WEB FORENSICS

LA PROVA DIGITALE

a cura di

Emanuele Casadio, Tommaso Grotto, Luis Peréz Sanchéz, Matteo Scapin

Estratto dal volume “La prova digitale” edito da Giuffrè Francis Lefebvre

Kopjra

LA *DIGITAL FORENSICS* E LO STANDARD ISO/IEC 27037:2012

di Emanuele Casadio, Tommaso Grotto

Il ciclo di vita dei documenti analogici e digitali

L'approccio aziendale alla gestione dei documenti è diverso a seconda del caso che si tratti, ad esempio, di una stipula avvenuta tramite canale analogico, mediante sottoscrizione di un documento cartaceo, oppure tramite canale digitale, come una pagina web. Nel primo caso, un operatore dell'azienda si dovrebbe preoccupare di far sottoscrivere all'utente un contratto cartaceo e potrebbe anche richiedere a quest'ultimo di identificarsi mostrando un proprio documento di identità rilasciato da un'autorità pubblica.

Si pensi alle caratteristiche di questo approccio:

- è possibile garantire l'identità del soggetto che ha sottoscritto il contratto tramite riconoscimento con documento di identità (**autenticità**);
- è possibile garantire che il contenuto non sia stato alterato durante il processo o in un momento successivo all'apposizione della sua firma (**integrità**);
- è possibile garantire che lo stesso soggetto non possa successivamente negare di aver compiuto tale sottoscrizione (**non ripudio**).

Queste caratteristiche sono garantite dall'apposizione della firma autografa sul documento cartaceo.

Gli approcci comunemente utilizzati in ambito digitale non seguono i principi precauzionali per i quali invece si è abituati nel mondo analogico. Si pensi ad esempio all'iscrizione a un concorso a premi su un sito web aziendale dedicato. In questo caso l'utente procede di sua iniziativa alla compilazione di un modulo *online* (*form*) immettendo liberamente i propri dati personali, presta i consensi che preferisce riguardo le diverse finalità di trattamento, può visualizzare l'informativa e gli eventuali termini di servizio, infine invia il *form* premendo l'apposito pulsante. In questo caso viene totalmente a mancare l'identificazione dell'utente dato che chiunque abbia compilato il *form* potrebbe aver impersonato qualcun altro, di conseguenza, non essendo certa l'identità del sottoscrittore, anche il concetto di non ripudio viene totalmente a mancare. Inoltre, l'integrità dei dati forniti è interamente in carico all'azienda: nel caso del documento cartaceo, è sempre possibile procedere con una perizia calligrafica per determinarne un'eventuale manomissione da parte dell'azienda stessa. Viceversa, nel caso del dato fornito *online*, non esistono metodologie di verifica oggettive che possano stabilire con sufficiente precisione se tale dato non sia stato alterato unilateralmente dall'azienda che lo aveva in gestione. Questo è possibile perché **il dato spesso non è altro che un *record* di una base di dati, eventualmente supportato da una riga di un *file* di *log*. In sostanza, ciò che spesso manca è proprio una firma elettronica**. Ovviamente la firma elettronica non è quasi mai un requisito, tuttavia, in caso di contenzioso potrebbe risultare complicato, se non impossibile, dimostrare che una specifica azienda non abbia, ad esempio, manomesso deliberatamente le finalità di trattamento pre-

state dai suoi utenti, indicando come accettate delle finalità commerciali assolutamente opzionali quando queste erano state invece rifiutate dai suoi utenti.

Dal documento analogico a quello digitale: le caratteristiche da tenere a mente

- **Autenticità**: la garanzia che il soggetto che ha prodotto i dati sia proprio lui
- **Integrità**: il fatto che i dati non siano stati alterati a posteriori da un soggetto terzo
- **Non ripudio**: l'impossibilità da parte del soggetto che ha prodotto i dati di negare tale azione

Il valore probatorio delle firme elettroniche semplici, avanzate e qualificate

Prendiamo ad esempio uno dei casi maggiormente disciplinati. Le banche dispongono di processi ben codificati e tipicamente ne gestiscono la dematerializzazione con accortezza. Qualora sia necessaria la firma di un contratto, si provvede preventivamente all'identificazione dell'utente con documento di identità che può avvenire direttamente in filiale, oppure da remoto tramite *webcam*. Nel caso in cui occorra firmare digitalmente un documento in filiale, si procede tramite firma grafometrica che ha valore di firma elettronica avanzata, l'efficacia probatoria della scrittura privata e valore probatorio limitato al contesto specifico d'uso, grazie all'inclusione di informazioni legate al tratto grafico quali accelerazione e pressione dell'utente che l'ha apposta e che possono essere usate per un'eventuale perizia. Alcune banche addirittura permettono ai loro clienti l'uso di strumenti di firma remota: dopo essersi identificati e autenticati, per alcune operazioni particolarmente critiche come la firma di contratti corrispondenti a nuovi prodotti bancari, viene generato un documento PDF contenente il contratto che si sta per firmare, contestualmente viene inviato un codice OTP (*one-time password*) via SMS al numero di telefono precedentemente autorizzato dal cliente e viene richiesto a quest'ultimo di immettere il codice OTP appena ricevuto. Tale metodologia (identificazione effettuata in precedenza, autenticazione tramite coppia di credenziali utente e codice OTP su numero di telefono autorizzato) è considerata sufficiente per il rilascio e l'uso di un certificato di firma (almeno avanzata) usa e getta, pertanto anche per l'uso di una firma remota, che ha lo stesso valore probatorio di una firma autografa, rispetto ai rapporti intercorsi tra sottoscrittore ed emittente della soluzione di firma. A livello europeo, il regolamento di riferimento per le firme elettroniche o più in generale i *trust services* è eIDAS (*electronic IDentification Authentication and Signature*). In Italia, invece, devono essere presi in esame il CAD (Codice dell'Amministrazione Digitale, ora armonizzato con eIDAS) e le linee guide dell'AgID (Agenzia per l'Italia Digitale), la quale pubblica e aggiorna la lista dei TSP (*Trust Service Provider*) italiani.

Esistono però operazioni per le quali non viene utilizzata una firma elettronica avanzata o qualificata, come ad esempio un bonifico impartito dal servizio di *online banking*. In questo caso, oltre alle consuete credenziali, viene richiesto all'utente di confermare l'operazione tramite inserimento di un codice di conferma usa e getta che solamente lui può conoscere, fornito da un dispositivo di autenticazione a due fattori in suo possesso. Questo meccanismo può essere riconducibile a una

sorta di firma elettronica semplice, la cui efficacia probatoria è liberamente interpretabile dal giudice. Ciò è ragionevole anche in merito al meccanismo di funzionamento tecnico della maggior parte dei dispositivi commerciali di autenticazione a due fattori. Ogni dispositivo è identificato univocamente da un codice seriale. All'interno del dispositivo vi è un sistema di cifratura simmetrica e un piccolo orologio in grado di generare un tempo codificato come numero binario utilizzato come messaggio in chiaro dal sistema di cifratura. Immutabile all'interno della sua memoria interna, ogni dispositivo contiene un altro numero definito seme (*seed)* che caratterizza il dispositivo rispetto a tutti gli altri e che viene utilizzato come chiave di cifratura. Il sistema, infine, riduce il messaggio cifrato tramite apposito algoritmo di *hashing* a un singolo messaggio di tipicamente 8 cifre e cioè il codice di conferma usa e getta di cui sopra. La banca, per verificare che il codice sia corretto e che quindi l'utente sia chi sostiene di essere, recupera dalla propria base di dati l'informazione corrispondente al dispositivo associato, ottiene il suo *seed*, calcola il tempo corrente, genera quindi il messaggio cifrato, lo riduce a 8 cifre e infine verifica che queste corrispondano.

