Web Forensics - Acquisizione delle fonti di prova online

Vincenzo Giovanni Calabrò

Sommario

Web Forensics - Acquisizione delle fonti di prova online.

Chi effettua Investigazioni Digitali Online o l'attività di Open Source Intelligence prima o poi avrà la necessità di "fissare" una pagina web, un'immagine, un post e quant'altro sia rinvenibile sul web, prima che il proprietario possa modificarlo, rimuoverlo o renderlo inaccessibile. Tale circostanza diventa rilevante quando le informazioni trovate generano conseguenze giuridiche che possono assumere rilevanza sia in ambito civile che penale.

Le casistiche che possono essere affrontate nelle investigazioni digitali sono diverse. Possiamo immaginare il caso in cui qualcuno abbia scritto un post su un social che possa pregiudicare l'immagine o la reputazione di qualcun'altro e questi abbia intenzione di querelarlo, oppure l'ipotesi che una persona abbia pubblicato una foto senza chiedere il consenso dell'interessato e, pertanto, la dimostrazione dell'immagine servirà per sporgere denuncia per violazione del diritto all'immagine. Pensiamo alla circostanza in cui il contenuto di un testo sia copiato e pubblicato su un sito, violando il diritto d'autore, e quest'ultimo vuole chiedere un risarcimento del danno. Le fattispecie di reato o le condotte illecite possono essere infinite, ma in tutti i casi dobbiamo raggiungere l'obiettivo di fornire al giudice la prova del contenuto digitale che dimostra un determinato evento o l'informazione che avvalora la tesi. Ciò potrebbe non essere più possibile qualora la controparte, avendo avuto notizia della nostra azione, l'abbia immediatamente modificata o messa off line. Non è raro che le prove digitali rilevanti ai fini di un procedimento penale si trovino in uno Stato diverso da quello di commissione del reato sfuggendo così alla sovranità esclusiva di quest'ultimo.

Come si risolve il problema? Come si può dimostrare la veridicità di una pagina web? Come si può dare valore legale al contenuto di un sito o di un social network?

1 Introduzione alla Digital Forensics

La maggior parte degli utenti della Rete pensa che il metodo più semplice e veloce per dare valenza di prova legale ad una pagina web sia quello di salvarla sull'hard disk sottoforma di file, oppure di stamparla su carta o anche di scattare una foto allo schermo del computer, mentre gli utenti più avanzati la convertiranno in un file pdf oppure realizzeranno uno screenshot del monitor. Nelle aule di Tribunali, ancora oggi, si assiste alla mera produzione della pagina con i metodi predetti, ritenendo detta allegazione idonea a provare in giudizio il fatto lesivo dei propri diritti.

Questa metodologia è ritenuta non sufficiente e inidonea, sia nel panorama giurisprudenziale italiano, che nelle regole tecniche internazionali e nelle varie linee guida, in particolare nel caso in cui avvenga la contestazione circostanziata, in quanto tale produzione documentale non è idonea a garantire l'immodificabilità, la non alterabilità, l'integrità di ciò che rappresenta.[1]

Risulta evidente che la sola rappresentazione grafica, (stampa su carta, salvataggio in formato pdf o immagine, screenshot, etc.) non consente di determinare in che modo e da chi sono giunti i singoli contenuti che compongono la pagina web, si da non poter avere la certezza del fatto digitale alla base delle doglianze espresse in giudizio. Ed infatti, ben potrebbe esser alterata la pagina web prima di essere stampata, andando a rappresentare una realtà non fidefacente e alterando sostanzialmente, con evidente lesione del raggiungimento di ogni procedimento giudiziario: l'accertamento della verità giudiziale. Alla luce di quanto sinora dedotto, risulta evidente come la pagina web possa esser qualificata come documento informatico che, per le caratteristiche intrinseche della stessa e per poter esser validamente depositata in giudizio ed aver efficacia, dovrà esser acquisita secondo le tecniche proprie dell'informatica forense.[2]

Le fonti di prova informatiche in un processo civile o penale sono spesso trattate con poco

---

[1] L'esibizione in giudizio di riproduzioni cartacee delle schermate ricavate dal sito Internet non consente di assolvere al proprio onere probatorio (Trib. Napoli, 2 febbraio 2006), in quanto la pagina web visualizzata dall'utente è composta da differenti file provenienti da web server tutti diversi. Basti pensare, per chiarire, alla composizione della stessa costituita da singoli elementi quali, ad esempio, immagini, filmati, parti di testo, banner pubblicitari che vengono personalizzati a seconda dell'utente che la sta consultando. Infatti la medesima pagina web contattata risulta composita con elementi differenti a seconda del luogo, dell'ora e dell'utente che la contatta, il quale avrà, invece, l'impressione che tutto ciò che viene visualizzato sia fornito unicamente dal sito contattato originariamente.

[2] Cfr. V. COLAROCCO, T. GROTTO, G. VACIAGO, La prova digitale, Giuffrè Francis Lefebvre, Milano, 2020, p. 22 ss.

rigore tecnico: una corretta acquisizione forense di una pagina web, di una chat o di un documento informatico in genere può fare la differenza tra un successo e una rovinosa disfatta.

