48a6
Ancoraggi della radice del giorno	marca temporale RFC 3161 (FreeTSA) · OpenTimestamps (Bitcoin) · validazione temporale qualificata eIDAS (GLOBALTRUST)
Pacchetto	machinewitness-extract-witness-1-2026-09-28-d0199b52c7cc.zip, SHA-256 3188c88a114c739d32122f7a89c6f4fa06c96c70eb1105886a2c4710c5633fb7

WITNESS-2

Testimone	witness-2
Prelevato alle (UTC)	2026-09-28T03:01:20+00:00
Richiesta	GET, nessun cookie, reindirizzamenti seguiti, HTTP/1.1
Indirizzo finale	https://machinewitness.eu/robots.txt

Stato HTTP	200
TLS	TLSv1.3 TLS_AES_256_GCM_SHA384
Certificato, titolare	CN=machinewitness.eu
Certificato, emittente	C=US, O=Google Trust Services, CN=WE1
Certificato valido	Sep 20 12:45:20 2026 GMT al Dec 19 13:45:17 2026 GMT
Catena dei certificati (SHA-256 di ogni DER)	aec098364a0137418a01ed8935ac9d0070ffb370429a16df8b70a8cd73cd5e53 · 1dfc1605fbad358d8bc844f76d15203fac9ca5c1a79fd4857ffaf2864fbebfb96 · 76b27b80a58027dc3cf1da68dac17010ed93997d0b603e2fadbe85012493b5a7
Completezza	Conservato per intero; a questa osservazione non si è applicato alcun limite di byte.
SHA-256 dei byte consegnati	ae6ef8da7be4397f9d37a57be7b522f3f2b84d2b6af133ba26e8379acab36e32
SHA-256 della provenienza	a20e01fd655b9927a077d667fbcf68afe2a2600552863b6ac8ae84297974a730
Foglia	10f22b28b520a9ea35e4e1be81f525f7aa04035157b9d1cb22ced67375f3fd52
Posizione nell'albero del giorno	indice 24 di 586,787 foglie, 20 passaggi fino alla radice
Radice del giorno	d568805980fc63d4fdbb54959ec16efda605b13fc1cae54b88fb94a7ebdc55d
Ancoraggi della radice del giorno	marca temporale RFC 3161 (FreeTSA) · OpenTimestamps (Bitcoin) · validazione temporale qualificata eIDAS (GLOBALTRUST)
Pacchetto	machinewitness-extract-witness-2-2026-09-28-d0199b52c7cc.zip, SHA-256 d69cce6fbdda19d2a951419677ace17a25d2e079ff7799e2fea49ef21e5ed5f6

Entrambi i testimoni hanno ricevuto gli stessi byte: lo SHA-256 dei byte consegnati è identico in entrambi i pacchetti. Le loro foglie differiscono, come devono: ogni foglia vincola anche l'ora di prelievo propria del testimone e la sua registrazione di provenienza.

2. Prelievo

Ogni testimone è una macchina distinta presso un fornitore distinto in un paese distinto, con le proprie chiavi. Nessuno dei due può scrivere nell'altro. Ciascuno preleva l'indirizzo con una semplice richiesta HTTP GET, identificandosi con l'agente utente pubblicato MachineWitnessBot/0.1 (+https://machinewitness.eu/bot; evidence archive; contact: bot@machinewitness.eu), senza inviare cookie e seguendo i reindirizzamenti; l'indirizzo che ha risposto per ultimo è registrato come indirizzo finale. Il testimone registra lo stato, tutte le intestazioni di risposta, la versione e la cifratura TLS, il certificato del server e lo SHA-256 di ogni certificato della catena presentata e, dove registrati, il proprio indirizzo e l'indirizzo che ha risposto. Non effettua l'accesso, non clicca, non compila nulla e non esegue gli script della pagina. Ciò che è registrato è quindi ciò che questo indirizzo ha servito a questa richiesta in questo momento, non ciò che potrebbe aver mostrato a un altro visitatore in un altro momento.

3. Conservazione e impronta

I byte consegnati sono conservati così come ricevuti. La loro impronta SHA-256 è calcolata esattamente su quei byte. Se i byte conservati siano completi è a sua volta registrato nella provenienza (truncated), e la riga sulla completezza qui sopra lo riporta. La registrazione di provenienza (indirizzo finale, intestazioni, dati TLS, hash dei certificati, indirizzi) è serializzata come JSON compatto con chiavi ordinate e riceve a sua volta un'impronta.

4. La foglia

L'osservazione è ridotta a un unico valore, la foglia:

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

Il byte di prefisso `0x00` separa le foglie dai nodi interni dell'albero, così che nessun nodo interno possa essere presentato come foglia. Per questa descrizione la foglia di ogni testimone è stata ricalcolata dai suoi campi registrati e corrisponde alla foglia del pacchetto.

5. L'albero e la radice del giorno

Ogni osservazione che un testimone compie in un giorno UTC diventa una foglia dell'albero di Merkle di quel giorno. I nodi interni sono `SHA-256(0x01 || sinistra || destra)`. Il valore unico in cima, la radice del giorno, cambia se cambia un qualsiasi byte di una qualsiasi osservazione di quel giorno. Il pacchetto contiene il percorso da questa foglia alla radice: gli hash fratelli e il loro lato. Ripiegandoli in ordine si riottiene la radice. La radice è pubblicata nel registro pubblico di questo archivio a un indirizzo fisso per il giorno.

