



tinexta
defence

Dati Senza Confini

La Digital Forensics riscrive
la privacy

#TinextaDefenceBusiness

DFIR

Il Gruppo DFIR di Tinexta Defence è una Threat Response Unit specializzata in Digital Forensics & Incident Response che supporta imprese e pubbliche amministrazioni nella gestione di incidenti di sicurezza e nella produzione di evidenze digitali con valore probatorio.

L'attività del Gruppo integra competenze multidisciplinari e si articola in quattro aree principali:

- **Incident Response:** capacità di intervento rapido per contenere, eradicare e mitigare incidenti, riducendo l'impatto operativo;
- **Consulenze Tecniche d'Ufficio (CTU) e di Parte (CTP):** perizie informatiche conformi alle best practice di catena di custodia, a supporto del contesto giudiziario;
- **Forensic Readiness:** predisposizione preventiva di processi, tecnologie e standard per garantire che i dati raccolti siano accurati, integri e attestabili;
- **Ricerca e innovazione:** sperimentazione di tecnologie avanzate (eBPF, kernel telemetry, AI per anomaly detection, container forensics) per anticipare le minacce e sviluppare strumenti di nuova generazione.

In qualità di Threat Response Unit, il Gruppo DFIR non si limita alla fase di indagine post-evento, ma affianca i Security Operations Center (SOC) e le organizzazioni nella detection proattiva, nel threat hunting e nella gestione di crisi cyber.

La missione del Gruppo è elevare i livelli di sicurezza e resilienza delle infrastrutture critiche e dei sistemi informativi, coniugando rigore scientifico, innovazione tecnologica e capacità operativa a supporto della difesa digitale e del contesto giudiziario.

Sommario

Abstract	04
Introduzione	05
Capitolo 1 – La Digital Forensics oggi	06
Capitolo 2 – Privacy e rischi: un nuovo modello di minacce nella Digital Forensics	07
Capitolo 3 – Nuove tecnologie e il loro impatto sulla Digital Forensics	09
Capitolo 4 – Sicurezza vs Diritti: il contesto europeo	10
Conclusioni	12
Bibliografia	13

Abstract

La digital forensics contemporanea si estende ben oltre la semplice acquisizione di dispositivi fisici, coinvolgendo cloud, dispositivi mobili, IoT, blockchain e intelligenza artificiale, con impatti significativi sulla sicurezza e sulla gestione dei dati personali. L'analisi mette in luce come l'espansione delle capacità investigative comporti nuove minacce alla privacy, dalla raccolta massiva di dati non pertinenti all'esposizione di informazioni sensibili di terzi. Tuttavia, spesso è necessario analizzare dati personali, come conversazioni private, per individuare informazioni rilevanti ai fini dell'indagine.

Il report propone strategie concrete per conciliare efficacia investigativa e tutela dei diritti fondamentali, tra cui l'uso di sistemi multi-parte per l'accesso ai dati, tecniche di verifica basate su hash e blockchain, ambienti di analisi isolati, funzioni di forensics readiness nei dispositivi IoT e audit periodici dei sistemi AI. L'obiettivo è promuovere un approccio etico, trasparente e legalmente consapevole alla digital forensics, in grado di garantire sicurezza senza compromettere la privacy degli utenti.

Autrice:

- Gaia Calamari: Digital Forensic Analyst

Introduzione

Negli ultimi anni la digitalizzazione ha trasformato radicalmente ogni aspetto dell'esistenza quotidiana, rendendo la vita di ciascun individuo un flusso costante di dati che si generano, transitano, si conservano e vengono elaborati da una molteplicità di piattaforme. Smartphone, servizi in cloud, social media, oggetti connessi nelle nostre case e nei nostri ambienti di lavoro, applicazioni di intelligenza artificiale integrate in attività apparentemente banali: tutto concorre a formare una traccia digitale che racconta molte più informazioni di quante immaginiamo. In questo contesto, la **Digital Forensics**, ovvero l'insieme di procedure volte all'acquisizione, conservazione e analisi delle prove digitali, ha assunto un ruolo centrale non solo per il contrasto al crimine informatico, ma anche per indagini tradizionali, incidenti aziendali, controversie legali e attività di sicurezza nazionale.