Il tema della prova è centrale all'interno del processo, costituendo il campo più critico entro il quale si dispiega l'attività degli operatori del diritto e che oggi non può prescindere dall'informatica, dalla volatilità e fragilità del dato informatico, dall'importanza della corretta acquisizione e gestione dei bit, dalla fonte di prova digitale.

La giurisprudenza, pertanto, incoraggia l'utilizzo delle tecniche di informatica forense, affinché siano estratti contenuti in copia dei dati presenti nelle pagine web in Internet, cristallizzati in copie forensi consentendo la produzione di elementi giudiziali certi, in relazione ad integrità dei dati, non manipolazione e certezza temporale, rendendo la copia forense prodotta immodificabile e tendenzialmente vincolante per il giudicante[3].

1.1 Definizioni: Digital Evidence, Digital Investigation e Digital Forensics

La maggior parte delle controversie legali coinvolge elementi di carattere informatico anche quando la materia è tutt'altra. L'avvento delle tecnologie dell'informazione ha determinato un "*cambiamento nelle modalità di rilevazione, gestione, raccolta ed analisi di elementi che, in senso lato e assolutamente generico, si potrebbero definire fonti di prova, prova, indizio o testimonianza*"[4]. In questa sede sono trattati solo gli aspetti tecnici, mentre si rimanda alla lettura di testi più autorevoli, citati nelle note, per un approfondimento giuridico sulla tematica. Prima di addentrarci nell'illustrazione dei metodi di acquisizione e trattamento, introduciamo i concetti di Digital Evidence, Digital Investigation e Digital Forensics.

Digital Evidence - Nella letteratura internazionale è possibile recuperare diverse definizioni di digital evidence o fonte di prova digitale. Tra le varie meritano di essere citate quella di Eoghan Casey, il quale ha definito la digital evidence come "*qualsiasi dato digitale che possa stabilire se un crimine è stato commesso o che può fornire un collegamento tra il crimine e chi l'ha*

[3] Cfr. V. COLAROCCO, M. FERRAZZANO, La pagina web come prova digitale nel processo civile, in "Questioni di informatica forense", Aracne editrice, Roma, 2015, p. 239 ss.
[4] Cfr. L. LUPARIA, G. ZICCARDI, Investigazione penale e tecnologia informatica, Giuffrè, Milano, 2007, p. 3 e ss.

commesso"[5], e la classificazione di digital evidence di Stephen Mason[6], che ha individuato tre diverse categorie:

- *La prova creata dall'uomo*: è tale ogni dato digitale che figuri come il risultato di un intervento o di un'azione umana. Questo può essere di due tipi: human-to-human, come ad esempio uno scambio di e-mail, che presuppone un'interazione tra due individui, e human-to-PC, come ad esempio la redazione di un documento attraverso un software di videoscrittura.
- *La prova creata autonomamente dal computer*: ogni dato che figuri come il risultato di un processo effettuato da un software secondo un preciso algoritmo e senza l'intervento umano (esempi possono essere i tabulati telefonici o i file di log).
- *La prova creata sia dall'essere umano che dal computer*: ogni dato che risulta essere il frutto di un contributo umano e di un calcolo generato e memorizzato da un elaboratore elettronico (un esempio può essere un foglio di calcolo elettronico dove i dati vengono inseriti dall'essere umano, mentre il risultato viene calcolato dal computer).

A prescindere dalla definizione che vogliamo utilizzare, le peculiarità che contraddistinguono la fonte di prova digitale, che non possono essere ignorate, consistono in:

- *Immaterialità*: la prova digitale è il contenuto e non il supporto su cui è memorizzata;
- *Dispersione*: la prova digitale può essere dislocata su più dispositivi molto distanti tra loro,
- *Promiscuità*: la prova digitale può trovarsi all'interno di dispositivi che contengono altre informazioni non attinenti all'indagine,
- *Congenita modificabilità*: la prova digitale è estremamente alterabile.

Dal punto di vista giuridico, si configura come un nuovo mezzo di prova, anche se riconducibile nell'alveo delle prove scientifiche, in virtù dell'impiego della tecnologia; si configura inoltre come prova diretta, avendo ad oggetto il fatto stesso che deve essere provato, direttamente apprezzabile dall'organo giudicante[7]. *"Il valore probatorio della prova informatica deve essere inteso, secondo una parte della dottrina, come la capacità di resistenza ad eventuali contestazioni e capacità di convincimento del giudice, delle parti processuali o di altri soggetti*

---

[5] Cfr. E. CASEY, Digital Evidence and Computer Crime (Third Edition): Forensic Science, Computers, and the Internet, Academic Press, Cambridge, 2011.
[6] Cfr. S. MASON, Electronic Evidence. Discovery and Admissibility, LexisNexis Butterworths, London, 2007.
[7] Cfr. F. CARNELUTTI, Teoria generale del diritto, in "Società del Foro italiano", 1951, Roma, pp. 379-382.

in ordine alla genuinità, non ripudiabilità, imputabilità e integrità del dato stesso e dei fatti dallo stesso dimostrati"[8].