Un sistema di questo tipo è sicuro finché l'interlocutore, in questo caso la banca, rimane parte fidata. Nel caso in cui l'interlocutore non potesse essere ritenuto parte fidata, le considerazioni da fare sono differenti. La tecnologia, pur proteggendo da attacchi *replay* consistenti nel tentativo non autorizzato di riutilizzare lo stesso codice per più operazioni, non protegge adeguatamente da attacchi di ingegneria sociale nonché *man-in-the-middle*, questi ultimi consistenti nell'intercettazione dei codici a opera di soggetti terzi e conseguente utilizzo improprio, seppur tale eventualità sia drasticamente mitigabile tramite l'adozione di TLS/SSL. Inoltre, diversamente da tecnologie basate sulla crittografia asimmetrica, a livello puramente teorico un dipendente malintenzionato dell'istituto di credito oppure un attaccante che è riuscito a prendere controllo del sistema informativo aziendale della banca, conoscendo potenzialmente il *seed* del dispositivo di autenticazione a due fattori, potrebbe inserire nel sistema informativo delle disposizioni perfettamente arbitrarie. Si consideri ad esempio il fenomeno avvenuto negli Stati Uniti negli anni '80 noto come *salami slicing*, per cui alcuni impiegati maligni di un istituto di credito hanno inserito arbitrariamente delle disposizioni di prelievo di pochi centesimi di dollaro su molteplici conti correnti intestati a soggetti differenti, incassando personalmente le somme complessive per diversi milioni di dollari. Questi sono casi difficili da riscontrare nella realtà, però si consideri che l'utilizzo di una firma digitale, implementazione specifica di una firma elettronica qualificata tramite uso di una coppia di chiavi (pubblica e privata), apposta su un documento tramite l'utilizzo di una *smart card* è immune ai problemi appena evidenziati. Dando per scontato l'utilizzo di algoritmi di *hash* sufficientemente resistenti alle collisioni e chiavi sufficientemente lunghe, l'unico attacco possibile alla firma digitale consiste nella sottrazione della chiave privata, fatto comunque mitigabile a posteriori tramite iscrizione del certificato di firma all'interno delle liste pubbliche di revoca da parte dell'autorità che lo ha emesso. In questo caso l'unica assunzione forte è che l'autorità di certificazione sia una parte fidata da entrambe le parti e idealmente inattaccabile. Tuttavia, esistono casi di autorità di certificazione non iscritte ad AgID (e quindi che non sono mai state in grado di emettere certificati di firma qualificati) che hanno falsificato la data di emissione di più certificati a interesse di una parte, rompendo quindi il legame di fiducia incondizionato che godeva tra tutte.

Con ciò non si intende asserire che sia necessario per ogni operazione generare un documento informatico riepilogativo su cui apporre una firma digitale, ma che è importante tenere sempre a mente i pregi e i difetti di ogni strumento di firma in relazione alla criticità del documento da sottoscrivere e al fatto che il costo di tale strumento in termini economici, di peggioramento dell'esperienza utente

e appesantimento dei processi, sia proporzionato.
È complesso individuare tecnologie che permettano di associare in modo inequivocabile l'identità di un firmatario a un documento in assenza di qualsiasi vincolo di fiducia. Alcune tecniche basate su *blockchain* permettono di registrare un contenuto arbitrario all'interno di un blocco. Questo permette di ottenere le stesse caratteristiche di una marca temporale, strumento utilizzato di norma per apporre una data certa su un documento anche in totale mancanza di fiducia verso qualunque ente, però con costi e imprecisioni temporali maggiori.
Le soluzioni tecniche sono variegate e ognuna si distingue da un'altra per caratteristiche, pregi, difetti e ambiti di applicazione. **È difficile individuare una tecnologia *passe-partout* che possa essere utilizzata indistintamente in ogni contesto applicativo.** Occorre quindi effettuare una minuziosa ricerca sia tecnica sia legale per individuare la tecnologia più idonea al caso specifico, senza dimenticare che non esiste una tecnologia totalmente inattaccabile**.**
Riassumendo, **la firma elettronica qualificata ha lo stesso valore probatorio di una firma autografa. Medesimo discorso per quella avanzata ma limitatamente ai rapporti tra sottoscrittore ed emittente della soluzione di firma. Quella semplice, invece, è liberamente interpretabile dal giudice.** Se rimaniamo ancorati alla sottoscrizione di documenti, analogici o digitali che siano, possiamo asserire che la firma più idonea è quella che rispetta i requisiti normativi, in casi particolarmente regolamentati come quello bancario, o le politiche interne dell'azienda, prestando sempre attenzione a bilanciare la complessità e il costo della procedura di firma rispetto al rischio di contenzioso e, di conseguenza, all'importanza di disporre di un documento con valore probatorio più o meno forte. **Se, invece, proviamo a riflettere sulle possibili modalità di firma di un illecito commesso su una pagina web, come ad esempio un caso di diffamazione, ci rendiamo conto che ad oggi non esistono firme elettroniche semplici, avanzate o qualificate per sopperire a tale esigenza. Una soluzione potenziale, però, può essere individuata interpretando in modo originale lo standard internazionale di informatica forense ISO/IEC 27037:2012.**

Princìpi di *digital forensics* secondo lo standard ISO/IEC 27037:2012

Il già citato standard ISO/IEC 27037:2012 è il capostipite di una famiglia di standard tecnici relativi alla sicurezza informatica, e il suo obiettivo è quello di definire le linee guida per l'identificazione, la raccolta, l'acquisizione e la conservazione delle prove digitali. Tale standard nasce per l'utilizzo in ambito penale e mostra quindi come ottenere elementi digitali aventi valore di prova, al fine di poterli produrre in giudizio. È evidente che per poter essere applicabile nei più svariati paesi e contesti operativi, manca di qualsiasi tipo di riferimento legislativo, giurisprudenziale o a specifici software o hardware commerciali.

***Framework* ISO/IEC nel complesso: dallo standard 27035 al 30121**

- ISO/IEC 27035-1:2016: *Principles of incident management*
- ISO/IEC 27035-2:2016: *Guidelines to plan and prepare for incident response*
- ISO/IEC 27035-3: *Guidelines for incident response operations* (cancellato)
- **ISO/IEC 27037:2012: *Guidelines for identification, collection, acquisition and preservation of digital evidence***
- ISO/IEC 27038:2014: *Specification for digital redaction*

- ISO/IEC 27040:2015: *Storage security*
- ISO/IEC 27041:2015: *Guidance on assuring suitability and adequacy of incident investigative method*
- ISO/IEC 27042:2015: *Guidelines for the analysis and interpretation of digital evidence*
- ISO/IEC 27043:2015: *Incident investigation principles and processes*
- ISO/IEC 27044: *Guidelines for security information and event management* (non ancora pubblicato)
- ISO/IEC 27050-1:2016: *Electronic discovery*
- ISO/IEC 30121:2015: *Governance of digital forensics risk framework*

Lo standard riconosce quattro procedure principali: **l'identificazione, la raccolta, l'acquisizione e la conservazione**, tutte quante eseguite da professionisti forensi.

Per **identificazione** si intende il processo che comporta la ricerca, il riconoscimento e la documentazione di potenziali prove digitali. Nel caso più semplice può quindi includere la fase di ricerca di un dispositivo fisico come uno *smartphone* o un disco rigido che verosimilmente potrebbe contenere dati di interesse, ma per estensione può includere anche l'identificazione di un disco virtuale esistente su una *Storage Area Network* oppure la ricerca di un *bucket* su *storage* distribuito a oggetti nell'ambito di un'infrastruttura di *cloud computing*. La ***digital forensics*** copre quindi tutti i dispositivi possibili e immaginabili, qualificandosi ogni volta in maniera più specifica in base al tipo di dispositivo identificato e arrivando anche a coprire dati volatili come possono essere quelli in transito su reti. Ad esempio, si parla di ***computer forensics*** quando i dati sono salvati su un PC o un *server*, di ***mobile forensics*** quando i dispositivi oggetto di analisi sono *smartphone* e, talvolta, *tablet*, e infine ***network forensics*** quando i dati sono volatili in transito su reti. Si parla di ***cloud forensics***, invece, quando i dati sono in transito su infrastrutture *cloud*. La fase di identificazione è forse una delle più delicate, dato che non esiste una procedura standardizzata ma richiede sforzi anche di natura investigativa da parte del personale inquirente.

Per **raccolta** si intende il processo che comporta il prelievo del dispositivo fisico contenente i dati e il conseguente trasporto presso il proprio laboratorio attrezzato. La differenza sostanziale da tenere a mente è tra dispositivo spento o acceso; a seconda dell'uno o dell'altro stato, infatti, mutano le attività da effettuare. In generale, la raccolta di un dispositivo acceso si presta alle problematiche che, per il trasporto deve essere necessariamente scollegato, e ciò potrebbe comportare la perdita dei dati in memoria volatile (RAM): in tale caso può convenire acquisire i dati volatili prima di procedere con la raccolta, attività che prende il nome di ***memory forensics***. Si noti che individuare la locazione fisica dei dati presenti su architetture distribuite su scala molto grande è un problema tutt'altro che banale. Per i dati presenti su infrastrutture *cloud* pubbliche o ibride, e quindi di proprietà e in gestione a terze parti, ciò è impraticabile. In poche parole, con l'avvento delle infrastrutture *cloud* e similari il processo di raccolta si è reso molto complicato se non impossibile da portare a termine.

