Ordine degli Ingegneri
della Provincia di Palermo

Evento Formativo

INFORMATICA FORENSE

Relatore: ing. Dario Ferrante
Data: 02/04/2026
Responsabile scientifico: ing. Dario Ferrante

Agenda

Ordine degli Ingegneri
della Provincia di Palermo

01 

L’informatica forense per fini di Giustizia
Relatore: ing. Dario Ferrante

02 

Acquisizione, custodia ed analisi di fonti di prova digitali: Smartphone
Relatore: Brig. Capo CC - dott. Claudio Scaduto

03 

Acquisizione, custodia ed analisi di fonti di prova digitali: Dispositivi di memoria
Relatore: ing. Emanuele Cipolla

L’informatica forense per fini di giustizia

Ordine degli Ingegneri della Provincia di Palermo

Definizione

L'**informatica forense** è la branca delle scienze forensi che si occupa dell'**identificazione**, **preservazione**, **acquisizione**, **analisi** e **presentazione** di evidenze digitali contenute in dispositivi elettronici e sistemi informatici, secondo metodologie scientificamente validate e giuridicamente ammissibili.

Identificazione

Individuare le sorgenti di prova digitale

Acquisizione

Copia forense dei supporti

Analisi

Esame tecnico approfondito dei reperti

Presentazione

Report e testimonianza in sede legale

L’informatica forense per fini di giustizia

Ordine degli Ingegneri della Provincia di Palermo

1. Identificazione

Individuazione dei dispositivi e delle fonti di prova

2. Preservazione

Isolamento e protezione delle prove da alterazioni

3. Acquisizione

Copia forense con strumenti conformi

4. Analisi

Esame dei dati con strumenti certificati

5. Documentazione

Report dettagliato di ogni operazione eseguita

Principio Fondamentale: Integrità dei Dati

Ogni operazione deve garantire la non-alterazione dei dati originali.
L'uso di write-blocker (hardware/software) e la verifica degli hash (MD5, SHA-256) sono obbligatori in ogni fase del processo.

Gli ambiti di applicazione dell’informatica forense

Ordine degli Ingegneri
della Provincia di Palermo

Device Forensics

- File system analysis
- Recupero file cancellati e file carving
- Analisi timeline e artefatti di sistema
- Slack space del cluster e unallocated space
- Mobile device acquisition (iOS/Android)
- Analisi chat, SMS, dati app e geolocalizzazione
- **In generale ogni dispositivo che contiene informazioni digitali**

Network Forensics

- Packet capture & deep packet inspection
- Analisi log di rete e firewall
- Ricostruzione sessioni e flussi di dati
- Analisi DNS, proxy e log di accesso
- Correlazione eventi multi-sorgente
- Tracciamento connessioni e data exfiltration

Cyber Risk Assicurativo

- Ricostruzione della dinamica dell'incidente
- Quantificazione del danno e perimetro di impatto
- Analisi delle cause: errore umano, vulnerabilità, attacco
- Verifica conformità policy assicurativa
- Perizia tecnica forense per la liquidazione del sinistro
- Documentazione probatoria per contenzioso

Quadro Normativo

Il quadro normativo

Quadro Normativo

- L. 48/2008 — Ratifica Conv. Budapest
- Art. 244-254 c.p.p. - Ispezioni e sequestri
- Art. 359-360 c.p.p. - Accertamenti Tecnici
- Art. 191 c.p.p. - Inutilizzabilità
- GDPR e protezione dati personali
- Standard ISO/IEC 27037 — Digital Evidence

Catena di Custodia

- Documentare chi, cosa, quando, dove
- Sigillatura e etichettatura dei reperti
- Registro degli accessi e trasferimenti
- Verifica hash ad ogni passaggio
- Conservazione in ambienti controllati

L. 48/2008
Ratifica convenzione di Budapest

Contesto e Finalità

La Legge 18 marzo 2008, n. 48 ratifica la Convenzione del Consiglio d'Europa sulla criminalità informatica (Budapest, 23.11.2001).
È il pilastro normativo italiano per la digital forensics.