Digital Investigation - Si sviluppa come "*un processo investigativo mediante il quale si utilizzano tecniche informatiche per raccogliere indizi o fonti di prova di varia natura, oppure quando l'informatica assume il ruolo di mero strumento facilitatore dell'investigatore stesso*"[9].

Tale disciplina non può limitare il proprio raggio d'azione alle sole indagini relative ai c.d. reati informatici, in quanto molti illeciti, così come le azioni della vita quotidiana, non hanno ad oggetto le tecnologie dell'informazione e della comunicazione, ma sono caratterizzate dall'interazione diretta o indiretta con le stesse e, di conseguenza, anche le indagini classiche ricorrono alla Digital Investigation per scoprire e acquisire elementi utili alle indagini.

Digital Forensics – È "*un processo teso alla manipolazione controllata e più in generale al trattamento di dati e/o informazioni digitali e/o sistemi informativi per finalità investigative e di giustizia, adottando procedure tecnico organizzative tese a fornire adeguate garanzie in termini di integrità, autenticità e disponibilità delle informazioni e dei dati in parola*"[10].

In altri termini, la digital forensics può essere definita come una scienza che studia quattro aspetti:

- il problema dell'identificazione della fonte di prova digitale,
- il problema dell'acquisizione e della conservazione della fonte di prova digitale,
- il problema dell'analisi della fonte di prova digitale,
- la documentazione, presentazione o reportistica della forte di prova digitale.

Come si evince dalla definizione, le caratteristiche intrinseche della digital evidence rappresentano le criticità da affrontare attraverso l'applicazione delle metodologie e tecniche offerte dalla digital forensics. Il processo di digitalizzazione delle informazioni relative alla persona, alla sua vita, sia privata che lavorativa, ha ampliato notevolmente il campo d'indagine dei giuristi alla ricerca delle orme digitali: attività oggi possibile grazie alla digital forensics.

Quando è necessario produrre un'informazione in formato digitale, nell'ambito di un procedimento giudiziario, occorre procedere con l'acquisizione della stessa al fine di garantire

---

[8] Cfr. L. LUPARIA, G. ZICCARDI, op. cit.
[9] Cfr. E. CASEY, op. cit.
[10] Cfr. L. LUPARIA, G. ZICCARDI, op. cit., p. 11 e ss.

l'integrità, l'inalterabilità, la paternità e la certezza della data. Per risolvere il problema di disporre di evidenze digitali non disconoscibili, fedeli all'originale e verificabili da tutte le parti occorre impiegare metodologie e tecniche previste dall'informatica forense.

Come accennato, spesso accade di vedere nei fascicoli processuali evidenze, che nascono e sono digitali, in formato cartaceo o in altri formati, perdendo una serie di informazioni rilevanti non più presenti nel nuovo formato, ma che arricchiscono il significato di ciò che rappresentano. Un esempio per tutti sono i cosiddetti metadati – quali ad esempio la data di ultima modifica o di ultima stampa, l'ultimo autore, la provenienza – o in dati correlati – come la stratificazione dei documenti utile per provare l'evoluzione nel tempo.

Eoghan Casey[11] sostiene che l'affidabilità delle fonti di prova digitali è ormai un problema che coinvolge tutte le questioni giuridiche ed individua quattro grandi rischi nel trattamento delle evidenze che possono pregiudicare l'attendibilità:

- *Il rischio di una cattiva gestione (mishandling*): le evidenze sono state acquisite male perché spesso non si aderisce a degli standard che sono ormai riconosciuti e a principi che la comunità scientifica ritiene come corretti. Inoltre, una cattiva gestione delle fonti di prova digitali può generare responsabilità in capo a chi maneggia i dati e raccoglie le fonti di prova, oltre a rendere più difficile, poi, stabilire la provenienza e l'integrità dei dati, così come la affidabilità dei risultati dell'analisi forense e delle conclusioni. Il risultato è che, alla fine, se la fonte di prova è gestita male, diventa assai complesso e difficile stabilire la sua affidabilità;
- *Il rischio di una cattiva interpretazione (misinterpretation):* le fonti di prova sono osservate tramite sistemi e strumenti che possono portare errori tecnici (dati incompleti, inaccurati, alterati o corrotti), a cui si aggiunge la possibilità di fonti di errore non tecniche, che includono incompetenza, bias cognitivi e pregiudizi vari, oltre a problemi pratici di gestione e di organizzazione. La combinazione degli errori tecnici e non tecnici porta ad un esito errato;
- *Il rischio di manipolazione (concealment):* qualcuno cerca di ingannare l'analista, attraverso l'uso di tecniche di anti-forensics che cancellano o alterano le evidenze digitali,

[11] Cfr. E. CASEY, Trust in digital evidence, in "Forensic Science International: Digital Investigation", F. 31 (2019) 200898, Elsevier, Amsterdam, 2019.

e di conseguenza si rischia di trarre delle conclusioni errate. Nel caso in cui si rilevino attività di occultamento o falsificazione, può essere utile concentrarsi sulle tracce di alterazione piuttosto che sulla generale affidabilità delle evidenze o della fonte;

- *Il rischio di incomprensione (misexplanation):* l'analista non si riesce ad esporre bene le attività svolte. In giudizio diventa essenziale essere chiari e spiegare ai non addetti ai lavori (spesso ostili e disinteressati) concetti tecnici anche complessi. Una spiegazione troppo complessa, e ragionamenti deboli, possono minare la comprensione generale dei fatti.