L'**acquisizione** serve proprio per intervenire in questi casi, ovvero quando la raccolta è impercorribile perché decisamente sproporzionata rispetto alle necessità. **Essa consiste nella creazione di una copia esatta (immagine) dei dati che contengono un elemento di interesse significativo per l'indagine e il suo prodotto viene infatti definito potenziale prova digitale.** Come già citato in precedenza, inoltre, l'acquisizione è fondamen-

tale qualora si rendesse necessario dare evidenza di dati volatili come ad esempio quelli presenti su RAM oppure in transito su reti.
Infine, per **conservazione** si intende il processo perpetuato nel tempo che permette di dimostrare come la potenziale prova digitale sia rimasta integra e immutata dal momento in cui è stata creata a quello in cui è stata prodotta in giudizio. Nel caso dell'acquisizione, il supporto è indifferente, purché si riesca a garantire l'immutabilità dei dati in esso contenuti; discorso differente per la raccolta, visto che andrebbero sempre conservati anche i supporti originali, oltre alle eventuali copie di lavoro.
Appare quindi evidente come identificazione e conservazione siano sempre imprescindibili mentre raccolta e acquisizione possano essere considerate come alternative o complementari tra loro.

Le procedure principali dello standard ISO/IEC 27037:2012

- **Identificazione**: per individuare e documentare i dati di interesse
- **Raccolta**: per ottenere il dispositivo fisico contenente tali dati
- **Acquisizione**: nel caso la raccolta fosse impercorribile, per creare una copia esatta dei dati, chiamata anche **potenziale prova digitale**
- **Conservazione**: per dimostrare che la potenziale prova digitale è rimasta integra dalla creazione alla produzione in giudizio

Ad eccezione di alcune situazioni basilari, lo standard non definisce minuziosamente i singoli procedimenti da adottare in relazione alle specifiche casistiche sulle quali ci si può imbattere; **definisce invece le caratteristiche desiderate dei processi e dei loro sottoprodotti, ovvero la giustificabilità, la verificabilità, la ripetibilità e la riproducibilità.** Un principio cardine è quello della **giustificabilità** dei processi, sia dal punto di vista tecnico sia in relazione al rapporto costi e benefici, fermo restando la **sufficienza** delle potenziali prove digitali acquisite, come si vedrà in seguito. Ad esempio, lo standard prevede che non sia necessario acquisire un intero disco rigido per provare la presenza di un particolare *file*. Se la partizione su cui tale *file* risiede è più piccola rispetto all'intero disco, si potrebbe valutare di acquisire solamente la partizione o addirittura il singolo *file*. In alternativa, **se il *file* incriminato dovesse risiedere in uno spazio di archiviazione remoto, si potrebbe scaricare il *file*, coadiuvando il tutto con ulteriori elementi a garanzia della verificabilità del processo e quindi rendendo decisamente improbabile che la potenziale prova digitale sia stata costruita o manipolata ad arte. La metodologia che si può applicare al contesto appena descritto prevede l'acquisizione dell'intero traffico di rete e di ulteriore traffico generato appositamente per dimostrare che gli instradamenti e i meccanismi di risoluzione dei nomi non siano stati alterati, costruendo quindi una sorta di pacchetto dell'acquisizione che assume valore di potenziale prova digitale.** Per quanto concerne la **verificabilità**, idealmente la potenziale prova digitale dovrebbe includere una metodologia di verifica oggettiva che permetta di compararla con l'originale, come ad esempio una impronta crittografica. Sempre a tale scopo, è opportuno che la metodologia adottata garantisca la **ripetibilità** o la **riproducibilità**. Questi termini in apparenza simili esprimono concetti distinti: il primo si riferi-

sce alla possibilità di ripetere la procedura nelle medesime condizioni previste per l'acquisizione e ottenere gli stessi risultati, partendo dall'originale; il secondo, invece, si riferisce alla possibilità di operare in condizioni differenti, ad esempio utilizzando strumenti diversi.

I principi fondamentali che regolano una prova digitale sono la **rilevanza, l'affidabilità e la sufficienza**. Si noti che alcune caratteristiche e proprietà sono strettamente correlate tra loro, ad esempio una prova non affidabile sarà difficilmente verificabile, così come una prova non sufficiente sarà difficilmente giustificabile. Per **rilevanza** si intende semplicemente che quanto acquisito debba essere significativo per dimostrare la propria tesi investigativa, come ad esempio l'illecito subito. Per **affidabilità** si intende che la prova debba effettivamente possedere le caratteristiche dichiarate e richieste dal dibattito processuale. Infine, per **sufficienza** si intende che non è necessario acquisire integralmente tutto il materiale a disposizione (si pensi ad esempio a filmati che pesano molteplici GB): è, appunto, sufficiente acquisire il materiale necessario per provare in modo incontrovertibile il proprio punto, compatibilmente con i vincoli di costi e tempo.

Per quanto concerne l'affidabilità, è opportuno fare qualche ulteriore precisazione su quali strategie sia possibile mettere in campo per ottenerla. Chiaramente il metodo più immediato è quello di avere processi che siano il più possibile rigidi, documentati e perciò revisionabili. Inoltre, quantomeno sarebbe necessario dare prova che gli elementi non siano variati dopo l'acquisizione o la raccolta e cioè che l'integrità sia rimasta tale e che sia stata mantenuta la catena di custodia. Per addivenire a ciò, una tecnica comune è – specialmente su elementi di potenziale prova digitale molto grandi – quella di creare un archivio autocontenuto che includa tutti i *file* ottenuti, e adottare metodologie e tecniche per garantirne il contenuto nel tempo. Ad esempio, al termine della procedura di acquisizione o raccolta, è possibile definire uno speciale *file* che contiene i percorsi relativi di tutti i *file* inseriti nell'archivio, assieme alla loro **impronta crittografica**. L'impronta caratterizza in maniera specifica una particolare sequenza di *byte* e ne determina la sua "impronta digitale"; si ottiene attraverso una funzione crittografica di ***hash*** (ad esempio SHA-512/256), ovvero una funzione non invertibile che associa una sequenza di dati di lunghezza arbitraria a una sequenza di dati di lunghezza fissa. Una volta definita l'impronta dei *file* inseriti nell'archivio, è possibile applicare una marca temporale e, opzionalmente, un sigillo elettronico o una firma elettronica a tale speciale *file*, infine aggiungere anche questo *file* all'archivio e per ultimo persisterlo in modo che non subisca alterazioni.

Attraverso la tecnica definita qui sopra è possibile infatti dimostrare che un archivio effettivamente integro non abbia subito alterazioni. Per farlo, è sufficiente decomprimere l'archivio, verificare con un opportuno software la validità della marca temporale e, opzionalmente, del sigillo elettronico o della firma elettronica applicate allo speciale *file*; se tale *file* è integro, è sufficiente ricalcolare tutte le impronte dei *file* presenti nell'archivio decompresso e verificarle con le impronte riportate nel *file* speciale. Se tutti i valori coincidono, allora l'archivio, e quindi la potenziale prova digitale, è **integra**.

Come già detto, la funzione di *hash* permette quindi di associare anche *file* enormi a stringhe prefissate di indicativamente qualche centinaio di *byte*. Ciò che può, in linea del tutto teorica, accadere è quindi che due *file* diversi generino la stessa impronta, fenomeno definito "collisione". Questo permetterebbe ad esempio di effettuare una modifica mirata ad un *file*, mantenendo però la stessa impronta e quindi rendendo invisibile l'alterazione. Le funzioni di *hash* vengono caratterizzate anche in base alla propria robustezza a questi e altre tipologie di attacchi (come ad esempio l'attacco lunghezza-estensione). Si noti che la già citata funzione di *hash* SHA-512/256 è ritenuta computazionalmente sicura. Ciò significa che con la tecnologia attualmente nota non è possibile effettuare attacchi in tempi ragionevoli.

Come fare, però, a garantire che l'archivio non subisca modifiche accidentali? Gli accorgimenti possibili sono molteplici: lo scrivente ne suggerisce uno commerciale. Attraverso il servizio gestito *Simple Storage Service Glacier* (S3 Glacier) di Amazon Web Services è possibile definire degli speciali spazi (*bucket*) in cui persistere oggetti. Per tali spazi è possibile definire caratteristiche quali il meccanismo di crittografia, per impedire consultazioni non autorizzate, politiche di blocco e di versionamento. Una volta impostate le politiche di blocco per un *bucket*, queste non sono modificabili nemmeno dall'amministratore di sistema. Un esempio di politica di blocco è: «una volta salvato un *file* e una volta trascorse 48 ore, impediscine la modifica o la cancellazione per 10 anni». È anche possibile definire semplicemente una politica di versionamento per cui ogni qual volta viene sovrascritto un oggetto, in verità viene mantenuta per sempre anche la versione precedente, e lo stesso per la cancellazione. Dal punto di vista "fisico", il fornitore garantisce ridondanza e replicazione multipla dei dati. Ad ogni modo, il suggerimento è sempre quello di effettuare copie multiple utilizzando fornitori, sistemi e locazioni distinte quando si sta operando con dati critici, dato che una previsione contrattuale molto forte potrebbe comunque essere disattesa.