- Introduce reati informatici specifici nel codice penale
- Disciplina le indagini su dati digitali
- Regola la cooperazione internazionale
- Modifica gli artt. 244, 247, 254-bis, 352, 354 c.p.p.

Struttura

Si compone di **14 articoli** che intervengono su tre direttrici: la modifica del codice penale (introducendo nuove fattispecie di reato informatico), la modifica del codice di procedura penale (adeguando gli strumenti investigativi al contesto digitale) e la disciplina della cooperazione giudiziaria internazionale in materia di cybercrime.

Concetto di sistema informatico

Definisce il sistema informatico come "**qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica di dati**".
Questa definizione è volutamente ampia: comprende computer desktop, server, smartphone, tablet, dispositivi IoT, sistemi embedded, infrastrutture cloud. L'aggettivo "telematico" estende il concetto ai sistemi connessi in rete, quindi qualsiasi apparato che trasmette o riceve dati attraverso reti di telecomunicazione.

Il quadro normativo
Art.244/247/254-bis c.p.p.

Ordine degli Ingegneri
della Provincia di Palermo

Art. 244 c.p.p.
Ispezioni

Prima della L. 48/2008

L'ispezione riguardava solo luoghi, persone e cose in senso fisico.

Novità introdotta

Aggiunta la possibilità di disporre l'ispezione di sistemi informatici o telematici, con obbligo di adottare misure tecniche per conservare i dati originali e impedirne l'alterazione.

In pratica

Introduce la possibilità di ispezionare computer, server, smartphone con il vincolo di garantire che il dato non cambi. Fondamento giuridico dell'obbligo di write-blocker e imaging forense.

Art. 247 c.p.p.
Perquisizioni

Comma 1-bis (nuovo)

Estende la perquisizione ai sistemi informatici o telematici, con fondato motivo che contengano tracce del reato.

Obblighi

Misure tecniche per conservazione dati, impedire alterazione e accesso da parte di soggetti non autorizzati.

Differenza con art. 244

La perquisizione è ricerca attiva di elementi specifici; l'ispezione è verifica dello stato. Il decreto del PM può riguardare l'intero sistema o aree logiche (partizioni, account, cartelle).

Art. 254-bis c.p.p.
Sequestro presso ISP

Articolo interamente nuovo

Non esisteva prima della L. 48/2008. Disciplina l'acquisizione di dati presso fornitori di servizi informatici, telematici o di telecomunicazioni.

Modalità

Il sequestro avviene tramite copia dei dati su supporto adeguato, non con asportazione fisica del server. Procedura che garantisca conformità e immodificabilità.

Esempio pratico

Sequestrare email su Libero Mail o log di un hosting provider senza spegnere l'infrastruttura. Il provider deve "congelare" i dati e consegnarli in forma forense.

Il quadro normativo
Art.352 c.p.p. – Art.354 c.p.p.

Art. 352 c.p.p.
Perquisizioni della P.G.

Contesto

Disciplina le perquisizioni che la Polizia Giudiziaria può effettuare di propria iniziativa in situazioni di urgenza e senza attendere il decreto del PM: flagranza, evasione, fondato motivo di occultamento.

Comma 1-bis (L. 48/2008)

Estende la facoltà ai sistemi informatici o telematici, anche se protetti da misure di sicurezza (password, cifratura), quando vi siano fondati motivi di ritenere che contengano dati pertinenti al reato che possano essere cancellati o dispersi.

Aspetto cruciale

La PG può procedere d'urgenza prima della convalida del PM, ma con l'obbligo tassativo di adottare misure tecniche per garantire la conservazione dei dati originali e impedirne l'alterazione. La convalida deve intervenire entro 48 ore..

Esempio pratico

Se la PG sorprende qualcuno nell'atto di commettere un reato o immediatamente dopo, può perquisire la persona, i luoghi e (dopo la L.48/2008) i sistemi informatici nella sua disponibilità per cercare il corpo del reato o le cose pertinenti.