In altre parole, la digital forensics deve essere fondata su principi e pratiche molto ferme che gli esperti seguono per gestire e interpretare correttamente le fonti di prova, per evitare incomprensioni e per affrontare anche le ipotesi di anti forensics. Lo scopo dell'informatica forense si esplicita nelle seguenti prerogative: di identificare, acquisire, conservare, documentare e interpretare i dati contenuti all'interno dei dispositivi di memorizzazione di dati digitali o trasmessi in una rete di comunicazione in maniera affidabile.

L'ordinamento italiano, dopo l'approvazione della Legge 48 del 2008 di ratifica della Convenzione sul Cybercrime di Budapest, ha stabilito che, nel processo penale, tutte le attività probatorie che hanno ad oggetto le prove digitali devono essere disposte attraverso tecniche idonee ad assicurare la conservazione dei dati originali ed impedirne l'alterazione. Pertanto, è necessario che anche le metodologie utilizzate per il trattamento delle evidenze digitali abbiano la capacità di resistenza ad eventuali contestazioni e capacità di convincimento del giudice e delle parti processuali in ordine alla loro verificabilità, ripetibilità, riproducibilità e giustificabilità. Per tale motivo è fortemente consigliato impiegare tecniche e standard ispirati al metodo scientifico[12].

1.2 Standard Internazionali

Perché è importante acquisire le fonti di prova digitale secondo una corretta metodologia prevista dalla digital forensics? Le ragioni sono sostanzialmente due: la prima è una ragione di natura normativo-giurisprudenziale. L'approvazione della Legge 48 del 2008, che ha ratificato la Convenzione sul Cybercrime, ha creato una prima pietra miliare sulla necessità di acquisire

[12] Il metodo scientifico (o metodo sperimentale) è la modalità tipica con cui la scienza procede per raggiungere una conoscenza della realtà oggettiva, affidabile, verificabile e condivisibile.

la prova secondo una corretta metodologia che sia in grado di garantire la non alterabilità, una data certa, la non modificabilità, in pratica una serie di requisiti che ovviamente sono necessari affinché una evidenza possa essere acquisita da un giudice e possa essere ritenuta valida a tutti gli effetti dal punto di vista giuridico. La seconda ragione è di natura evidentemente pratica. Sempre di più utilizziamo gli strumenti dell'ICT, i servizi cloud, le piattaforme social, viviamo, sostanzialmente, con il nostro smartphone attaccato al nostro corpo e, pertanto, è evidente che l'utilizzo pervasivo della fonte di prova digitale necessita di soluzioni, anche software, in grado di acquisirla in maniera corretta e in maniera assolutamente anche semplificata. Negli ultimi decenni sono stati avviati diversi gruppi di studi allo scopo di sviluppare delle metodologie, previste dalla best practice della digital forensics, nel rispetto di quanto previsto dalla legge 48 del 2008. In generale, si tratta di individuare le modalità e le tecnologie migliori per soddisfare i seguenti obiettivi:

- acquisire le prove senza alterare o modificare il sistema informatico su cui si trovano,
- garantire che le prove acquisite siano identiche a quelle originarie,
- analizzare i dati senza alterarli,
- esplicitare il processo per renderlo ripetibile,

allo scopo di "*dar voce alle prove*"[13].

Tra le varie proposte, il Technical Committee ISO/IEC[14] JTC 1/SC 27- Information security, cybersecurity and privacy protection, ha sviluppato un insieme di norme che hanno lo scopo di proteggere le informazioni che vengono mantenute ed elaborate da un'organizzazione. In questa serie troviamo le linee guida, focalizzate sull'analisi degli incidenti informatici, divenute lo standard *de facto* per la gestione delle evidenze digitali:

- ISO/IEC 27043 "*Incident investigation principles and processes*" (pubblicato il 04.03.2015) fornisce una panoramica generale di tutti i principi e processi di indagine sugli incidenti[15];
- ISO/IEC 27035 "*Information security incident management - Part 1, 2, 3*" (pubblicato a partire dal 28.10.2016) fornisce i concetti e le fasi principali della gestione degli incidenti

[13] Cfr. C. MAIOLI, Dar voce alle prove: elementi di informatica forense, in "La sicurezza preventiva dell'informazione e della comunicazione" (a cura di P. Pozzi), Bologna, 2004, pp. 66-75.
[14] ISO: International Organization for Standardization – IEC: International Electrotechnical Commission.
[15] ISO/IEC 27043:2015 (https://www.iso.org/standard/44407.html).

