# LegalAudit

LegalAudit SA — Lugano, Svizzera

## PERIZIA TECNICA FORENSE

**Riferimento caso:** LA-2026-06-02-9F2A1B
**Generato il:** 2026-06-02 09:42:00 UTC

### Richiedente

**Nome:** Sig.ra Rossi (caso didattico)
**Ruolo:** Privato cittadino
**Email:** didattico@legalaudit.ch

### ESITO: INDICATORI DI RISCHIO CRITICO

Confidenza analitica: 94%

**Verifica online: scansiona il QR code**

https://legalaudit.ch/it/verify/f1c2b3a4-5d6e-4f78-9012-3456789abcde

# Indice

## Tabella sinottica

| Indicatore | Esito | Evidenza |
|---|---|---|
| Impersonificazione familiare | Critico | E-1 |
| Frode finanziaria | Critico | E-1 |
| Manipolazione documento | Critico | E-2 |
| Integrità metadati | Anomalo | E-2 |
| Reputazione del numero mittente | Critico | E-1, E-6 |

## Periti firmatari

### LegalAudit SA

Ruolo: Sistema Mythos automatizzato
Iscrizione albo: Sede legale Lugano, Svizzera
Recapito: info@legalaudit.ch

## Sommario esecutivo

L'analisi forense indica HIGH-RISK al 94% di confidenza sulla base di cinque dimensioni indipendenti convergenti: impersonificazione familiare, frode finanziaria con IBAN destinatario in lista nera interna, manipolazione digitale del documento di identità prodotto come prova, integrità metadati compromessa e reputazione del numero mittente classificata come scam. Il caso è un esempio paradigmatico della tipologia 'ciao mamma / ciao papà' (cfr. E-1, E-6, E-7).

Il vettore di attacco combina ingegneria sociale (rapporto familiare simulato, urgenza temporale, blocco del canale originale) con due elementi forensi rilevabili strumentalmente: l'IBAN beneficiario, sintatticamente valido secondo l'algoritmo mod-97, risulta riferito a un istituto bancario presente in 14 dossier interni convergenti negli ultimi 30 giorni (cfr. E-7); la presunta carta di identità inviata come 'prova' presenta firma esplicita di software di editing (GIMP 2.10) e variance di Error Level Analysis pari a 0,78 contro una soglia di 0,45 (cfr. E-2, E-8, E-9).

Il verdetto è motivato dalla convergenza di tre segnali a severità 'danger' provenienti da artefatti tecnicamente indipendenti (cfr. E-1, E-2) e da due segnali tool-derivati (cfr. E-6, E-7) che amplificano l'evidenza. La raccomandazione operativa prioritaria è l'immediato blocco del bonifico presso l'istituto del richiedente (priorità P0) e la presentazione di querela ex artt. 640 c.p. e 494 c.p. presso la Polizia Postale.

## Risultati per dimensione forense

Dimensione 'Impersonificazione familiare' (cfr. E-1): la trascrizione della conversazione WhatsApp evidenzia un pattern statisticamente coerente con la tipologia 'ciao mamma' rilevata su 312 casi documentati nel database interno LegalAudit. I primi tre messaggi nei primi 90 secondi contengono tre asserzioni indipendenti di identità ('sono io', 'tuo figlio', 'è il mio nuovo numero'), seguite da una giustificazione del cambio di canale ('mi si è rotto il telefono, è il nuovo numero') che neutralizza preventivamente l'eventuale verifica out-of-band. Lo score di pressione vocabolare misurato è pari a 0,92 contro una soglia operativa di 0,55.

Dimensione 'Frode finanziaria' (cfr. E-1, E-7): la richiesta di bonifico è inserita in linea con la conversazione al minuto T+4'30" dalla prima asserzione di identità, prima che la vittima abbia potuto verificare il canale. L'IBAN proposto (IT00X00000000000000000000, qui anonimizzato per finalità didattiche) supera il controllo sintattico mod-97 ma l'istituto ricevente compare in 14 segnalazioni interne convergenti negli ultimi 30 giorni, conformi alla tipologia 'mule account' descritta in ENISA ETL §4.3.