Art. 354 c.p.p.
Accertamenti Urgenti

Modifica al comma 2

Integrato per prevedere che, in relazione ai dati informatici, la PG possa compiere accertamenti urgenti sui sistemi adottando misure tecniche per assicurare la conservazione dei dati e impedirne l'alterazione e l'accesso non autorizzato.

Distinzione con art. 360

L'art. 354 riguarda interventi urgenti e conservativi (preservazione). L'art. 360 riguarda accertamenti irripetibili (analisi che altera il dato). Qui non si fa analisi: si "fotografa" lo stato del Sistema e si impedisce l'alterazione del dato, sia essa di natura fortuita che intenzionale.

Finalità

Preservazione d'urgenza: creazione di una copia forense sul posto prima che i dati possano essere alterati o cancellati. Non è un'analisi vera e propria, ma un congelamento della scena digitale.

Esempio pratico

La PG si trova davanti a un server che qualcuno sta per formattare: l'art. 354 legittima l'intervento immediato di copia forense bit-a-bit senza attendere il PM.

Art. 359 c.p.p.
Accertamento Ripetibile

Definizione

Il PM nomina consulenti tecnici per accertamenti che non alterano l'oggetto dell'analisi. L'operazione può essere ripetuta in qualsiasi momento successivo ottenendo lo stesso risultato.

Avviso alla difesa

Non richiesto. Non c'è pregiudizio per l'indagato: l'accertamento potrà sempre essere replicato e verificato autonomamente dalla difesa.

Contraddittorio

Nessun contraddittorio preventivo. Il PM ha piena discrezionalità nella nomina e nell'affidamento del quesito. La difesa contesterà i risultati in dibattimento.

Esempio forense

Analisi di una copia forense bit-a-bit: il consulente lavora sull'immagine, l'originale resta sigillato. Hash verificabile in ogni momento. La difesa può creare una nuova copia e ripetere l'analisi.

Conseguenza se violato

Nessuna sanzione processuale specifica. I risultati restano utilizzabili.

Art. 360 c.p.p.
Accertamento Irripetibile

Definizione

Accertamenti che per loro natura modificano irreversibilmente l'oggetto. Una volta eseguiti, la cosa o il dato non saranno più nello stesso stato e nessuno potrà ripetere l'operazione nelle stesse condizioni.

Avviso alla difesa

Obbligatorio. Il PM deve comunicare giorno, ora, luogo dell'accertamento e la facoltà di nominare consulenti tecnici propri. La difesa ha diritto di presenziare.

Contraddittorio

Garantito. La difesa partecipa con un proprio consulente che assiste a tutte le operazioni e può formulare osservazioni e riserve a verbale.

Esempio forense

Acquisizione della memoria RAM di un sistema acceso: la RAM è volatile, il sistema si modifica durante il dump, e una volta spento quei dati sono persi per sempre. Mai più ripetibile.

Conseguenza se violato

Inutilizzabilità assoluta della prova (art. 191 c.p.p.). Esclusione totale dal fascicolo: sanzione processuale irreversibile.

Il quadro normativo
Art.191 c.p.p. – Inutilizzabilità

Ordine degli Ingegneri
della Provincia di Palermo

Norma

"Le prove acquisite in violazione dei divieti stabiliti dalla legge non possono essere utilizzate." (Art. 191 comma 1 c.p.p.)

Natura giuridica

Sanzione processuale più grave del c.p.p. Soggetta a legalità e tassatività: solo la legge può stabilire un divieto probatorio. Non estensibile per analogia.

Caratteristiche

Tassativa

Opera solo nei casi espressamente previsti dalla legge. Non estensibile per analogia né per interpretazione.

Insanabile

Il vizio è radicale e permanente: non può essere convalidato o sanato in alcun modo successivo.

Rilevabile d'ufficio

Il giudice la rileva autonomamente in ogni stato e grado, inclusa la Cassazione, anche senza eccezione di parte.