di sicurezza delle informazioni[16];

- ISO/IEC 27037:2012 "*Guidelines for identification, collection, acquisition and preservation of digital evidence*" (pubblicato il 15.10.2012 e confermato il 09.07.2018) fornisce le linee guida per le specifiche attività di gestione delle potenziali prove digitali, concentrandosi in particolar modo sulle fasi di identificazione, raccolta, acquisizione e conservazione di quelle evidenze che potrebbero avere valore probatorio[17];
- ISO/IEC 27042:2015 "*Guidelines for the analysis and interpretation of digital evidence*" (pubblicato il 19.06.2015) fornisce una guida all'analisi e all'interpretazione delle evidenze digitali utili ad affrontare i problemi di continuità, validità, riproducibilità e ripetibilità[18];
- ISO/IEC 27041:2015 "*Guidance on assuring suitability and adequacy of incident investigative method"* (pubblicato il 19.06.2015) fornisce una guida per garantire che i metodi e i processi utilizzati nelle indagini sugli incidenti di sicurezza delle informazioni siano idonei[19].

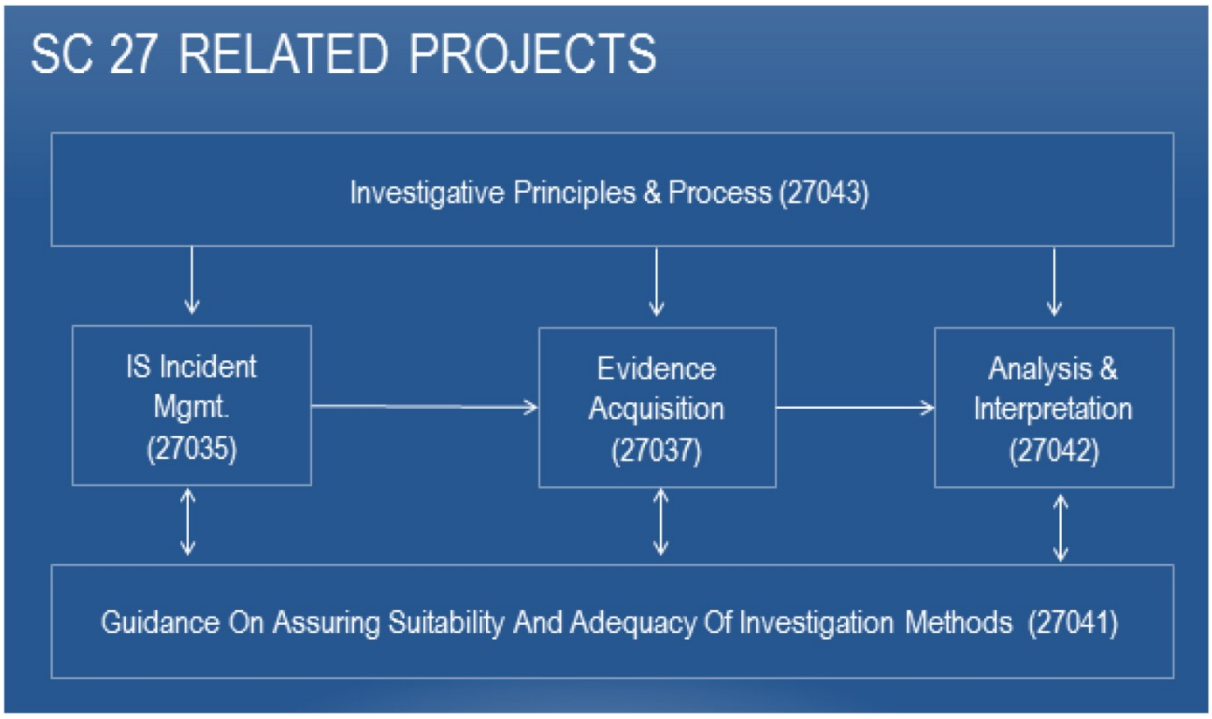


Fig. 1 – Gli standard ISO/IEC focalizzati per la gestione delle evidenze digitali.

[16] ISO/IEC 27035-1:2016 (https://www.iso.org/standard/60803.html), ISO/IEC 27035-2:2016 (https://www.iso.org/standard/62071.html); ISO/IEC 27035-3:2020 (https://www.iso.org/standard/74033.html).
[17] ISO/IEC 27037:2012 (https://www.iso.org/standard/44381.html).
[18] ISO/IEC 27042:2015 (https://www.iso.org/standard/44406.html).
[19] ISO/IEC 27041:2015 (https://www.iso.org/standard/44405.html).

I requisiti che devono caratterizzare l'evidenza raccolta possono essere sintetizzati nelle nozioni di:

- *Pertinenza*: occorre dimostrare che il materiale è rilevante, cioè che contiene dati utili e che pertanto esiste una buona ragione per acquisirli,
- *Affidabilità*: tutti i processi eseguiti devono essere ben documentati producendo un risultato riproducibile,
- *Sufficienza*: occorre raccogliere tutto il materiale informatico necessario, valutando in base al caso e alle limitazioni di carattere giuridico.