La *digital forensics* di oggi è un campo vastissimo che va ben oltre la semplice copia forense di un disco rigido. Riguarda infrastrutture cloud distribuite, reti complesse, dispositivi IoT, sistemi di controllo industriale, comunicazioni cifrate, intelligenza artificiale e tanto altro. L'impatto di questa espansione, tuttavia, si scontra inevitabilmente con un tema altrettanto cruciale: la **protezione della privacy** e dei dati personali. Ogni processo forense comporta, infatti, l'accesso potenzialmente invasivo alla vita digitale dei singoli utenti di questi dispositivi. Da questo punto di vista, il 2025 ha rappresentato un anno particolarmente significativo: da un lato si registra un aumento delle capacità investigative e delle necessità legate alla sicurezza; dall'altro, l'Europa e molti altri Paesi hanno e stanno ridefinendo normative e linee guida per evitare che tali capacità degenerino in forme di sorveglianza incontrollata.

L'obiettivo di questo articolo è fornire un quadro organico e contemporaneo sul rapporto tra digital forensics e privacy, analizzando lo stato dell'arte della disciplina, le principali minacce emergenti, l'impatto delle tecnologie più recenti e gli orientamenti normativi che hanno caratterizzato l'ultimo biennio.

Capitolo 1 – La Digital Forensics oggi

La digital forensics, così come si presenta oggi, è profondamente diversa da quella dei primi anni 2000. La crescente complessità dei dispositivi e dei sistemi informativi ha portato alla nascita di sotto-discipline sempre più specializzate e all'evoluzione di tecniche capaci di operare in contesti molto diversi tra loro. Oggi il perito informatico forense non deve limitarsi a saper acquisire un hard disk o recuperare dei file cancellati, ma deve conoscere servizi cloud, tecniche di network forensics, web forensics, mobile forensics, strumenti per il reverse engineering e metodologie per analizzare grandi volumi di dati.

A livello operativo, uno dei cambiamenti più significativi riguarda il passaggio da un mondo "localizzato" a un mondo pienamente **distribuito**. Un tempo il computer era un'entità fisica da analizzare integralmente; oggi la maggior parte delle informazioni risiede su server remoti, spesso dislocati in Paesi diversi, soggetti a normative differenti e accessibili soltanto previa collaborazione con i fornitori di servizi. La crescita del cloud computing ha quindi introdotto problemi di giurisdizione, sicurezza, affidabilità e trasparenza, rendendo necessario un nuovo modo di concepire l'acquisizione forense.

Un altro ambito cruciale è quello dei dispositivi mobili. Lo smartphone è ormai un archivio completo della vita di ognuno di noi: contiene conversazioni, fotografie, dati sanitari, geolocalizzazioni, documenti, cronologie di navigazione, reti sociali e molto altro. Eppure, l'accesso a questi contenuti è sempre più complicato, complice la diffusione di sistemi di cifratura avanzata e di meccanismi di protezione hardware. La mobile forensics moderna non riguarda solo l'acquisizione fisica del dispositivo, ma anche l'estrazione selettiva, la gestione della cifratura e l'analisi delle app, molte delle quali utilizzano protocolli criptati e sincronizzano dati verso il cloud. In parallelo, si assiste a un aumento della complessità nelle attività di network forensics, necessarie per ricostruire attacchi informatici e movimenti laterali nelle reti aziendali.

Uno degli esempi più emblematici è l'indagine sul **caso Sky ECC** (2021–2023), in cui diverse forze di polizia europee riuscirono ad accedere a una piattaforma di messaggistica criptata usata da gruppi criminali per coordinare traffici internazionali. L'operazione mostrò come l'analisi di sistemi distribuiti e cloud possa essere determinante, ma anche quanto sia difficile ottenere accesso ai dati quando non esiste un dispositivo fisico unico da sequestrare.

Infine, un ruolo importante lo ricoprono le aziende. Oggi la digital forensics non è più solo una disciplina per forze dell'ordine o tribunali, ma anche un elemento strategico di sicurezza per le imprese. Incidenti come ransomware, insider threat o data breach richiedono interventi forensi tempestivi, capaci di ricostruire la dinamica dell'accaduto, preservare le prove e supportare attività legali e assicurative. Ciò ha dato vita a nuove figure professionali ibride, in bilico tra la sicurezza informatica e la disciplina forense, in grado di operare in contesti altamente dinamici.

Tuttavia, l'espansione della digital forensics porta con sé un necessario interrogativo: come si colloca tutto ciò rispetto ai diritti fondamentali degli individui?