Non si propaga (regola generale)

Il vizio dell'atto di ricerca (es. perquisizione) non si trasferisce automaticamente agli atti successivi autonomi (es. sequestro corpo del reato). Principio: male captum, bene retentum.

Inutilizzabilità DIRETTA (scatta art. 191 c.p.p.)

L'atto stesso viola un divieto probatorio di legge. I risultati sono direttamente inutilizzabili perché il divieto è nell'atto che produce la prova.

- **Art. 360 violato**: accertamento irripetibile senza avviso difesa → i dati estratti dall'analisi sono inutilizzabili
- **Art. 271 c.p.p.:** intercettazioni eseguite fuori dai casi di legge → inutilizzabili
- **Art. 103 c. 7 c.p.p.:** perquisizioni in violazione garanzie difensore → risultati inutilizzabili

Giurisprudenza di riferimento

Cass. S.U. n. 5021/1996	Sentenza fondante: il sequestro è "atto dovuto", il vizio della perquisizione non si propaga.
Corte Cost. n. 332/2001	Primo intervento costituzionale confermativo.
Corte Cost. n. 219/2019	Inammissibilità: materia riservata al legislatore, natura eccezionale e tassativa.
Corte Cost. n. 252/2020	Manifesta inammissibilità: deterrente abusi affidato a responsabilità disciplinare e penale della PG.

Concetti fondamentali e processi

Best practice

Preservare l'Integrità

Non intervenire mai su un dispositivo senza gli strumenti adatti. Documentare lo stato iniziale con foto e video.

Documentare Tutto

Ogni azione deve essere tracciabile: orari, operatori, strumenti utilizzati, risultati ottenuti.

Utilizzo di Strumenti Validati

Utilizzare solo software e hardware certificati e mantenere traccia delle versioni utilizzate.

Formazione continua

Formazione permanente e aggiornamento su nuove tecnologie, minacce e giurisprudenza.

Funzione di Hash Crittografico

Standard attuali

- **MD5 (128 bit) -** Veloce, legacy
- **SHA-1 (160 bit) -** Deprecato
- **SHA-256 (256 bit)** - Standard usato
- **SHA-384 (384 bit)** - Maggiore Sicurezza
- **SHA-512 (512 bit)** - Massima sicurezza

Definizione

In informatica forense, l'hash (o *digest crittografico*) è una stringa alfanumerica di lunghezza fissa, generata da un algoritmo matematico applicato al **contenuto binario di un file**. Funziona come un'impronta digitale univoca: qualsiasi modifica al file, anche di un singolo bit, produce un hash completamente diverso

.

Le proprietà fondamentali che lo rendono utile in informatica forense sono:

Determinismo: lo stesso file produce sempre lo stesso hash

Non invertibilità: dall'hash non è possibile risalire al contenuto originale.

Effetto valanga: una minima variazione nell'input produce un output radicalmente diverso.

Resistenza alle collisioni: è computazionalmente impossibile trovare due file diversi con lo stesso hash (per gli algoritmi moderni).

In ambito forense, l'hash è lo strumento principale per certificare l'integrità di una prova digitale: se l'hash calcolato al momento dell'acquisizione coincide con quello ricalcolato in seguito, il file non è stato alterato.

Metadati e Hash Crittografico

Principio base

L'hash viene calcolato sull'intera sequenza di byte del file, inclusi tutti i dati incorporati nella sua struttura binaria.

Conseguenza

I metadati, se fisicamente inclusi nel file, fanno parte di quei byte e modificano l'hash. Bisogna distinguere due categorie:

INTERNI → Modificano l'hash

ESTERNI → Nessun effetto

Metadati Interni al File (Embedded Metadata)

Fanno parte del contenuto binario quindi modificano l'hash

Documenti Office

DOCX, XLSX, PPTX (ZIP/XML)

- Autore, co-autori
- Date creazione / ultima modifica
- Nome azienda / organizzazione
- Commenti e revisioni tracked
- Versione software, template, UUID