La norma ISO stabilisce i seguenti ulteriori aspetti per il trattamento della prova in formato digitale:

- *Verificabilità*: documentare tutte le attività svolte, un consulente tecnico informatico terzo deve essere in grado di verificare le attività svolte, valutando metodo scientifico, le tecniche e le procedure seguite,
- *Ripetibilità*: le operazioni svolte devono essere ripetibili, usando le stesse procedure, lo stesso metodo, gli stessi strumenti, sotto le stesse condizioni,
- *Riproducibilità*: le azioni possono essere riprodotte usando lo stesso metodo, strumenti diversi, sotto condizioni diverse,
- *Giustificabilità*: bisogna essere in grado di dimostrare che le scelte adoperate erano le migliori possibili o le uniche possibili.

1.3 Fasi della Digital Forensics

Dalla lettura delle linee guida ISO sopra menzionate, ricaviamo sinteticamente due (2) macro attività, suddivise in sei (6) fasi, con cui si sviluppa l'intero processo di digital forensics. Questa ripartizione di funzioni consente di esplicitare i risultati attesi ad ogni singolo passo e risulta particolarmente utile nei casi in cui l'attività forense è frazionata oppure è sviluppata da attori diversi.

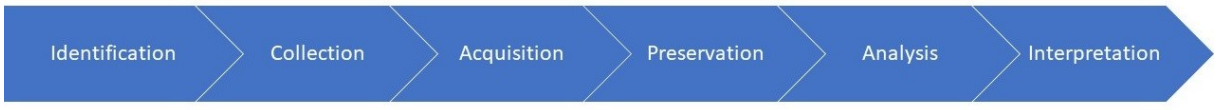
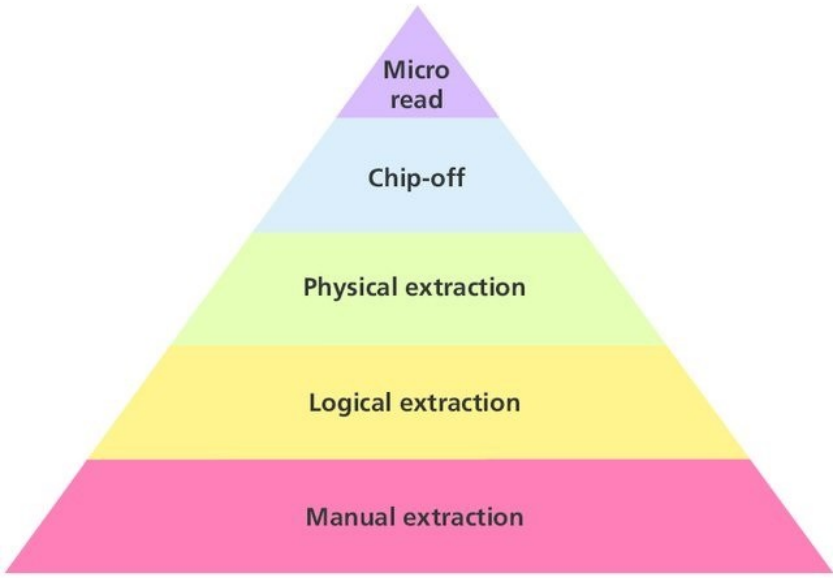


Fig. 2 – Fasi della Digital Forensics.

La prima macro attività (cfr. ISO/IEC 27037:2012) si concentra, sostanzialmente, sulla gestione dell'evidenze digitali e si concretizza nelle seguenti fasi:

1. *Identification*: Il processo di identificazione implica la ricerca, l'individuazione e la documentazione delle potenziali prove digitali. Si dovranno individuare i supporti di archiviazione digitale e i device di elaborazione che possono contenere potenziali prove digitali. Comprende anche un'attività di attribuzione della priorità nella raccolta delle prove basata sulla loro volatilità. Inoltre, si dovrà accertare l'eventualità di potenziali prove digitali nascoste. Il risultato di questa fase è un inventario dei dispositivi individuati a cui è associato un identificativo (ID). Una volta completata questa fase, occorre decidere se procedere con l'operazione di raccolta (collection) o con quella di (acquisitation) acquisizione;
2. *Collection (Raccolta):* Questa fase prevede la rimozione dei dispositivi, precedentemente identificati nella loro locazione originaria, al fine di trasferirli in laboratorio (o in un ambiente controllato equivalente) per effettuare le operazioni di acquisizione ed analisi. In questa fase occorre quindi porre particolare attenzione allo stato del dispositivo (acceso/spento) e, a secondo del caso, è necessario utilizzare differenti approcci e/o strumenti. La persona incaricata a svolgere la fase di raccolta deve scegliere il miglior metodo possibile basandosi sul contesto, il costo e il tempo a disposizione. Inoltre, deve accuratamente documentare tutta l'attività, inclusa la preparazione dei dispositivi al trasporto, e utilizzare appropriati strumenti d'imballaggio. Nel caso in cui si scelga di non prelevare tutti i dispositivi identificati, la scelta deve essere opportunamente documentata e giustificata in conformità alle normative vigenti;
3. *Acquisition (Acquisizione):* Questa fase riguarda la produzione di una copia forense del dispositivo che potrebbe contenere prove digitali e la stesura della documentazione riguardante i metodi utilizzati e le attività effettuate a tale scopo. La documentazione prodotta dovrà consentire di rendere riproducibile e verificabile tutto il processo. Inoltre, la bontà del metodo di acquisizione (identità tra fonte originale e copia) dovrebbe essere verificabile tramite l'utilizzo di una funzione di verifica attendibile (es. una funzione di hash) in modo tale che l'output della funzione applicata all'originale ed alla copia sia identico. Potrebbe succedere che l'acquisizione porti ad inevitabili modifiche dei dati digitali, nel qual caso le attività svolte vanno accuratamente documentate per poter risalire alle responsabilità delle modifiche. Possono inoltre verificarsi casi in cui non è possibile