Dimensione 'Manipolazione documento' (cfr. E-2, E-8, E-9): la presunta carta di identità inviata come prova presenta tre indicatori forensi cumulativi. (i) Il tag EXIF Software è popolato con 'GIMP 2.10', identificando l'editor di immagini OSS impiegato e una LastSave timestamp 2026-06-01 18:22 UTC, posteriore di tre ore rispetto al timestamp dichiarato di rilascio del documento. (ii) L'Error Level Analysis restituisce variance 0,78 sui rettangoli pixel-region corrispondenti ai campi NOME, COGNOME e DATA DI NASCITA, valore che supera la soglia operativa 0,45 ed è statisticamente incompatibile con un'unica fase di compressione JPEG sequenziale. (iii) Il riconoscimento visivo non identifica corrispondenza con i template ufficiali CIE/passaporto IT (cfr. E-5).

Dimensione 'Integrità metadati' (cfr. E-2, E-9): la sezione EXIF IFD0 dell'immagine non contiene i tag Make, Model né DateTimeOriginal, e la sezione GPS è assente. L'immagine non è dunque un'acquisizione diretta dal sensore di un dispositivo fisico ma un derivato esportato da software, coerentemente con la presenza del tag Software=GIMP 2.10. La combinazione [Software popolato, Make/Model nulli] è patognomonica di un workflow di manipolazione digitale.

Dimensione 'Reputazione del numero mittente' (cfr. E-1, E-6): il numero del mittente è classificato come MVNO italiano (carrier Iliad Italia su SIM ricaricabile) e presenta uno score Tellows pari a 8/10 sul campione di 47 voti aggregati. Tre crosscheck indipendenti su database antiscam pubblici confermano segnalazioni recenti (T-14 giorni) con tipologia 'impersonificazione familiare', circostanza che concorre alla confidence aggregata del verdetto.

### Impersonificazione familiare

D **Scam familiare 'ciao mamma' con pattern impersonificazione del figlio della vittima e richiesta urgente di bonifico bancario.**

`Evidenza: 8 messaggi tra le 18:14 e le 18:39 dello stesso giorno; 3 affermazioni di identità ('sono io', 'tuo figlio', 'è il mio nuovo numero') concentrate nei primi 90 secondi.`

`Riferimento: asset:11111111-1111-4111-8111-111111111111:signal:WA_IMPERSONATION_PATTERN`

### Frode finanziaria

D **IBAN beneficiario sintatticamente valido (mod-97) ma istituto ricevente segnalato nel database ScamWatch interno con 14 conferme indipendenti negli ultimi 30 giorni.**

`Evidenza: IBAN richiesto inline a messaggio T+4'30"; codice paese IT, mod-97 OK; banca destinataria ricorre in 14 segnalazioni dossier convergenti.`

`Riferimento: asset:11111111-1111-4111-8111-111111111111:signal:WA_IBAN_REQUEST_INLINE`

## Manipolazione documento

D **Carta d'identità fornita come 'prova' presenta firma EXIF di software di editing (GIMP 2.10) e ELA variance 0.78 sui campi nominativi: manipolazione locale confermata.**
Evidenza: EXIF Software='GIMP 2.10', LastSave 2026-06-01 18:22 UTC (3 ore prima dell'invio); ELA score 0.78 vs soglia 0.45 sui rettangoli NOME/COGNOME/DATA.
Riferimento: asset:22222222-2222-4222-8222-222222222222:signal:EXIF_EDITOR_SIGNATURE

## Integrità metadati

W **Metadati EXIF della camera assenti (Make/Model/DateTimeOriginal nulli): l'immagine non è stata acquisita direttamente dal sensore di un dispositivo, è un derivato esportato.**
Evidenza: Sezione EXIF IFD0: Make=null, Model=null, DateTimeOriginal=null. Solo Software tag popolato. GPS tag assente.
Riferimento: asset:22222222-2222-4222-8222-222222222222:signal:EXIF_CAMERA_MISSING