Immagini

JPEG, TIFF, PNG, RAW

- EXIF: data/ora, GPS, fotocamera, obiettivo
- IPTC: copyright, didascalie, keyword
- Profilo colore ICC embedded
- Thumbnail embedded nel JPEG
- Dati XMP (Adobe)

File PDF

Portable Document Format

- Titolo, autore, soggetto, parole chiave
- Data creazione / modifica
- Producer / Creator software
- UUID e numero revisioni incrementali
- Font incorporati e relativi metadati

Audio / Video

MP3, MP4, MKV

- Tag ID3: titolo, artista, album
- Copertina album come flusso dati
- Metadati container: codec, bitrate
- Durata e dati tecnici nel header
- Sottotitoli e capitoli embedded

In ambito forense: qualsiasi operazione che modifica anche un solo byte del file ne invalida l'hash e compromette la prova.

Metadati del Filesystem (Esterni al File)

NON fanno parte del contenuto binario e quindi non modificano l'hash del file

Metadato	Effetto sull'hash
Nome del file	Nessuno
Percorso / cartella	Nessuno
Data creazione (File System)	Nessuno
Data ultima modifica (File System)	Nessuno
Data ultimo accesso	Nessuno
Attributi (nascosto, r/o)	Nessuno
Permessi UNIX (chmod)	Nessuno
Proprietario (owner/group)	Nessuno

Gestiti dal filesystem (NTFS, ext4, APFS) e risiedono nelle strutture di directory, esterne al flusso dati del file.

Casi Pratici di variazione dell'Hash

1

Copia di un file JPEG

Copiare un'immagine da una cartella all'altra non modifica l'hash: il contenuto binario resta identico. Ma se il software aggiorna il thumbnail embedded o i metadati EXIF, l'hash cambia.

2

"Salva con nome" in Word

Un documento Word risalvato può avere hash diverso anche senza modifiche al testo: Word aggiorna automaticamente data modifica, contatore revisioni e autore nei metadati interni.

3

Rimozione metadati

Strumenti come ExifTool o "Rimuovi proprietà" di Windows modificano fisicamente i byte del file e di conseguenza l'hash cambia e la prova risulta alterata ai fini forensi.

4

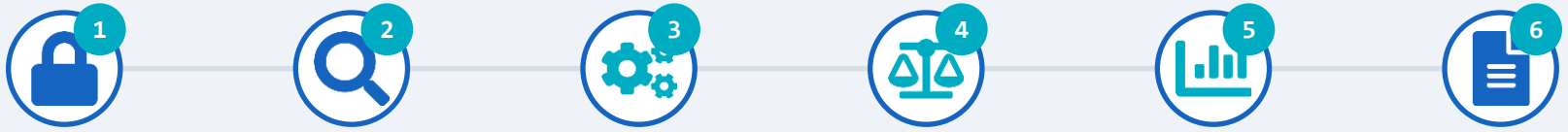
Compressione o ricodifica

Ricodificare un video o una foto (anche alla stessa qualità) produce sempre un hash completamente diverso: la sequenza di byte viene ricalcolata dall'encoder.

Il tema Cyber Risk

Perizia cyber risk
Metodologia dell'ingegnere forense

Ordine degli Ingegneri
della Provincia di Palermo



1. Ingaggio e Preservazione

- Ricevere incarico formale dall'assicurato o dal broker/compagnia
- Acquisire copia della polizza cyber e delle condizioni particolari
- Emettere direttiva di preservazione: nessun sistema deve essere alterato, ripristinato o reinstallato prima dell'acquisizione forense
- Documentare lo stato della scena: foto, screenshot, log attivi, sistemi accesi/spenti

2. Acquisizione Forense

- Imaging forense bit-a-bit dei sistemi coinvolti (dischi, server, VM, cloud snapshot)
- Acquisizione log: firewall, IDS/IPS, SIEM, Active Directory, VPN, proxy, DNS
- Acquisizione email sorgente (header completi) relative all'incidente
- Calcolo e verbalizzazione hash (SHA-256) di ogni reperto acquisito