6. Ancoraggi

La notte stessa la radice del giorno viene consegnata a soggetti esterni a questo archivio: un'autorità di marcatura temporale RFC 3161, i calendari OpenTimestamps, che la aggregano nella blockchain di Bitcoin, e, dal 31 luglio 2026, GLOBALTRUST (e-commerce monitoring GmbH, Austria), prestatore di servizi fiduciari qualificato iscritto nell'elenco di fiducia dell'UE, che rilascia una validazione temporale elettronica qualificata. Ogni ancoraggio attesta che la radice esisteva nel momento che indica. Da quel momento una radice non può essere sostituita senza che gli ancoraggi smettano di corrispondere. La validazione temporale qualificata è quella che gode della presunzione di cui all'articolo 41, paragrafo 2, del regolamento (UE) n. 910/2014 quanto all'accuratezza della data e dell'ora che indica e all'integrità dei dati ai quali sono associate.

7. Due testimoni

Il secondo testimone effettua il proprio prelievo, costruisce il proprio albero e prende i propri ancoraggi. Le due radici non sono identiche e non devono esserlo: ogni testimone osserva secondo il proprio calendario e registra la propria ora di prelievo. Ciò che consentono è un confronto: per lo stesso indirizzo nello stesso giorno, il pacchetto di ciascun testimone mostra ciò che quel testimone ha ricevuto, e i due possono essere messi a confronto. Entrambi i testimoni hanno ricevuto gli stessi byte: lo SHA-256 dei byte consegnati è identico in entrambi i pacchetti. Le loro foglie differiscono, come devono: ogni foglia vincola anche l'ora di prelievo propria del testimone e la sua registrazione di provenienza.

8. Ripetere i passaggi senza di noi

1. **Byte.** `sha256sum payload-<id>.bin` dà il valore che figura in `leaf-<id>.json` come `payload_sha256`.
2. **Provenienza.** `sha256sum provenance-<id>.json`, il file così com'è, dà `provenance_sha256`.
3. **Foglia.** La formula della sezione 4, con i cinque campi di `leaf-<id>.json`, dà `leaf`. Va bene qualsiasi strumento che calcoli SHA-256.
4. **Radice.** Ripiegare il percorso di `proof-<id>.json` come descritto nella sezione 5; il risultato è la radice di `<giorno>.root.txt` e del registro pubblico.
5. **Ancoraggi.** `openssl ts -verify` per i due token RFC 3161 rispetto alle catene di certificati degli emittenti; `ots verify` per la prova OpenTimestamps.

Ogni pacchetto contiene questi passaggi in un file `VERIFY.txt`. Nessuno richiede software di questo archivio.

9. Obiezioni abituali e risposta tecnica

Il gestore potrebbe aver modificato la registrazione in seguito.

La modifica di un qualsiasi byte modifica la foglia, la radice e gli ancoraggi del giorno. Gli ancoraggi sono stati rilasciati la notte in cui il giorno è stato sigillato e sono in mano a terzi. Una registrazione modificata non vi corrisponde più, e ciò si verifica senza di noi (sezione 8, passaggi 4 e 5).

La registrazione mostra ciò che il testimone ha scelto di conservare, non ciò che il server ha inviato.

I byte sono conservati così come ricevuti e ricevono la loro impronta prima di qualsiasi altra operazione. La completezza è registrata come campo sigillato, non affermata in seguito. Dove si è applicato un limite di byte, la registrazione lo indica per quell'osservazione.

Il server potrebbe aver mostrato altro ad altri visitatori.

È vero ed è detto, non nascosto: la registrazione copre ciò che questo indirizzo ha servito a questa richiesta, identificata dall'agente utente pubblicato, nel momento indicato. Non afferma nulla su altre richieste.

L'ora del prelievo si basa sull'orologio del testimone.

L'ora del prelievo è registrata dal testimone. Gli ancoraggi fissano in modo indipendente il momento entro cui esisteva l'intero giorno, compresa questa osservazione. La validazione temporale qualificata indica la sua ora sotto la vigilanza descritta nella sezione 6.

Una sola macchina potrebbe sbagliare.

Sono due, presso fornitori diversi, con chiavi separate, e nessuna può scrivere nell'altra (sezione 7).

10. Che cosa non è la presente descrizione

Non contiene alcuna dichiarazione su una vicenda, alcuna valutazione della condotta di chiunque né alcuna opinione sulle prospettive di un procedimento. Descrive una procedura e i parametri di un'osservazione. Ciò che ne consegue lo decidono le parti e il giudice.

Parte B · Risposte tecniche scritte, giro 1

Domande ricevute per iscritto sull'osservazione di cui sopra, con risposta scritta. Le risposte si rifanno al metodo pubblicato e non dicono nulla sulla vicenda.

L'estratto indica due radici del giorno diverse per il 28 settembre 2026, una per testimone. Quale delle due è quella corretta?

Entrambe. Ogni testimone costruisce il proprio albero sulle proprie osservazioni di quel giorno e ancora la propria radice; i due alberi contengono insieme diversi di foglie, registrate in momenti diversi, per cui le loro radici differiscono per costruzione. Una radice si verifica rispetto al registro e agli ancoraggi del testimone che l'ha prodotta. Ciò che i due testimoni hanno in comune non è la radice, ma l'osservazione: per questo indirizzo entrambi i pacchetti riportano lo stesso SHA-256 dei byte consegnati.

Come si può verificare che il robots.txt non sia stato modificato dopo la conservazione?

Ricalcolando, senza di noi: lo SHA-256 di payload-<id>.bin deve corrispondere a payload_sha256 nel file della foglia; la foglia deve potersi ricalcolare dai suoi cinque campi (sezione 4); il percorso in proof-<id>.json deve ripiegarsi fino alla radice del giorno; e la radice del giorno deve corrispondere agli ancoraggi rilasciati la notte stessa (sezione 8). Se dopo il 28 settembre 2026 fosse stato modificato anche un solo byte, una di queste quattro verifiche fallirebbe.

Luogo, data

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

ESEMPIO, non firmato.