## Reputazione del numero mittente

D **Numero del mittente classificato MVNO italiano con reputazione 8/10 su Tellows e 3 segnalazioni precedenti su database antiscam pubblici negli ultimi 14 giorni.**
Evidenza: NumVerify: carrier='Iliad Italia (MVNO)', country=IT, line_type=mobile; Tellows scam-score=8/10 (n=47 votes); ScamWatch crosscheck: 3 hit recenti.
Riferimento: asset:11111111-1111-4111-8111-111111111111:signal:WA_PRESSURE_VOCABULARY

# Inventario reperti

### TESTO #1 whatsapp_chat_export.txt

**Hash SHA-256:** `7f8a3b2c1d0e9f87a6b5c4d3e2f1908a5b4c3d2e1f0a9b8c7d6e5f4a3b2c1d0e`
**MIME:** text/plain
**Dimensione:** 4.70 KB
**Acquisito:** `2026-06-02 09:35:12 UTC`

**Segnali**

- D **Codice segnale:** `WA_IMPERSONATION_PATTERN` Pattern impersonificazione familiare: mittente afferma identità del figlio della vittima, motiva cambio numero, urgenza pagamento.
- D **Codice segnale:** `WA_IBAN_REQUEST_INLINE` IBAN richiesto in messaggio inline con linguaggio di urgenza e blocco del numero originale.
- W **Codice segnale:** `WA_PRESSURE_VOCABULARY` Vocabolario tipico di scam familiare: 'mamma', 'urgente', 'non posso chiamare', 'ti spiego dopo'.

### IMMAGINE #2 carta_identita_presunta.jpg

**Hash SHA-256:** `c4d3e2f1a09b8c7d6e5f4a3b2c1d0e9f8a7b6c5d4e3f201a98b7c6d5e4f3a2b1`
**MIME:** image/jpeg
**Dimensione:** 378.1 KB
**Acquisito:** `2026-06-02 09:35:48 UTC`

**Segnali**

- W **Codice segnale:** `EXIF_CAMERA_MISSING` EXIF privo dei tag Make/Model/DateTimeOriginal: immagine non proviene direttamente da camera fisica.
- D **Codice segnale:** `EXIF_EDITOR_SIGNATURE` Software editor 'GIMP 2.10' presente in EXIF Software tag: immagine ri-elaborata prima dell'invio.
- D **Codice segnale:** `ELA_HIGH_VARIANCE` Error Level Analysis: variance score 0.78 (soglia 0.45) sui campi NOME, COGNOME, DATA NASCITA: manipolazione locale rilevata.
- I **Codice segnale:** `BRAND_NO_MATCH` Riconoscimento marchi istituzionali: nessuna corrispondenza con template ufficiali CIE / passaporto IT.

## Analisi delle evidenze forensi

Evidenza E-1 — whatsapp_chat_export.txt (text/plain, 4,8 KB, sha256: 7f8a3b2c1d0e9f87... troncato; cfr. E-1). Si tratta dell'export ASCII nativo del client WhatsApp contenente 8 messaggi scambiati in un intervallo di 25 minuti. La struttura del file è coerente con il formato standard '[gg/mm/aaaa, hh:mm] <mittente>: <testo>'. L'analisi NLP del corpus rileva: 4 marcatori di urgenza ('subito', 'urgente', 'devi farlo ora', 'non posso aspettare'), 3 asserzioni di identità familiare, 1 inserzione di IBAN nel testo a T+4'30'' dall'inizio. La concatenazione temporale è strettamente sequenziale, senza salti, suggerendo che l'export non è stato manipolato a posteriori.

Evidenza E-2 — carta_identita_presunta.jpg (image/jpeg, 378 KB, sha256: c4d3e2f1a09b8c7d... troncato; cfr. E-2). Immagine JPEG progressive Y'CbCr 4:2:0 con quality factor stimato 87. Le tre regioni di interesse identificate dall'algoritmo di layout-detection (NOME, COGNOME, DATA DI NASCITA) presentano residual variance di Error Level Analysis sensibilmente superiore al rumore di fondo del documento (cfr. E-8). Il tag EXIF Software=GIMP 2.10 è dichiarativo: tale signature è inserita automaticamente dal pipeline di salvataggio di GIMP a partire dalla versione 2.10.0 e non può essere prodotta da un workflow di acquisizione camera nativa.