Come è stato descritto in precedenza, **l'acquisizione crea un'immagine** o comunque una copia **dell'originale.** Qualora avessimo necessità di ottenere effettivamente **l'originale, l'unica procedura** delle quattro descritte **che permetterebbe di disporre dell'originale sarebbe la raccolta, impraticabile** praticamente sempre se si considerano gli illeciti avvenuti *online*. A tal proposito occorre quindi precisare come **il processo di acquisizione non sia quindi ripetibile o riproducibile**, motivo per cui la documentazione tecnica a corredo della copia di potenziale prova digitale assume un valore ancora più importante, dato che occorre dare evidenza che l'attività svolta sia stata effettuata in maniera precisa, adottando tutte le precauzioni affinché i dati acquisiti non siano inavvertitamente mutati durante la procedura e che la conservazione sia avvenuta in maniera corretta. Questo è un aspetto di cui tenere conto specialmente in ambito penale, dato che le giurisdizioni tendono a definire minuziosamente come debba avvenire acquisizione o raccolta di un elemento di prova, specialmente se irripetibile; ad esempio, in Italia stando al c.p.p., eventuali prove irripetibili devono essere acquisite in contraddittorio. Ad ogni modo, il processo di estrazione dei singoli elementi informativi aventi valore di prova dall'intero pacchetto dell'acquisizione deve essere quantomeno riproducibile.

WEB FORENSICS

di Luis Pérez Sánchez, Matteo Scapin

Introduzione alla *network forensics*

L'acquisizione forense di pagine web è una metodologia utilizzata tipicamente da specialisti di informatica forense per "congelare" lo stato di una pagina web in modo da poter dimostrare in un tempo successivo, incluso in giudizio durante un contenzioso, che lo stato della pagina web fosse effettivamente quello registrato in quel dato istante. La differenza principale rispetto ad altre metodologie più native e tradizionali come il semplice *screenshot* della pagina web è il notevolmente maggiore valore probatorio.

I casi in cui questa attività può rendersi necessaria sono molteplici, si pensi ad esempio ad un qualsiasi tipo di danno subito su Internet, ovvero violazioni dei diritti di proprietà intellettuale e industriale ma anche casi di cyberbullismo, *sexting*, *revenge porn*, *stalking*, diffamazione, *hate speech*, infedeltà coniugale, ecc. Nel caso di reato, il tempo trascorso tra la denuncia alle autorità competenti e il momento in cui gli inquirenti arrivino effettivamente ad acquisire anch'essi la potenziale prova potrebbe essere sufficiente per permettere a chi ha commesso il reato di cancellare le proprie tracce, mentre nel caso di illecito civile è onere di parte attrice raccogliere elementi sufficienti a supportare la sua posizione sia in una eventuale causa ma anche in via stragiudiziale. In ogni caso, è necessario adottare una metodologia sufficientemente robusta che permetta appunto di "congelare" lo stato di una pagina web in modo tale da poterla produrre in un tempo successivo.

Immaginiamo un contesto in cui un soggetto ritenga che un suo diritto sia stato leso su Internet e pertanto abbia provveduto in autonomia a collezionare ciò che egli ritiene essere evidenze dell'illecito: come potrebbe sostenere davanti a un collegio peritale che è stato rispettato il requisito della verificabilità di quanto prodotto? Il potenziale elemento di prova, così come qualsiasi documento informatico, dovrebbe garantire alcune caratteristiche specifiche, già evidenziate nel precedente capitolo, qualora lo si intenda produrre in giudizio. Si osservi che, quantomeno in ambito penale, la prova è inizialmente sempre *potenziale*, dato il principio di contraddittorio nella formazione della stessa.

Lo standard internazionale ISO/IEC 27037:2012 descrive, senza scendere nei dettagli implementativi, come debbano essere svolte le attività di informatica forense, incluse quelle che riguardano risorse presenti su Internet e quindi trasmesse tramite una rete; l'acquisizione di pagine web è quindi un sottoinsieme della procedura di acquisizione descritta da tale standard e prende il nome di *network forensics*, o *cloud forensics* nel caso in cui ci riferissimo ad acquisizioni su infrastrutture di *cloud computing*.

Web Forensics

Web Forensics è un SaaS (*Software as a Service*) che permette di ottenere prove forensi di contenuti disponibili online.

Web Forensics mette a disposizione degli avvocati un software che permette di effettuare una navigazione sicura e forense dei contenuti da certificare, e come risultato pro-

duce un pacchetto probatorio autoconsistente, definito **pacchetto di evidenza forense**, contenente la prova forense del fatto che i contenuti visualizzati durante la navigazione fossero disponibili online a una certa data e ora, garantendo anche la provenienza di tali contenuti, la loro integrità e inalterabilità a posteriori.
Ad esempio, un utente vuole produrre in giudizio una prova del fatto che è stato diffamato online ma allo stesso tempo vuole rimuovere tempestivamente tale contenuto diffamatorio per limitare quanto più possibile il danno.
Per assolvere a questa necessità, e quindi poter richiedere tempestivamente la rimozione della diffamazione, è possibile creare un pacchetto di evidenza forense con funzione di prova legalmente valida in tribunale, in Italia e all'estero, della presenza online del contenuto in violazione in un determinato istante. Con l'ausilio di Web Forensics qualsiasi avvocato può creare autonomamente prove forensi di contenuti disponibili online.

Lessico dell'interfaccia

Utilizzando Web Forensics l'utente cre- erà quella che viene definita **sessione di acquisizione** (o più semplicemente **sessione**), ovvero la componente centrale attraverso cui l'utente potrà effettuare l'acquisizione forense e infine ottenere il pacchetto di evidenza forense e la relativa **relazione metodologica**.

LA RELAZIONE METODOLOGICA

La relazione metodologica è un particolare documento firmato digitalmente che contiene tutte le informazioni relative al procedimento messo in atto per acquisire la prova forense. Tale documento risponde ai criteri di revisionabilità dei processi richiesti dallo standard ISO/IEC 27037:2012 ed è producibile in giudizio assieme al pacchetto di evidenza forense

Con la creazione di una sessione Web Forensics metterà a disposizione dell'utente un **ambiente** sicuro e forense per effettuare la navigazione necessaria per confezionare la prova forense. Questo ambiente, chiamato anche **ambiente di acquisizione**, è composto da un browser, dalle console di log e da un sistema interno che confeziona la prova forense e infine la salva in una locazione *cloud* sicura.
Per confezionare una prova forense è fondamentale "cristallizzare" la navigazione. Il risultato di questa attività è definito appunto pacchetto di evidenza forense, ed è composto dai seguenti elementi:

- **PCAP**: *file* tecnico che contiene tutto il traffico di rete della navigazione avvenuta durante la sessione;
- **SSL_KEYS**: *file* tecnico che contiene tutte le chiavi SSL/TLS (*Secure Sockets Layer*/*Transport Layer Security*) scambiate durante la sessione. Necessario per decifrare il PCAP;
- **VIDEO**: *file* video della registrazione della sessione;
- **SCREENSHOTS**: insieme di *file* immagine che sono stati eventualmente creati dall'utente durante la sessione, con l'ausilio dell'apposito pulsante;

- **DOWNLOADS**: insieme di *file* che sono stati eventualmente scaricati dall'utente durante la sessione;
- **LOGS**: insieme di *file* di log generati automaticamente durante la sessione;
- **XML**: *file* XML che contiene l'impronta digitale di tutti i *file* precedenti. **A questo *file* sono apposti una marca temporale e una firma digitale, per garantire data certa, integrità e inalterabilità della prova.**

IL FILE PCAP	Un file PCAP (o PCAP-NG) è un particolare formato di file binario contenente la copia-immagine del traffico di rete trasmesso su un canale (fisico o virtuale, cablato o *wireless*). Può comprendere tutto il traffico generato a partire dal livello 2 della pila ISO/OSI e TCP/IP, quindi dal livello della trama in poi (Ethernet cioè IEEE 802.3, oppure Wi-Fi cioè IEEE 802.11). Il nome deriva dalla libreria che lo genera, ovvero *libpcap* nei sistemi *Unix-like*
L'IMPORTANZA DELLE CHIAVI SSL/TLS	SSL e TSL sono protocolli di rete utilizzati per garantire la confidenzialità del traffico scambiato tra due parti su una rete di *computer* (*end-to-end*). Storicamente il primo a vedere la luce è SSL (*Secure Sockets Layer*), ora considerato insicuro e non più utilizzato. Di TLS (*Transport Layer Security*) vengono considerate sicure le versioni dalla 1.2 in poi. Questi protocolli non corrispondono a un livello specifico della pila ISO/OSI o TCP/IP, dato che operano al di sopra del livello di trasporto ma prima del livello di sessione (ISO/OSI) o applicativo (TCP/IP). Dato che tali protocolli garantiscono la confidenzialità del traffico, una semplice copia di quest'ultimo sarebbe inutilizzabile in giudizio, dal momento che tutto il traffico risulterebbe crittografato e quindi incomprensibile. A tal proposito è necessario adottare opportuni accorgimenti affinché il traffico possa essere decifrato: una tecnica comune è quella di includere assieme al cosiddetto *dump PCAP*, citato precedentemente, anche i *pre-master secret*, ovvero, semplificando, le chiavi di cifratura
PERCHÉ PREDILIGERE LE ACQUISIZIONI SU HTTPS	In generale è preferibile acquisire traffico su HTTPS invece che HTTP, dato che ciò impedisce tecnicamente la possibilità che un soggetto intermedio possa aver alterato il traffico scambiato tra *browser* e *server*. Inoltre, la presenza di un certificato emesso da un'autorità di certificazione fornisce una sorta di garanzia tecnica (ma non legale) sull'identità del soggetto con

	cui si sta dialogando. Tipicamente, infatti, le autorità di certificazione verificano che un determinato soggetto abbia effettiva disponibilità di un nome di dominio prima di emettere il relativo certificato
I VANTAGGI DELL'ALGORITMO SHA-512/256	Web Forensics utilizza SHA-512/256 come algoritmo per il calcolo dell'impronta digitale dei file afferenti al pacchetto di evidenza forense, dato che tale algoritmo è considerato sicuro e non esistono attacchi noti, a differenza di MD5 o SHA-1