effettuare la verifica del metodo di acquisizione (es. settori danneggiati, sistema in esecuzione): in situazioni di questo tipo bisogna cercare di eseguire la verifica della maggior parte dei dati (utilizzando il miglior metodo disponibile e giustificandolo) o, se non fosse proprio possibile procedere in altro modo, documentare e giustificare l'assenza della verifica. Infine, se non fosse possibile procedere con la copia forense, occorre procedere con un'acquisizione logica del sistema (a livello di file o partizione), tenendo presente che alcuni dati (ad esempio lo slack space, i file cancellati) potrebbero non essere copiati;



SOURCE: NIST, 2013.

Fig. 3 - I metodi di acquisizione.

4. *Preservation (Conservazione):* Le potenziali prove digitali vanno conservate correttamente per garantire la loro utilizzabilità in fase di investigazione. Questa fase è quindi trasversale a tutte le altre ed inizia già a partire dalla fase di raccolta o acquisizione, in modo da garantire che in nessun momento la potenziale prova digitale possa venire alterata involontariamente o volontariamente. Il forenser, quindi, dovrebbe essere in grado di dimostrare che le prove non siano mai state modificate dal momento della loro raccolta o acquisizione, o nel caso in cui vi fossero state modifiche inevitabili, che queste siano state accuratamente documentate. Nella fase di conservazione delle prove bisogna considerare anche la confidenzialità dei dati, che può essere dettata da requisiti di business (es. proprietà industriale) o da requisiti legali (es. legge sulla privacy). Ogni reperto, originale e copia, deve avere una catena di custodia che possa documentarne la tracciabilità al fine di garantire la sua preservazione.

Description of Evidence		
Item #	**Quantity**	**Description of Item** (Model, Serial #, Condition, Marks, Scratches)

Chain of Custody				
Item #	**Date/Time**	**Released by** (Signature & ID#)	**Received by** (Signature & ID#)	**Comments/Location**

Fig. 4 – Esempio di Catena di custodia.

La seconda macro attività (cfr. ISO/IEC 27042:2015) ha ad oggetto l'analisi e l'interpretazione delle evidenze digitali e si sviluppa nelle seguenti fasi:

5. *Analysis (Analisi):* esamina ed analizza le prove acquisite, utilizzando le varie tecniche di identificazione delle prove digitali e, se necessario, spiega come eseguire la ricostruzione delle stesse.
6. *Interpretation (Interpretazione):* si occupa dell'interpretazione dei risultati ottenuti dal processo di esame e di analisi delle prove digitali. Per illustrare i risultati ottenuti, il processo d'interpretazione utilizza metodi e tecniche scientificamente provate. Successivamente, durante la fase di reporting, i risultati del processo di interpretazione delle prove digitali, sono presentati sotto forma di un rapporto scritto nel modo più semplice possibile, chiaro, conciso e inequivocabile. Presentazione: durante il processo di presentazione, il documento redatto nel processo di reporting è presentato ai diversi soggetti interessati nelle forme opportune, come le presentazioni multimediali o la relazione peritale. Questa fase è determinante perché, un errata rappresentazione, rischia di far perdere il potenziale che può derivare dall'utilizzo delle prove digitali in un eventuale dibattimento processuale o di renderle addirittura inammissibili.

Per ogni fase vengono indicate le linee guida relative alle operazioni di base ed alle operazioni

addizionali da svolgere per consentire l'utilizzo efficace delle evidenze digitali in sede processuale.

In sintesi, l'adozione delle predette direttive ha l'obiettivo di produrre dati in formato digitale godendo delle caratteristiche di verificabilità e riproducibilità, consentendo in tal modo di:

- produrre copie forensi dei dati digitali identiche ai dati originari;
- ridurre la possibilità di disconoscimento della copia prodotta in giudizio;
- consentire attività di verifica da parte della controparte;
- consentire agli altri consulenti, in contraddittorio tra le parti, la verifica della genuinità e inalterabilità dell'acquisita fonte di prova digitale.