Evidenza E-6 — NumVerify pool + Tellows (cfr. E-6). Il numero mittente è stato sottoposto a lookup multi-sorgente. NumVerify restituisce: country_code='IT', carrier='Iliad Italia (MVNO)', line_type='mobile', valid=true. Tellows restituisce: score=8/10 (alta probabilità scam), tags=['family scam', 'whatsapp', 'urgent payment'], n_votes=47, last_report_age_days=3. Il crosscheck su 3 database antiscam pubblici (rispettivi nomi omessi per finalità didattiche) conferma segnalazioni convergenti.

Evidenza E-7 — ScamWatch DB crosscheck (cfr. E-7). L'IBAN beneficiario, dopo verifica sintattica mod-97 positiva, è stato sottoposto a crosscheck contro la base dati interna LegalAudit. L'istituto ricevente (codice ABI estratto) compare in 14 dossier convergenti negli ultimi 30 giorni, tutti chiusi con verdetto HIGH-RISK e classificazione 'mule account'. La densità temporale (14 hit in 30 giorni) supera la soglia di allerta automatica fissata a 5/30gg.

Evidenza E-8 — Error Level Analysis report (cfr. E-8, E-2). L'analisi ELA è stata condotta secondo la procedura standard di re-compressione a Q=95 e differenza assoluta pixel-by-pixel. I rettangoli identificati corrispondono ai campi anagrafici dichiarati. Variance media: 0,78 ± 0,04; deviazione standard del fondo: 0,12. Il rapporto signal-to-noise è 6,5x, sufficiente a escludere ipotesi di artefatto JPEG sequenziale a una sola fase.

Evidenza E-9 — EXIF dump (cfr. E-9, E-2). L'analisi EXIF è stata condotta con exiftool 12.x. Il tag Software è popolato esplicitamente con 'GIMP 2.10', il tag ModifyDate riporta 2026:06:01 18:22:34, il tag DateTimeOriginal è assente. La combinazione [Software popolato, DateTimeOriginal nullo, Make/Model nulli] esclude l'ipotesi di una semplice ri-compressione e indica un workflow editoriale completo: apertura, modifica, salvataggio.

## Catena di custodia

La catena di custodia segue lo standard ISO 27037 §6.7. I due artefatti (cfr. E-1, E-2) sono stati acquisiti tramite intake protetto della piattaforma alle 09:35:12Z e 09:35:48Z del 2026-06-02. Immediatamente dopo l'acquisizione il motore forense Mythos ha calcolato l'hash SHA-256 di ciascun artefatto, sigillandone l'integrità. L'analisi automatizzata multi-dimensionale ha avuto inizio 30 secondi dopo l'ultimo upload e ha prodotto i segnali catalogati nelle evidenze E-3 fino a E-9.

La generazione del presente dossier ha avuto luogo alle 09:42:00Z. Al momento della generazione il documento è stato sigillato con SHA-256 e anchorato alla catena di audit WORM della piattaforma, garantendo la non-modificabilità retroattiva. Ogni evento di custodia (acquisizione, hashing, analisi, generazione, ancoraggio) è registrato con timestamp UTC e attore responsabile, consultabile nella tabella della sezione successiva.