Assieme al pacchetto di evidenza forense è disponibile la relazione metodologica, ovvero un *file* di testo in formato PDF contenente la descrizione della metodologia utilizzata per effettuare l'acquisizione forense, informazioni relative ai *file* presenti all'interno del pacchetto di evidenza forense, l'elenco di URL visitati durante la navigazione e, infine, ulteriori dettagli tecnici sull'ambiente messo a disposizione per l'esecuzione della sessione. **La relazione metodologica è firmata digitalmente.**

Web Forensics introduce anche il concetto di **credito**. Durante la sessione vengono consumati dei crediti, intesi come unità di tempo e risorse, che possono essere rigenerati tramite il pulsante "**Aggiungi crediti**". Una sessione come minimo consuma un credito, e come massimo la quantità di crediti disponibili.

Tour dell'interfaccia

Di seguito verrà illustrata l'interfaccia di Web Forensics con l'ausilio di *screenshot* di esempio e descrizioni, evidenziando le scelte di design effettuate per offrire un'esperienza utente semplice e immediata.

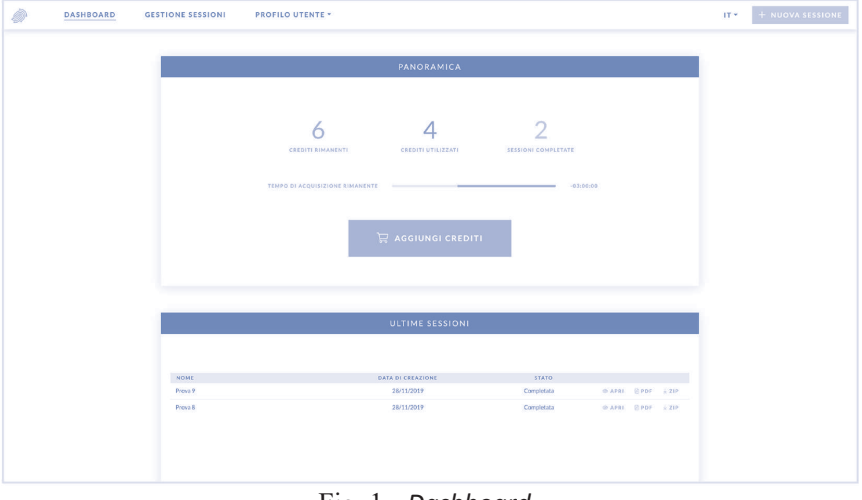

Fig. 1 - *Dashboard*

Dopo essersi autenticato, l'utente atterra sulla *dashboard* di Web Forensics (fig. 1), un cruscotto che offre, *in primis*, una panoramica delle sessioni effettuate e la possibilità di iniziarne una nuova.
L'interfaccia si presenta composta dai seguenti elementi:

1. **Barra di navigazione**, permette di spostarsi tra le diverse sezioni di Web Forensics, nello specifico:

a. ***Dashboard***: pagina corrente, permette di visualizzare la *dashboard*.
b. **Gestione sessioni**: pagina di gestione e anteprima delle sessioni effettuate (paragrafo 1.2.3).
c. **Profilo utente**: menù per la gestione del profilo dell'utente, dei dati di autenticazione e fatturazione.
d. **Lingua**: permette di scegliere la lingua dell'interfaccia e, di conseguenza, delle sessioni.
e. **Nuova sessione**: pagina di configurazione di una nuova sessione (paragrafo 1.2.4).

2. **Riquadro "Panoramica"**, riepiloga lo stato dei consumi relativamente ai crediti disponibili e permette di acquistarne di aggiuntivi.
3. **Riquadro "Ultime sessioni"**, riepiloga le ultime sessioni effettuate e permette di eseguire alcune azioni come la visualizzazione dei singoli *file*, il *download* della relazione metodologica oppure il *download* del pacchetto di evidenza forense.

Gestione delle sessioni

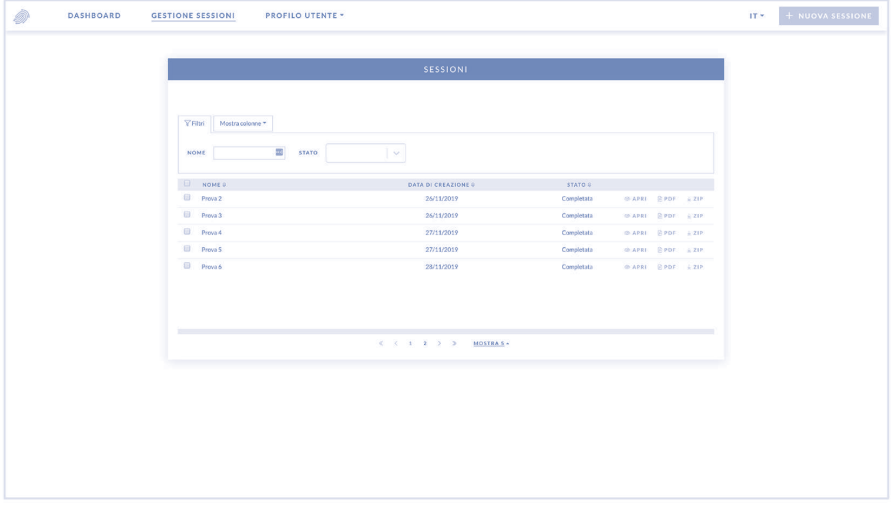

Fig. 2 - Gestione sessioni

La pagina "**Gestione sessioni**" permette di visualizzare l'elenco completo delle sessioni effettuate, mostrando informazioni sul titolo assegnato, sulla data di creazione e sullo stato (Pronta/In elaborazione/Completata).

Dalla tabella è possibile applicare dei filtri per limitare la visualizzazione delle sessioni e ordinare le colonne per il valore desiderato.
Per ogni sessione è possibile compiere alcune azioni:

- **Apri**: permette di visualizzare l'elenco dei *file* che compongono il pacchetto di evidenza forense, mostrarne un'anteprima e scaricarli singolarmente (fig. 3).
- **PDF**: permette di scaricare la relazione metodologica, in formato PDF.
- **ZIP**: permette di scaricare il pacchetto di evidenza forense, in formato ZIP. **Questo *file* dovrà essere prodotto in giudizio, tramite PCT o depositato presso la cancelleria di riferimento, così com'è, senza essere aperto. La memoria predisposta per l'occasione dovrà includere la relazione metodologica, che fornirà al CTU e alla controparte gli elementi essenziali per poter valutare correttamente la prova.**