Capitolo 2 – Privacy e rischi: un nuovo modello di minacce nella Digital Forensics

Con l'aumento delle capacità tecniche e dei software a disposizione dei tecnici forensi, cresce inevitabilmente anche il rischio di violazioni della privacy. La digital forensics, per sua natura, attraversa confini delicati; infatti, in alcuni casi, l'analisi forense può rivelare dati estremamente sensibili, come informazioni mediche, preferenze personali, credenze religiose, orientamenti politici o dettagli intimi che non hanno alcuna rilevanza rispetto all'indagine.

Negli ultimi anni diversi studi accademici hanno iniziato a proporre veri e propri **modelli di minaccia applicati alla privacy nelle attività forensi**, mostrando come il processo investigativo possa esporre rischi non solo tecnici, ma anche legali e sociali. Uno dei problemi più evidenti riguarda l'asimmetria informativa: i tecnici forensi hanno accesso a strumenti sofisticati, spesso non facilmente comprensibili a un giudice o a un cittadino comune, e questa disparità rischia di creare "zone d'ombra" in cui la potenziale intrusività delle tecniche non è percepita né controllata adeguatamente.

Le minacce alla privacy non derivano solo da possibili comportamenti scorretti, ma anche da strutture operative inefficaci. Ad esempio, l'acquisizione completa di uno smartphone può portare alla raccolta di una mole gigantesca di dati, dei quali solo una piccola parte è realmente pertinente all'indagine. Inoltre, la conservazione delle evidenze digitali, necessaria per garantire la catena di custodia, può esporre le informazioni sensibili a rischi di perdita, diffusione non autorizzata o attacchi informatici.

In Europa è ancora vivo il dibattito sulla raccolta massiva dei dati di geolocalizzazione durante la pandemia COVID-19. Diversi Stati proposero di analizzare dati degli smartphone per verificare i movimenti dei cittadini durante i lockdown. Sebbene alcuni di questi progetti non furono portati avanti, la discussione mostrò quanto sia sottile il confine tra tutela della collettività e sorveglianza generalizzata.

Un'altra criticità riguarda i dati dei terzi. Nella maggior parte delle applicazioni forensi, soprattutto in ambito mobile o cloud, l'analisi coinvolge inevitabilmente persone estranee all'indagine: contatti, conversazioni, immagini condivise, metadati. Questo solleva un importante problema di proporzionalità: fino a che punto è corretto acquisire informazioni di individui non direttamente coinvolti in un procedimento giudiziario? E quali meccanismi di tutela devono essere previsti per ridurre al minimo questo impatto?

In questo senso la privacy non è più solamente un vincolo normativo, ma un vero e proprio principio etico e operativo che dovrebbe guidare l'intero processo forense. Le moderne metodologie investigative dovrebbero essere progettate seguendo logiche di "privacy by design", garantendo minimizzazione dei dati, trasparenza dei processi, conservazione sicura e accesso strettamente limitato. Senza un approccio strutturato, il rischio è che la digital forensics diventi una forma di sorveglianza tecnologicamente sofisticata, ma scarsamente controllata.

Capitolo 3 – Nuove tecnologie e il loro impatto sulla Digital Forensics

L'evoluzione tecnologica degli ultimi anni ha introdotto scenari completamente nuovi per la digital forensics, che oggi deve confrontarsi con sistemi sempre più complessi. Tra le tecnologie più rilevanti spiccano l'Internet of Things, il cloud computing, la blockchain con le criptovalute e l'intelligenza artificiale.

L'**Internet of Things** è probabilmente il settore più caotico e difficile da gestire. Gli oggetti connessi presenti nelle abitazioni generano continuamente dati che possono avere importanza probatoria. Tuttavia, la varietà dei sistemi operativi e dei firmware, spesso proprietari e scarsamente documentati, rende estremamente complesso accedere a informazioni affidabili. Inoltre, molti dispositivi IoT inviano i loro dati a cloud remoti o utilizzano protocolli non standard, rendendo l'analisi frammentata e decisamente difficoltosa.