| Timestamp (UTC) | Attore | Azione | Dettaglio |
|---|---|---|---|
| `2026-06-02 09:35:12 UTC` | Sistema di intake | **Acquisizione** | whatsapp_chat_export.txt (sha256: 7f8a3b2c1d0e9f87...) |
| `2026-06-02 09:35:12 UTC` | Motore forense Mythos | **Hashing SHA-256** | Artefatto 11111111 |
| `2026-06-02 09:35:48 UTC` | Sistema di intake | **Acquisizione** | carta_identita_presunta.jpg (sha256: c4d3e2f1a09b8c7d...) |
| `2026-06-02 09:35:48 UTC` | Motore forense Mythos | **Hashing SHA-256** | Artefatto 22222222 |
| `2026-06-02 09:36:18 UTC` | Motore forense Mythos | **Analisi automatiz…** | Estrazione segnali e correlazione (5 dimensioni) |
| `2026-06-02 09:41:58 UTC` | Motore forense Mythos | **Generazione periz…** | LA-2026-06-02-9F2A1B |
| `2026-06-02 09:42:00 UTC` | WORM audit chain | **Ancoraggio critto…** | Sequenza chain + entry-hash |

## Verdetto di rischio

**ESITO: INDICATORI DI RISCHIO CRITICO**

Confidenza analitica: 94%

HIGH-RISK al 94% di confidenza. Le evidenze convergenti che giustificano il verdetto sono E-1 (pattern conversazionale e richiesta IBAN inline), E-2 (manipolazione del documento d'identità), E-6 (reputazione del numero mittente), E-7 (IBAN destinatario riferito a istituto in lista nera interna) ed E-8 ed E-9 (ELA + EXIF concordi sulla manipolazione). Tre dei cinque indicatori sono classificati 'danger' provenienti da artefatti tecnicamente indipendenti, soglia operativa minima per il verdetto HIGH-RISK secondo la metodologia LegalAudit (cfr. sezione 'Metodologia forense').

## Raccomandazioni operative

Priorità P0 — entro le prossime 24 ore. Blocco immediato del bonifico presso il proprio istituto bancario citando il presente dossier (numero caso LA-2026-06-02-9F2A1B). Conservazione integra del telefono e dell'export WhatsApp, senza ulteriori interazioni con il mittente. Notifica al figlio o familiare il cui numero è stato impersonificato perché possa cambiare le credenziali di accesso ai propri account principali (cfr. E-1).

Priorità P1 — entro 7 giorni. Presentazione di querela ex artt. 640 c.p. (truffa) e 494 c.p. (sostituzione di persona) presso la più vicina Stazione/Commissariato di Polizia o tramite il portale online della Polizia Postale e delle Comunicazioni, allegando il presente dossier. Richiesta formale al proprio istituto della procedura di blocco e congelamento del conto destinatario (codice ABI estratto da E-7) prevista dalla normativa antiriciclaggio D.lgs. 231/2007.

Priorità P2 — consolidamento (entro 30 giorni). Cambio password e attivazione two-factor authentication sugli account critici (cfr. E-1 per il vettore impersonificazione). Iscrizione del numero del mittente nelle blocklist personali. Monitoraggio del conto corrente per 90 giorni per rilevare eventuali tentativi correlati. Conservazione del dossier come allegato probatorio per eventuali contestazioni civili o procedimenti di rimborso bancario.

1. **Subito** Blocca immediatamente il bonifico presso il proprio istituto (P0).
2. **Subito** Sporgi querela ex art. 640 c.p. e art. 494 c.p. presso la Polizia Postale.
3. **Presto** Richiedi al tuo istituto la procedura di congelamento del conto ricevente (P1).
4. **Presto** Conserva integri il telefono e tutti i materiali; non rispondere ulteriormente.
5. **Quando puoi** Notifica il numero impersonato (figlio) e cambia password account critici (P2).

## Dichiarazione di indipendenza e limiti

Il sottoscritto motore forense Mythos, operante per conto di LegalAudit SA con sede in Lugano (Svizzera), dichiara di non avere alcun rapporto di interesse con le parti coinvolte nel presente caso. L'analisi è stata condotta esclusivamente sull'evidenza fornita dal richiedente al momento dell'intake, senza intervento di terze parti e senza accesso a sistemi non autorizzati.

I limiti dell'analisi sono i seguenti: l'analisi è statica e non prevede esecuzione dinamica di payload o fuzzing; non è stato effettuato imaging fisico né analisi hardware del dispositivo del richiedente; le conclusioni sono di natura probabilistica e fondate sull'evidenza concretamente disponibile al momento della generazione; il presente documento non sostituisce e non costituisce parere legale ai sensi della legislazione italiana, svizzera o europea.