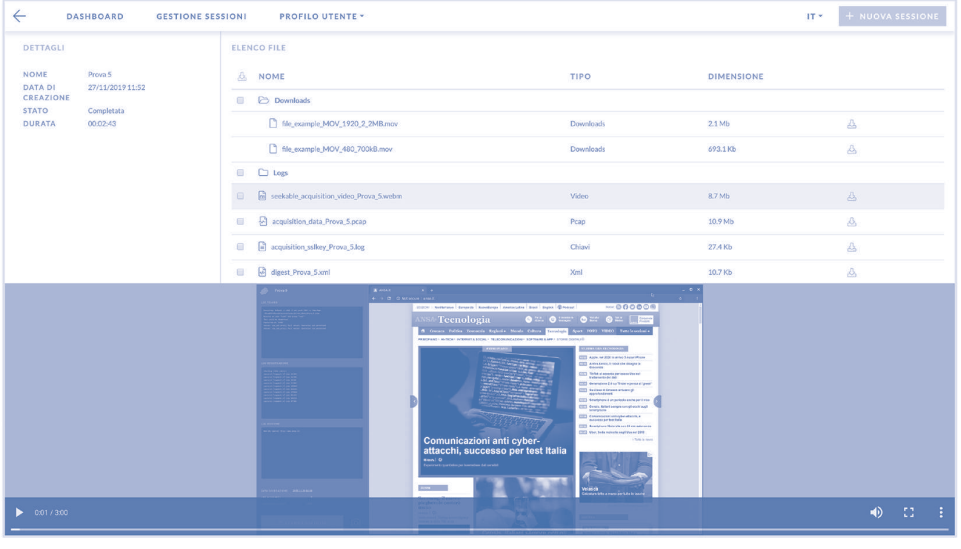

Fig. 3 - Anteprima del pacchetto di evidenza forense

La pagina accessibile premendo il pulsante "**Apri**", associato a ogni sessione, visualizza una schermata (fig. 3) in cui sono evidenziati i dettagli della sessione a sinistra, a destra l'elenco dei *file* che compongono il pacchetto di evidenza forense e in basso l'anteprima di uno dei *file*, se selezionato. In fig. 3, ad esempio, viene mostrata l'anteprima del video della sessione. Da questa pagina l'utente può effettuare il *download* dei *file* singolarmente o in gruppo, selezionando le relative caselle.
La relazione metodologica viene generata e firmata al momento della richiesta di *download*. Questa modalità di generazione istantanea permette all'utente di scegliere di volta in volta la lingua della relazione metodologica selezionando quella di suo gradimento da un menù a tendina collegato al pulsante "**PDF**".

Configurazione di una nuova sessione di acquisizione

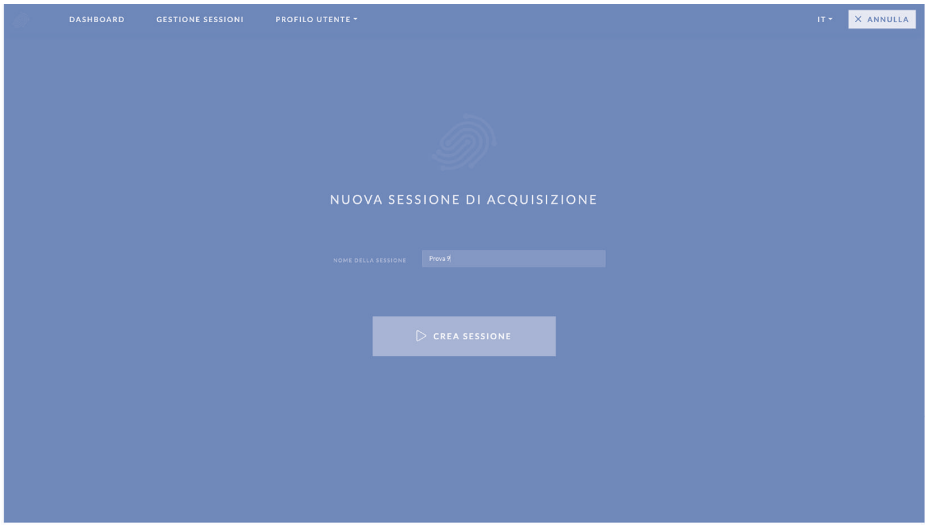

Fig. 4 - Nuova sessione

Cliccando sul pulsante "**Nuova sessione**" nella barra di navigazione si atterra sulla pagina di configurazione di una nuova sessione. Per avvisare l'utente che si sta entrando nell'ambiente l'interfaccia cambia tonalità virando su un tema scuro, dove l'attenzione ricadrà sul contenuto da certificare.
Prima di avviare la sessione l'utente deve assegnare un titolo, che sarà lo stesso che comparirà successivamente nella pagina "**Gestione sessioni**" e servirà anche a identificare in modo univoco il pacchetto di evidenza forense.
Cliccando sul pulsante "Crea sessione" si entra nell'ambiente vero e proprio (fig. 5), dal quale l'utente può avviare la sessione e iniziare l'acquisizione forense dei contenuti di suo interesse.

Fig. 5 - Ambiente di acquisizione

Dal momento in cui l'utente clicca sul pulsante "**Avvia sessione**" a quello in cui viene effettivamente reso disponibile l'ambiente, intercorre un tempo di attesa necessario per avviare gli strumenti funzionali a svolgere correttamente l'acquisizione forense.

Ogni ambiente è una macchina virtuale preconfigurata che deve essere avviata ogni volta da zero per garantire un totale isolamento. Tale tempo di attesa, quindi, permetterà all'utente di lavorare in un ambiente pulito ed estremamente sicuro.

Sessione di acquisizione

Fig. 6 - Sessione di acquisizione

L'ambiente rappresenta nella sua interezza la porzione di interfaccia che sarà registrata come **video della sessione** all'interno del pacchetto di evidenza forense.
L'interfaccia, che si differenzia dalle precedenti per l'assenza della barra di navigazione, si presenta composta dai seguenti elementi:

1. A sinistra una **barra laterale** con diverse informazioni e azioni. Dall'alto verso il basso:

a. Il **titolo della sessione** assegnato in fase di configurazione.
b. Tre **console di log** che visualizzano:
i. I log tecnici dello strumento utilizzato per acquisire il traffico di rete.
ii. I log tecnici dello strumento utilizzato per registrare il video della sessione. Questi log danno contezza della continuità della registrazione evidenziando, a intervalli di qualche secondo, la quantità di frame registrati.
iii. I log della sessione che raccolgono gli URL visitati dall'utente ed eventuali azioni svolte automaticamente dal sistema sottostante.
c. Le **informazioni della sessione**:
i. La data di creazione.
ii. Il numero di URL acquisiti.
iii. Il numero di crediti utilizzati.
d. Il pulsante "**Ferma e archivia**": conclude la sessione e istruisce il sistema di confezionare il pacchetto di evidenza forense, ovvero la creazione di un *file* XML contenente l'impronta digitale di ogni *file* collegato all'acquisizione forense, la marcatura temporale e firma digitale dello stesso e infine il caricamento di tutti i *file* all'interno di un archivio in formato ZIP. Questo archivio può essere visualizzato e scaricato tramite la pagina "**Gestione sessioni**" , ed è pronto per essere depositato in tribunaleassieme alla relazione metodologica.
e. Il pulsante "**Fotografa**": permette di effettuare uno *screenshot* di quanto mostrato dall'ambiente in quel preciso istante. **Uno o più *screenshot* dei momenti salienti della sessione potrebbero essere inseriti nella memoria per documentare in modo visuale le violazioni riscontrate. Possono tornare utili anche come elementi di prova da fornire al CTU o alla contro-**

parte, assieme al video della sessione, alla relazione metodologica e al pacchetto di evidenza forense. Quest'ultimo, infatti, contiene la prova forense a tutti gli effetti. *Screenshot* e video, però, supportano visivamente quanto descritto nella memoria e permettono una comprensione immediata dell'oggetto della discussione.

2. A destra un **browser forense** dove effettuare la navigazione dei contenuti da certificare.

Durante la sessione l'utente utilizzerà il browser forense per navigare le pagine che mettono a disposizione i contenuti di interesse. **Le console di log visualizzano in tempo reale informazioni tecniche, URL visitati ed eventuali azioni compiute dal sistema sottostante. Mostrare tali informazioni è un aspetto fondamentale per rispettare la proprietà di ridondanza della prova forense, così da limitare al massimo le possibili contestazioni. Per questo motivo si registra tutta la sessione mostrando anche le console di log all'interno del video.**

Per concludere la sessione e creare il pacchetto di evidenza forense è sufficiente cliccare sul pulsante "**Ferma e archivia**", che chiude l'ambiente e riporta l'utente alla *dashboard*.

Il pacchetto di evidenza forense sarà visibile nel riquadro "**Ultime sessioni**" e fruibile attraverso la pagina "**Gestione sessioni**".

Casi di utilizzo

Di seguito verranno illustrati alcuni casi di utilizzo reali di Web Forensics per diverse tipologie di contenuti da certificare come ad esempio **articoli di giornale**, **messaggi pubblicati sui *social network***, ***chat***, ***email***, **contenuti multimediali**, ecc.

Per ogni tipologia sarà descritta la sequenza delle operazioni da eseguire per acquisire i contenuti di interesse.

Acquisizione di un contenuto di pubblico dominio

Come esempio di acquisizione di un contenuto di pubblico dominio procederemo con una pagina web di un un'agenzia di stampa, nel caso specifico il sito web di **AGI** (agi.it).

Fig. 7 - AGI

Questa è la tipologia di acquisizione più semplice, ed è effettuata navigando con il browser forense il sito web in questione e successivamente la pagina web di interesse (fig. 7). Una volta che il contenuto è visibile sul browser forense può considerarsi acquisito.