Se possibile, ancora più complessa è la **cloud forensics**, un campo in rapida crescita. L'analisi di dati distribuiti su cloud comporta la necessità di ottenere accesso da parte dei provider, di garantire l'integrità delle informazioni attraverso snapshot e log distribuiti e di confrontarsi con problemi di giurisdizione internazionale. Il cloud, rispetto ai sistemi tradizionali, elimina la possibilità di un controllo completo sul dispositivo fisico: tutto avviene attraverso API, pannelli di amministrazione e richieste formali, con potenziali limitazioni. In molte indagini internazionali contro gruppi ransomware, come quelli del **gruppo Conti**, gli investigatori hanno ottenuto accesso ai log di servizi cloud che gli attaccanti usavano per immagazzinare dati esfiltrati. Senza cooperazione dei provider sarebbe stato impossibile ricostruire parte dei movimenti digitali.

Anche la diffusione delle **criptovalute** ha aperto nuove frontiere investigative. Sebbene le blockchain pubbliche siano trasparenti per natura, l'anonimato degli utenti, la presenza di servizi come la possibilità di utilizzare monete orientate alla privacy rendono la ricostruzione dei flussi finanziari complessa e richiedono strumenti specializzati. Il sequestro di portafogli digitali, inoltre, solleva questioni tecniche e legali ancora non del tutto risolte.

Infine, l'**intelligenza artificiale** rappresenta una delle innovazioni più significative del settore. Da un lato, l'AI permette di gestire enormi quantità di dati, automatizzare attività di analisi, individuare pattern nascosti e accelerare drasticamente i tempi delle indagini. Dall'altro, introduce rischi nuovi: modelli non trasparenti, bias che possono alterare le conclusioni, difficoltà nel certificare i risultati di un algoritmo e, soprattutto, rischi per la privacy. L'AI può essere anche oggetto di indagine, come nel caso dei *deepfake*, delle manipolazioni audiovisive o dei sistemi automatizzati coinvolti in attacchi informatici.

Europol ha pubblicato rapporti in cui spiega come l'analisi automatizzata di grandi dataset sia stata determinante in indagini sul traffico di esseri umani e sulla pornografia minorile, permettendo di identificare immagini duplicate o correlate in database mondiali. Parallelamente, nel 2023 un caso giudiziario negli Stati Uniti ha sollevato dubbi sull'uso di un algoritmo di riconoscimento facciale che aveva erroneamente identificato un sospetto, evidenziando i rischi dell'utilizzo di tali sistemi.

In sintesi, l'innovazione tecnologica offre alla digital forensics opportunità immense, ma allo stesso tempo espone a rischi più elevati e richiede un aggiornamento costante delle metodologie e delle normative.

Capitolo 4 – Sicurezza vs Diritti: il contesto europeo

Nel 2025 il dibattito europeo su sicurezza, privacy e accesso ai dati è stato particolarmente intenso. Le istituzioni europee stanno lavorando a nuove direttive e regolamenti per facilitare l'accesso ai dati in ambito investigativo, soprattutto in risposta a minacce transnazionali e all'aumento dei crimini informatici. L'obiettivo è garantire strumenti più efficaci alle forze dell'ordine, riducendo i tempi e le complessità burocratiche attualmente presenti.

Tuttavia, parallelamente, cresce anche la preoccupazione da parte di associazioni ed esperti che temono un possibile indebolimento della privacy. L'accesso ai metadati, la raccolta di informazioni massive, la cooperazione obbligatoria con i provider e l'utilizzo di tecniche automatizzate di analisi dei dati suscitano molte discussioni, soprattutto perché potrebbero aprire la strada a forme di sorveglianza non proporzionata.

Il GDPR continua a rappresentare la base normativa fondamentale, ma la sua applicazione in ambito forense non è sempre lineare. Concetti come minimizzazione dei dati, limitazione della conservazione e finalità specifica si scontrano talvolta con la necessità di preservare prove digitali intatte per lunghi periodi. Inoltre, nuove normative come il Data Governance Act, il Digital Services Act e la direttiva NIS2 interagiscono con la digital forensics, modificandone indirettamente i confini operativi.

Il tema dei dati dei cittadini è riemerso anche nel caso **“ChatControl”** discusso nel 2023–2024 dal Parlamento Europeo. L'idea di imporre ai provider controlli automatici sui contenuti privati per contrastare abusi minorili ha generato forti opposizioni da parte di esperti di privacy e crittografia, che avvertivano del rischio di sorveglianza generalizzata.