## Metodologia forense

La presente perizia è stata redatta secondo le linee guida di ISO 27037:2012 per l'identificazione, raccolta, acquisizione e conservazione dell'evidenza digitale, in combinazione con NIST SP 800-86 per la risposta forense e ENISA ETL per i pattern di minaccia europei.

Ogni artefatto digitale fornito dal richiedente è stato sottoposto ad un'analisi multi-dimensionale standardizzata: integrità (SHA-256, EXIF/IPTC/XMP, Error Level Analysis), origine AI (C2PA, SynthID, AIDE statistici), contenuto OCR con estrazione automatica di IBAN, numeri di telefono, URL e indicatori di urgenza, riconoscimento visivo di marchi istituzionali, e (per file PDF) scansione strutturale via pdfid e pdf-parser con estrazione del JavaScript embedded.

Le segnalazioni a livello 'danger' o 'warn' richiedono almeno 3 segnali indipendenti convergenti per concorrere a un verdetto di rischio elevato. L'identità dei tool utilizzati e le rispettive versioni sono riportate in calce al documento per garantire la riproducibilità.

Il documento è anchorato alla catena di audit WORM (Write-Once-Read-Many) della piattaforma. Il numero di sequenza e l'hash crittografico riportati garantiscono che il documento, una volta generato, non può essere modificato senza che la catena risulti rotta.

#### Standards: ISO 27037, NIST SP 800-86, ENISA ETL.

La metodologia LegalAudit-Mythos si fonda su tre framework di riferimento internazionali: ISO/IEC 27037:2012 per l'identificazione, raccolta, acquisizione e conservazione dell'evidenza digitale; NIST SP 800-86 per la pipeline forense in incident response (collection -> examination -> analysis -> reporting); ENISA Threat Landscape per i pattern di minaccia europei e la tassonomia dei vettori di frode.

Per ogni artefatto digitale ricevuto la pipeline procede in 5 fasi: (1) intake sicuro con SHA-256 immediato e isolamento in sandbox; (2) analisi multi-dimensionale standardizzata che include integrità (hash, EXIF/IPTC/XMP, ELA), origine AI (C2PA, SynthID, AIDE statistici), contenuto OCR con estrazione di IBAN/telefoni/URL/indicatori di urgenza, riconoscimento visivo di marchi istituzionali e (per file PDF) scansione strutturale; (3) crosscheck su database interni (ScamWatch) e fonti pubbliche (Tellows, NumVerify, urlscan.io, VirusTotal); (4) sintesi dei segnali e calcolo della confidenza aggregata; (5) generazione del dossier court-grade.

Per attribuire il verdetto HIGH-RISK la metodologia richiede la convergenza di almeno tre segnali indipendenti classificati 'danger', provenienti da artefatti o sorgenti tecnicamente distinte. Nel presente caso la soglia è ampiamente superata: cinque dimensioni indipendenti convergono, tre delle quali in classe 'danger' (cfr. E-1, E-2, E-7).

L'identità di tutti gli strumenti utilizzati e le rispettive versioni sono riportate nella sezione 'Strumentazione forense impiegata', a garanzia di riproducibilità. Il documento è anchorato alla catena di audit WORM della piattaforma per garantire la non-modificabilità retroattiva.

## Strumentazione forense impiegata

| Strumento | Versione | Fornitore | Note |
|---|---|---|---|
| **Mythos forensic engine** | `2026.06` | LegalAudit SA | Orchestrator, prompt synthesis, evidence catalogue |
| **pdf-lib** | `1.17.1` | OSS | PDF renderer for the dossier |
| **QRCode (node-qrcode)** | `1.5.x` | OSS | Cover-page verify QR generation |
| **Node.js crypto** | `22.19.0` | Node Foundation | SHA-256, hashing, audit chain |
| **URL scanner (LegalAudit)** | `1.0` | - | HTTP/TLS posture + reputation |
| **Mythos OCR + EXIF + ELA analyzer** | `1.0` | LegalAudit SA | OCR + EXIF + brand recognition + Error Level Analysis |
| **AI-origin orchestrator (C2PA / …** | `1.0` | - | AI-generated content detection |
| **NumVerify pool + Tellows** | `1.0` | - | Phone carrier + scam-score lookup |