Per procedere alla generazione del pacchetto di evidenza forense è sufficiente cliccare sul pulsante "**Ferma e archivia**" e concludere la sessione.

Acquisizione di un contenuto privato su un*social network*

Come esempio di acquisizione di un contenuto privato procederemo con una pagina web di un *social network*, nel caso specifico **Facebook** (facebook.com).

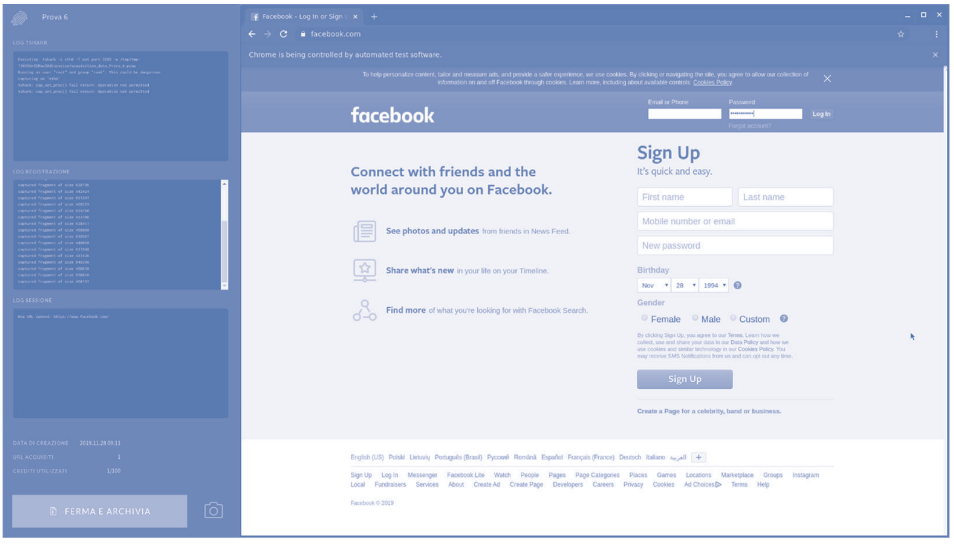

Fig. 8 - Facebook, parte 1 (autenticazione)

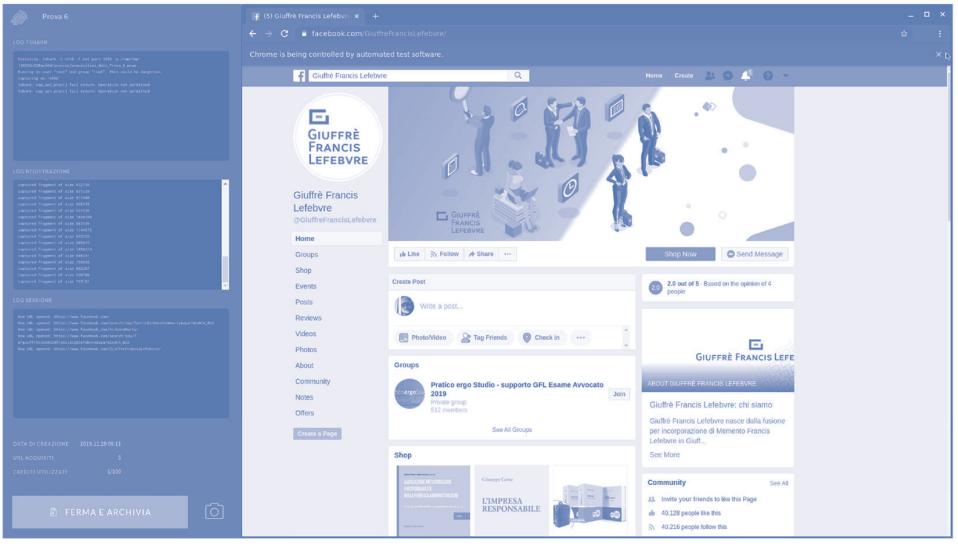

Fig. 9 - Facebook, parte 2 (contenuto)

In questo esempio si vuole acquisire un contenuto statico, ovvero un post pubblicato su una pagina Facebook. Dopo essersi autenticati (fig. 8) è sufficiente navigare fino a visualizzare il contenuto (fig. 9) e procedere alla conclusione della sessione tramite l'apposito pulsante.

Acquisizione di un'*email* fruibile da un *client web*

Come esempio di acquisizione di un'*email* fruibile da un *client web* procederemo con un servizio di posta elettronica molto diffuso, nel caso specifico **Gmail** (gmail.com).

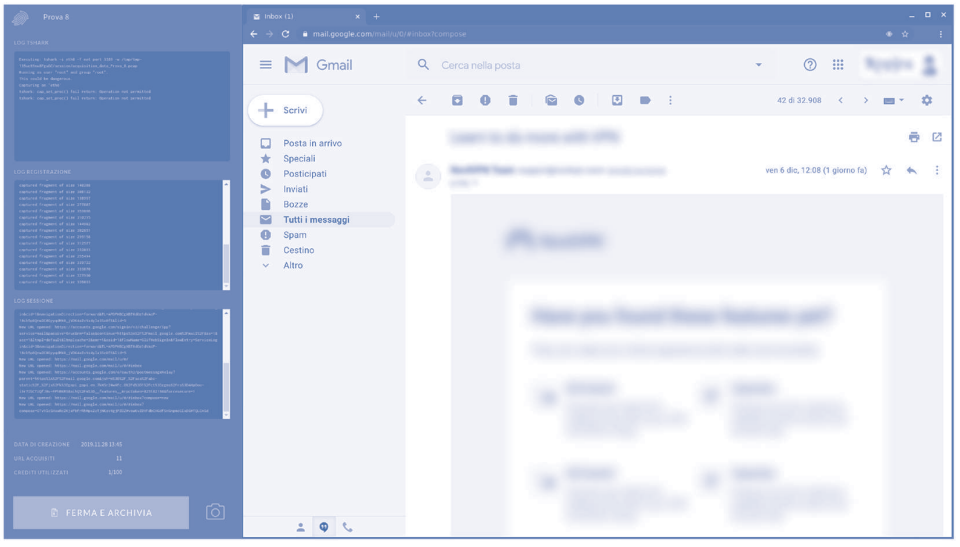

Fig. 10 - Gmail

Come nell'esempio presentato nel paragrafo 6.3.2, anche per Gmail occorre effettuare l'autenticazione, poi navigare fino all'*email* di interesse (fig. 10) e infine procedere alla conclusione della sessione tramite l'apposito pulsante.

CONSIGLI SULL'ACQUISIZIONE DELLE *EMAIL*

Quando si acquisisce un'*email* di interesse è consigliabile mostrarne anche il contenuto originale, cioè il corpo intero che è stato ricevuto dal *server* IMAP/POP3 del proprio fornitore di posta elettronica. Tipicamente tutti i *client web* dispongono di questa funzionalità. Su Gmail, ad esempio, viene definita con l'opzione "Mostra originale". Si noti che le garanzie tecniche sulle *email* dipendono dalle configurazioni avanzate messe in atto volontariamente da *server* del mittente e del destinatario. In generale, non è possibile avere garanzie sulla posta elettronica, in particolar modo non è possibile avere certezza della consegna presso la casella del destinatario. Esistono espedienti per cercare di ovviare a tali limitazioni, come ad esempio l'inserimento di *tracking pixel* nelle *email* inviate, ma esulano dallo scopo di questa breve trattazione

Acquisizione di una *chat* fruibile da un *client web*

Come esempio di acquisizione di una *chat* fruibile da un *client web* procederemo con un servizio di messaggistica istantanea molto diffuso, nel caso specifico **WhatsApp Web** (web.whatsapp.com).

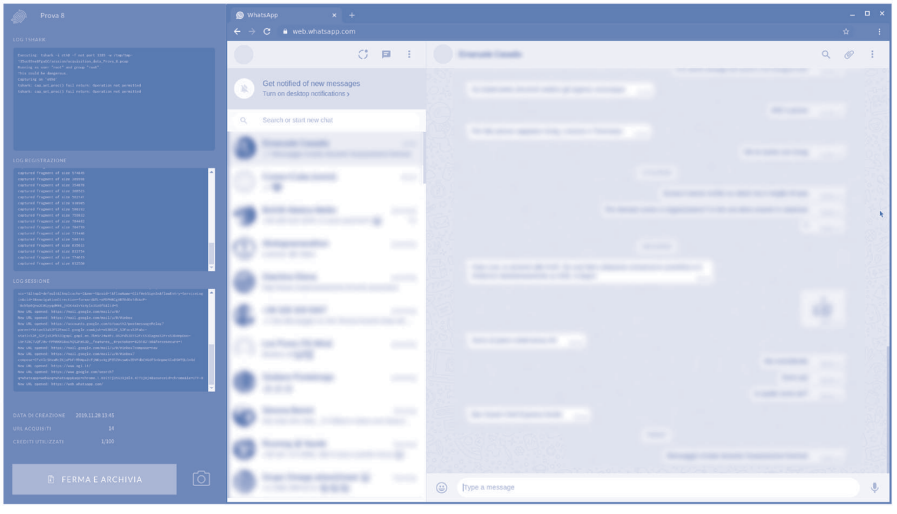

Fig. 11 - WhatsApp Web

Web Forensics permette di acquisire informazioni e messaggi scambiati all'interno di servizi di messaggistica istantanea, come WhatsApp e altri, a patto che questi ultimi offrano la possibilità di utilizzare un *client web*, come WhatsApp Web. Generalmente questi servizi utilizzano un'autenticazione tramite un codice QR che deve essere scansionato tramite l'app del servizio installata sul proprio *smartphone*. Una volta effettuata l'autenticazione è possibile accedere a una conversazione specifica (fig. 11) e navigare fino al messaggio di interesse. Tutte le interazioni effettuate tramite WhatsApp Web e visualizzate sul browser forense durante la sessione saranno disponibili all'interno del pacchetto di evidenza forense.