Un elemento particolarmente rilevante nel contesto attuale è la crescente attenzione alla formazione e alla certificazione dei tecnici. Le università e i centri di ricerca stanno investendo nella creazione di corsi specifici dedicati alla relazione tra digital forensics e diritto, con l'obiettivo di creare figure professionali capaci di operare in modo legalmente consapevole. Allo stesso tempo, gli organismi europei stanno promuovendo la standardizzazione degli strumenti forensi e la creazione di procedure uniformi che possano essere applicate in tutti gli stati membri.

Il dibattito politico e normativo si concentra dunque su una domanda centrale: come garantire sicurezza e strumenti efficaci alle autorità senza però compromettere i diritti fondamentali dei cittadini? Una risposta definitiva non è ancora stata trovata, ma è chiaro che il futuro della digital forensics in Europa dipenderà dalla capacità di mantenere questo equilibrio.

Conclusioni

Il tema principale del presente report è il bilanciamento tra efficacia investigativa e tutela dei diritti fondamentali. Senza regole chiare, strumenti trasparenti e tecnici correttamente formati, la digital forensics rischia di oltrepassare il confine tra indagine e sorveglianza. Per questo motivo è fondamentale adottare un approccio che integri tecnologie avanzate con procedure rigorose, garanzie legali, principi etici e un'attenta valutazione della proporzionalità.

Dall'analisi dei casi reali e dei problemi tecnici emergono alcune soluzioni concrete, che possono essere adottate tanto dalle forze dell'ordine quanto dalle organizzazioni pubbliche e private responsabili delle attività forensi:

- favorire sistemi di chiavi multi-parte in cui l'accesso ai dati critici avviene solo tramite la combinazione fra autorità giudiziaria, perito forense e custode dei dati
- utilizzare tecniche di verifica dell'integrità basata su hash e blockchain che permettono di garantire la validità probatoria senza esporre tutti i dati in chiaro;
- ricorrere ad ambienti di analisi isolati ed offline che consentono la lettura dei dati investigativi senza esportazione e/o duplicazione;
- implementare nei dispositivi IoT funzioni native di forensics readiness, come registri firmati o log protetti con chiavi hardware;
- introdurre audit obbligatori e indipendenti dei modelli di analisi forense basati su AI, con verifica periodica dei bias e delle performance.

Un approccio europeo coordinato, coerente con GDPR, NIS2 e le linee guida dell'EDPB, permetterebbe di garantire un equilibrio reale tra sicurezza e libertà, migliorando la qualità delle indagini e la protezione dei dati personali.

Bibliografia

Libri e manuali

- Carrier, B. (2020). File System Forensic Analysis. Addison-Wesley.
- Casey, E. (2021). Digital Evidence and Computer Crime. Academic Press.
- Sammons, J. (2020). The Basics of Digital Forensics. Syngress.

Articoli scientifici e conferenze

- Garfinkel, S. (2010). "Digital Forensics Research: The Next 10 Years". Digital Investigation.
- Yee Ching Tok (2023). "Identifying threats, cybercrime and digital forensic opportunities in Smart City Infrastructure via threat modeling".
- Asou Aminnezhad, Dehghantanha A., Mohd Taufik (2012). "A Survey on Privacy Issues in Digital Forensic"
- Fischinger D. and Boyer M. (2025). "DF2023: The Digital Forensics 2023 Dataset for Image Forgery Detection"
- "Che cos'è il ransomware Conti?" – <https://www.akamai.com/it/glossary/what-is-conti-ransomware>

Normativa e linee guida

- Regolamento UE 2016/679 (GDPR).
- Direttiva (UE) 2022/2555 (NIS2).
- Proposte e documenti della Commissione Europea (2024–2025)
 - Brussels (2025) – "Roadmap for lawful and effective access to data for law enforcement"
- European Data Protection Board (EDPB), linee guida su trattamento dati per fini giudiziari – https://www.edpb.europa.eu/sme-data-protection-guide/process-personal-data-lawfully_it

Report e documenti istituzionali

- ENISA (2024). Digital Forensics for Incident Response in the EU. https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf
- Europol (2025). IOCTA – Internet Organised Crime Threat Assessment. <https://op.europa.eu/en/publication-detail/-/publication/0a06109b-4b28-11f0-85ba-01aa75ed71a1>



tinexta
defence

Next | Donexit | Foramil | Innodesi

Via Giacomo Peroni, 452 – 00131 Roma
tel. 06.45752720 – info@defencetech.it
www.tinextadefence.it

#TinextaDefenceBusiness