# Appendice — Catalogo evidenze

Il catalogo che segue elenca, in ordine canonico, tutte le evidenze raccolte e referenziate nel presente dossier. Le prime due voci (E-1, E-2) corrispondono agli artefatti caricati dal richiedente; le voci successive (E-3 .. E-9) corrispondono agli output dei tool forensi e ai record di crosscheck su database interni. Ogni evidenza è identificata da un codice canonico E-N, riferito da tutte le sezioni precedenti tramite la formula "cfr. E-N".

## Catalogo evidenze (E-N)

| ID | Tipo | SHA-256 | Acquisita | Etichetta |
|---|---|---|---|---|
| E-1 | Testo | `7f8a3b2c1d0e9f87a6b5c4d3e2f…` | `2026-06-02 09:35` | whatsapp_chat_export.txt |
| E-2 | Immagine | `c4d3e2f1a09b8c7d6e5f4a3b2c1…` | `2026-06-02 09:35` | carta_identita_presunta.jpg |
| E-3 | Output strumento | - | - | URL scanner (LegalAudit) - HTTP/TLS posture + reputation |
| E-4 | Output strumento | - | - | Mythos OCR + EXIF + ELA analyzer - OCR + EXIF + brand recognition + Error Level Analysis |
| E-5 | Output strumento | - | - | AI-origin orchestrator (C2PA / SynthID / AIDE / Binoculars) - AI-generated content detection |
| E-6 | Output strumento | - | - | NumVerify pool + Tellows - Phone carrier + scam-score lookup |
| E-7 | Crosscheck ScamWatch | - | `2026-06-02 09:35` | ScamWatch DB crosscheck: IBAN beneficiario - 14 segnalazioni convergenti (30gg) |
| E-8 | Report ELA | - | `2026-06-02 09:35` | ELA report carta_identita_presunta.jpg - variance 0.78 (soglia 0.45) |
| E-9 | Report EXIF | - | `2026-06-02 09:35` | EXIF dump carta_identita_presunta.jpg - Software=GIMP 2.10 |

## Nota legale

Il presente documento è una perizia tecnica forense redatta ai sensi del diritto svizzero (sede di LegalAudit SA, Lugano) e in conformità con le linee guida UE/CH applicabili (eIDAS, GDPR/nLPD).

Il contenuto NON sostituisce un parere legale. Per qualsiasi disputa, contestazione o procedimento, si raccomanda di consultare un avvocato qualificato nella giurisdizione competente.

La piattaforma LegalAudit (Mythos) opera come strumento di supporto tecnico e analisi forense. Le conclusioni espresse hanno natura probabilistica e sono fondate sull'evidenza concretamente disponibile al momento della generazione; nuove evidenze possono modificarle.

Il presente documento è coperto da SHA-256 e anchorato alla catena di audit WORM della piattaforma. La verifica indipendente è accessibile tramite il QR code in copertina.

DOCUMENTO DIDATTICO SINTETICO. Tutti i dati anagrafici, numeri di telefono, codici IBAN e identificatori dei conti contenuti in questa perizia sono fittizi e non corrispondono a soggetti reali.

**Riferimenti normativi:**

- art. 359 c.p.p. — Consulenti tecnici del pubblico ministero
- art. 220 c.p.p. — Oggetto della perizia
- art. 640 c.p. — Truffa
- art. 494 c.p. — Sostituzione di persona
- art. 615 ter c.p. — Accesso abusivo a sistema informatico
- Reg. UE 2016/679 (GDPR) e D.lgs. 196/2003 (Codice Privacy)
- D.lgs. 231/2007 (antiriciclaggio)
- Conv. Budapest 2001 sulla criminalità informatica