3. Analisi Tecnica

- Ricostruzione della timeline: quando è iniziato l'attacco, come si è propagato, quando è stato rilevato
- Identificazione del vettore: phishing, vulnerabilità, credenziali compromesse, insider
- Analisi del malware (se presente): tipo, comportamento, IOC (Indicators of Compromise)
- Mappatura dei sistemi e dati impattati: perimetro esatto dell'incidente

4. Verifica di Polizza

- Confronto tra dinamica accertata e definizione di "evento cyber" in polizza
- Verifica obblighi dell'assicurato: misure di sicurezza minime, tempistica di notifica, obblighi di mitigazione
- Verifica esclusioni: atti dolosi interni, guerra, sanzioni, mancato aggiornamento critico
- Verifica conformità GDPR: notifica Garante entro 72h (art. 33) se dati personali coinvolti

5. Quantificazione del Danno

- **Danno diretto**: costi di incident response, bonifica, ripristino sistemi, sostituzione hardware
- **Business interruption**: mancato ricavo durante il downtime, costi operativi aggiuntivi
- **Costi di notifica e gestione data breach**: comunicazioni, call center, credit monitoring
- **Danni a terzi**: richieste risarcitorie, sanzioni del Garante, penali contrattuali

6. Relazione Peritale

- Descrizione dell'incarico e quesiti ricevuti
- Metodologia seguita e strumenti utilizzati (con versioni)
- Ricostruzione cronologica con evidenze a supporto
- Quantificazione dettagliata e risposta ai singoli quesiti
- Allegati: hash, catena di custodia, log, screenshot

Perizia cyber risk
Relazione peritale e criticità

Ordine degli Ingegneri
della Provincia di Palermo

Struttura della Relazione Peritale

1. Premessa e Incarico

Identificazione delle parti, data incarico, quesiti posti dalla compagnia o dal loss adjuster, polizza di riferimento con numero e decorrenza.

2. Descrizione dell'Assicurato

Attività aziendale, infrastruttura IT, numero dipendenti, dati trattati, misure di sicurezza preesistenti, certificazioni (ISO 27001, ecc.).

3. Descrizione dell'Evento

Cronologia dell'incidente: data di prima compromissione, data di rilevamento, data di contenimento, data di ripristino. Vettore di attacco identificato.

4. Attività Peritali Svolte

Acquisizioni forensi effettuate, strumenti utilizzati (con versione), hash calcolati, catena di custodia, analisi condotte.

5. Risultanze Tecniche

Ricostruzione dettagliata della dinamica con evidenze. Ogni affermazione deve essere supportata da un artefatto forense documentato.

6. Verifica Operatività di Polizza

Conformità dell'evento alla definizione contrattuale, rispetto degli obblighi, assenza di esclusioni applicabili.

7. Quantificazione del Danno

Tabella analitica delle voci di danno con documentazione a supporto (*fatture, preventivi, log downtime, calcolo mancato ricavo*).

8. Conclusioni e Risposta ai Quesiti

Sintesi e risposta puntuale a ciascun quesito ricevuto.

Errori critici da evitare

- Ripristinare i sistemi prima dell'acquisizione forense: le evidenze vengono distrutte irreversibilmente
- Operare senza preservare la catena di custodia: la perizia perde valore probatorio
- Quantificare il danno senza documentazione a supporto: la compagnia contesterà ogni voce
- Ignorare gli obblighi di polizza: se l'assicurato non ha rispettato le condizioni, il sinistro può essere declinato
- Non verificare la notifica GDPR: l'omessa notifica entro 72h può generare sanzioni autonome

Principi guida dell'ingegnere forense

Indipendenza
Il perito agisce come terzo tecnico imparziale, non come consulente di parte. Le conclusioni devono essere oggettive e ripetibili.

Tracciabilità
Ogni operazione deve essere documentata: strumento, versione, parametri, hash, data e ora. Il verbale è la garanzia della perizia.