Acquisizione di un contenuto multimediale

Come esempio di acquisizione di un contenuto multimediale, procederemo con uno *stream* video, nel caso specifico attraverso la piattaforma **YouTube** (youtube.com).

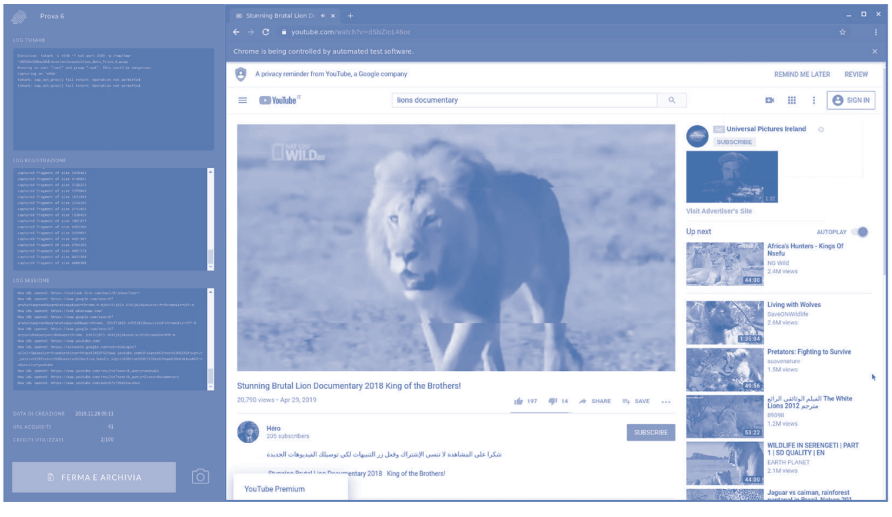

Fig. 12 - YouTube

L'acquisizione di contenuti multimediali comporta una complessità leggermente superiore rispetto a quella necessaria per i contenuti statici presentati negli esempi dei paragrafi precedenti. Le azioni da effettuare per acquisire correttamente uno *stream* video sono le seguenti: navigare fino

alla pagina YouTube riportante il video (fig. 12), avviarne la riproduzione e rimanere sulla pagina il tempo necessario per mostrare il contenuto di interesse.

CONSIGLI SULL'ACQUISIZIONE DI CONTENUTI MULTIMEDIALI DI DURATA ELEVATA

Qualora fosse necessario acquisire video di durata elevata, è possibile adottare alcuni *escamotage*, ad esempio si potrebbe acquisire solamente alcune porzioni in momenti diversi dei video (all'inizio, verso la metà e alla conclusione) o, in alternativa, avvalersi di soluzioni di terze parti per scaricare i video nella loro totalità, avendo premura di accertarsi preventivamente che tali soluzioni non violino i termini di servizio delle piattaforme in questione

Acquisizione del *download* di un *file*

Come esempio di acquisizione del *download* di un *file* procederemo con un *file* di installazione di una distribuzione Linux molto diffusa, nel caso specifico **Ubuntu** (ubuntu.com).

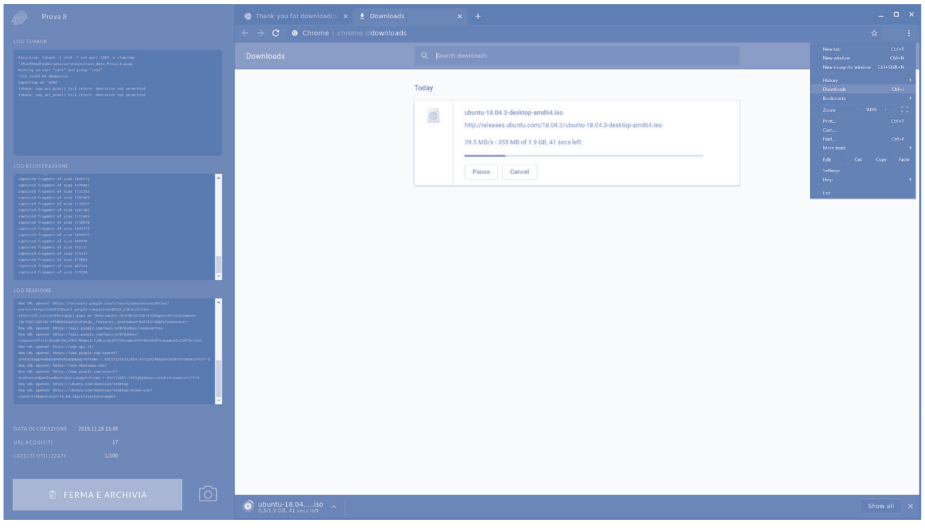

Fig. 12 - YouTube

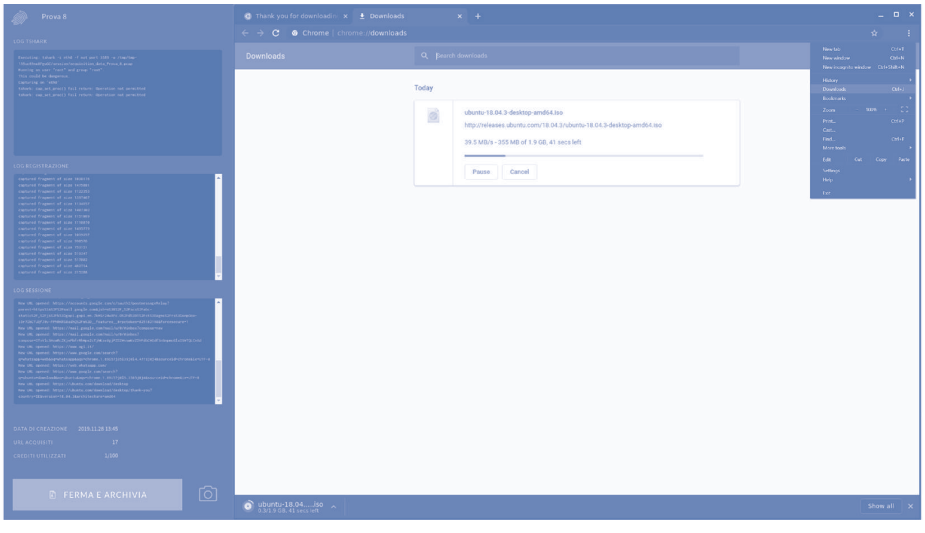

Fig. 13 - Ubuntu

Tramite il browser forense, oltre alla normale navigazione, è possibile effettuare il *download* di *file* che possono essere di interesse per integrare la prova forense. **Frequentemente non è il contenuto testuale o multimediale presente nella pagina web ad essere l'oggetto principale della prova forense, bensì uno o più *file* messi a disposizione del pubblico tramite la pagina web stessa, come ad esempio un documento riportante informazioni rilevanti, un video, un *file* eseguibile, ecc. Per questo motivo è necessario acquisire sia la pagina web, a dimostrazione della provenienza dei *file*, sia i *file* in questione.**

In questo esempio è sufficiente navigare il sito web di Ubuntu, accedere alla pagina web contenente i link per effettuare i *download* e scaricare la versione di interesse. Aprendo la sezione "***Downloads***" del browser forense (fig. 13) possono essere visualizzati i *file* scaricati. **È necessario attendere il corretto completamento di tutti i *download* avviati prima di concludere la sessione, altrimenti si correrà il rischio di ottenere una prova forense parziale. Così facendo alcuni *file* potrebbero risultare corrotti e non sarebbe nemmeno possibile aprirli a posteriori e mostrarne il relativo contenuto.**

Tutti i *file* scaricati durante la sessione possono essere visionati nei dettagli della sessione, accedendo alla cartella "***Downloads***" (fig. 3).

webforensics.kopjra.com

kopjra.com