Proporzionalità
Acquisire ciò che è necessario e pertinente, non l'intero patrimonio informativo aziendale. Minimizzazione anche nel rispetto del GDPR.

Curiosità forensi

Email Forensics
Certificazione di una email

Ordine degli Ingegneri
della Provincia di Palermo

Ciò che vede l'utente

Da: Mario Rossi <m.rossi@studiorossi.it>

A: Luigi Bianchi <l.bianchi@impresa.it>

Data: 10 Gen 2026 — 14:33

Ogg: Disdetta contratto di fornitura

Con la presente comunico la volontà di recedere dal contratto n. 2024/187 con effetto dal 28 febbraio 2026.
Distinti saluti, Avv. Mario Rossi

L'utente vede solo: Da, A, Data, Oggetto, Corpo

Ciò che vede l'ingegnere forense

```
Received: from smtp.studiorossi.it
  (93.42.xx.xx) by mx.impresa.it; 10 Jan 14:33:12
Received: from [192.168.1.10] by smtp.studio
  rossi.it; 10 Jan 2026 14:33:04 +0100
Message-ID: <d4e8a1c@smtp.studiorossi.it>
Date: Fri, 10 Jan 2026 14:33:02 +0100 (CET)
From: "Mario Rossi" <m.rossi@studiorossi.it>
To: "Luigi Bianchi" <l.bianchi@impresa.it>
X-Mailer: Microsoft Outlook 16.0
Authentication-Results: mx.impresa.it;
  spf=pass dkim=pass  dmarc=pass
X-Originating-IP: 93.42.xx.xx (Milano, IT)
```

Timestamp certificato
Date + Received: data e ora con fuso orario (CET), prova del momento esatto di invio

Percorso SMTP
I Received tracciano ogni server attraversato: prova della rotta e dei nodi coinvolti

Autenticità verificata
SPF/DKIM/DMARC pass: il server era autorizzato dal dominio, il messaggio è integro

Identità univoca
Message-ID irripetibile + IP di origine: collegamento univoco mittente-messaggio

Email Forensics
Certificazione di una email

Ordine degli Ingegneri
della Provincia di Palermo

Header "Received" – Gli IP in passaggio

Cosa sono

Ogni server SMTP che riceve e inoltra l'email aggiunge in testa al messaggio un header "Received:" con il proprio indirizzo IP, il nome del server, e il timestamp preciso del passaggio. Si leggono dal basso verso l'alto: l'ultimo Received è il primo server, il primo è l'ultimo.

Esempio di catena Received (dal basso verso l'alto)

```
③ Received: from smtp.studiorossi.it (93.42.xx.xx)
      by mx.impresa.it; Fri, 10 Jan 2026 14:33:12 +0100
② Received: from [192.168.1.10]
      by smtp.studiorossi.it; Fri, 10 Jan 2026 14:33:04 +0100
① Origine: PC dell'avvocato (IP privato 192.168.1.10 o pc hostname)
```

Valore forense degli IP in passaggio

- Ogni hop SMTP è un testimone indipendente: IP, hostname e timestamp certificano il transito
- L'IP pubblico (es. 93.42.xx.xx) è geolocalizzabile e associabile a un ISP/organizzazione tramite WHOIS
- I timestamp di ogni hop permettono di ricostruire la cronologia esatta con precisione al secondo
- La differenza di orario tra hop consecutivi rivela ritardi anomali o manipolazioni

Message-ID

Cos'è
Stringa univoca generata automaticamente dal server SMTP al momento dell'invio. Formato: <identificativo_unico@dominio_server>.

Perché è irripetibile
Combina timestamp ad alta precisione, ID di processo del server, contatore incrementale e nome del dominio. La probabilità statistica di collisione è praticamente nulla: nessun altro messaggio avrà mai lo stesso Message-ID.

Altri header identificativi

X-Originating-IP
IP del dispositivo che ha composto l'email (non del server). Geolocalizzabile, associabile all'utente fisico tramite log ISP. Questo dato comincia a perdere di interesse dalla diffusione dei webclient email.

Email Forensics
Certificazione di una email

Ordine degli Ingegneri
della Provincia di Palermo

SPF

Sender Policy Framework

Cos'è

Record DNS (tipo TXT) pubblicato dal dominio del mittente che elenca gli IP autorizzati a inviare email per conto di quel dominio.

Come funziona

Il server ricevente confronta l'IP del server che ha consegnato l'email con la lista di IP autorizzati nel record SPF del dominio mittente.

Risultato

pass = IP autorizzato
fail = IP non autorizzato
none = nessun record SPF
softfail = non autorizzato ma tollerato

Valore forense

Certifica che il server di invio era legittimamente autorizzato dal dominio. Un "pass" prova che il dominio ha delegato quel server all'invio.

DKIM

DomainKeys Identified Mail

Cos'è

Sistema di firma crittografica: il server mittente appone una firma digitale sugli header e sul corpo del messaggio usando una chiave privata.

Come funziona

Il server ricevente recupera la chiave pubblica dal DNS del dominio mittente e verifica la firma. Se il messaggio è stato alterato in transito, la verifica fallisce.

Risultato

pass = firma valida, messaggio integro
fail = firma non valida, possibile alterazione
none = nessuna firma DKIM

Valore forense

Prova l'integrità del contenuto: il messaggio non è stato modificato dal momento della firma. Equivalente concettuale dell'hash nel contesto email.

DMARC

Domain-based Message Auth.

Cos'è

Policy DNS pubblicata dal dominio che indica ai server riceventi cosa fare se SPF e/o DKIM falliscono. Unifica i due protocolli in un'unica direttiva.

Come funziona

Verifica l'allineamento: il dominio nel "From:" visibile deve corrispondere al dominio verificato da SPF e/o DKIM. Senza allineamento, anche con SPF pass il DMARC fallisce.

Risultato

pass = allineato + SPF/DKIM ok
fail = disallineamento o entrambi falliti
Policy: none / quarantine / reject

Valore forense

Certifica che il mittente visibile (From:) corrisponde effettivamente al dominio autenticato. È la prova più forte di autenticità del mittente.

Artefatti forensi
“Hai una chiavetta USB da prestarmi?”

Ordine degli Ingegneri
della Provincia di Palermo

Serial Number Hardcoded

Il numero di serie USB è scritto nel firmware del controller ed è immutabile dall'utente.

Registro di Sistema

USBSTOR registra Vendor ID, Product ID, serial number e revisione firmware automaticamente.

Timestamp Multipli

setupapi.dev.log → primo inserimento; Event Log → ogni plug/unplug con precisione al secondo.

Lettera di Unità & VSN

MountedDevices traccia la lettera assegnata; il Volume Serial Number del file system viene correlato.

Valore Probatorio

Il collegamento tra dispositivo specifico e PC specifico è estremamente robusto: il serial number non è falsificabile dall'utente comune.

ANCHE POCHI SECONDI BASTANO

Un inserimento senza alcuna interazione utente lascia tracce sufficienti a dimostrare quale dispositivo, su quale macchina, quando e per quanto tempo.

Conclusioni

Consigli pratici

Operare solo in caso di assoluta certezza procedurale e solo se a conoscenza del sistema su cui si sta operando.

Oltre che Tecnici dobbiamo essere concoscitori del c.p.p. per quanto concerne il nostro ambito operativo.
Un errore procedurale può invalidare la prova o peggio portarci a rispondere di errori di operato.

Formarsi e aggiornarsi è un tema estremamente importante per rimanere allineati con l'evoluzione delle procedure e fornire una prestazione di qualità

È caldamente consigliato per chi opera nel settore dell'informatica forense valutare una RC professionale con estensione di copertura Cyber Risk (*diffusa e relativamente economica*), anche se in generale è buona prassi per tutti i professionisti che trattano nel quotidiano dati informatizzati.

Ordine degli Ingegneri
della Provincia di Palermo

Grazie per l’attenzione