Nell'ambito dell'analisi forense tali macro-attività rappresentano il ciclo di vita del dato dal momento della sua identificazione fino alla chiusura delle indagini. In particolare, le azioni più delicate sono quelle relative alla gestione delle evidenze (cfr. ISO/IEC 27037:2012), mentre le successive sono meno rischiose, ma più complesse, in quanto si lavora su una copia forense del dato in parola (cfr. ISO/IEC 27042:2015). Comunque, le operazioni devono essere sempre affiancate dalla redazione della documentazione sulla catena di custodia e di appositi verbali nei quali sono riportate dettagliatamente tutte le attività svolte per garantire la ripetibilità e la verifica delle operazioni ed il contraddittorio tra le parti.

2 Web Forensics: peculiarità, evidenze e modalità di acquisizione

L'Internet Forensics si contraddistingue dalle altre branche della digital forensics per la tipologia dei dati d'interesse e la configurazione delle apparecchiature su cui gli stessi sono rinvenibili e, di conseguenza, si caratterizza anche per il modus operandi impiegato nel trattamento delle evidenze digitali nelle varie fasi di identificazione, raccolta, acquisizione, esame ed analisi.

Secondo gli standard internazionali di informatica forense è necessario produrre in giudizio un pacchetto di evidenza forense contenente la prova del fatto che i contenuti visualizzati durante la navigazione fossero online ad una certa data e ora, garantendo la provenienza di tali contenuti, la loro integrità e inalterabilità. Alla prova digitale deve essere collegata una relazione tecnica contenente informazioni puntuali circa la metodologia di acquisizione e ulteriori dettagli tecnici a supporto della verificabilità del processo complessivo.

2.1 Architettura dei servizi Internet

Per comprendere al meglio le predette affermazioni è opportuno ricordare sinteticamente i concetti essenziali dell'architettura di rete e dei servizi Internet.

Internet è una "*rete di telecomunicazione*" che collega tra loro vari nodi. Un "nodo" è qualsiasi dispositivo in grado di comunicare con gli altri nodi e può essere rappresentato da un elaboratore, un router, una stampante, un sensore, una telecamera, ecc. In altre parole, un nodo è qualsiasi dispositivo, dotato di almeno una "*scheda di rete*", in grado di comunicare con gli altri nodi della rete sfruttando la "*suite di protocolli di comunicazione Internet"* (tra questi i protocolli più noti sono: http, HTTPS, FTP, POP3, IMAP, SMTP, DNS, SNMP, DHCP).

Senza addentrarci molto sugli aspetti tecnici (per chi fosse interessato ad un approfondimento si segnala il testo indicato in nota[20]) evidenziamo alcune nozioni basilari utili a riconoscere le evidenze di interesse e attuare le fasi dell'Internet Forensics:

- Ogni nodo è identificato sulla rete a cui è connesso con un identificativo univoco, definito *"indirizzo IP*" (Internet Protocol), composto da 4 numeri (un esempio di

[20] Cfr. A. S. TANENBAUM, D. J. WETHERALL, Fondamenti di reti di calcolatori, Pearson, Milano, 2013.

indirizzo IP è 192.168.1.100);

- Si distinguono indirizzi IP "*Pubblici*" e "*Privati*"[21]: i primi consentono di identificare il nodo sull'intera Rete Internet, gli altri sono riservati ai dispositivi connessi alle reti locali e non sono direttamente raggiungibili sulla Rete Internet;
- Alcuni nodi, denominati "*Router*" (instradatore), sono dotati di 2 o più schede di rete, e di altrettanti indirizzi IP, e si occupano, attraverso opportuni algoritmi, dell'instradamento delle informazioni attraverso la Rete Internet. In altre parole, collegano due o più reti – pubbliche o private – e consentono il trasferimento delle informazioni da un nodo collegato ad una rete ad un altro nodo afferente ad un'altra rete (per esempio collegano una rete locale LAN alla rete Internet);
- Per agevolare l'operazione di ricerca degli indirizzi IP, questi ultimi possono essere associati ad etichette mnemoniche gestite da nodi prestabiliti chiamati "*DNS*" (domain name server) i quali forniscono, su richiesta, l'indirizzo IP associato ad una determinata stringa. (ad esempio al nome www.google.com corrisponde l'indirizzo IP 172.217.168.196);
- Ogni nodo può ugualmente, e contemporaneamente, ricevere e inviare informazioni agli altri nodi. Quando un nodo effettua una richiesta si identifica come "*client*", quando, invece, risponde alla richiesta di un altro nodo riveste il ruolo di "*server*";
- I nodi "*server*" rendono accessibili le proprie informazioni agli altri nodi attraverso determinate funzionalità denominate "*servizi*", ogni servizio è identificabile da un nome e da un numero di port (p.e. il nodo che ospita il sito web www.google.com è identificato "*dall'indirizzo ip*" 172.217.168.196 e dal numero di "*port*" 80 normalmente associato al servizio basato sul protocollo "*http*". Per cui, se un nodo volesse interrogare il sito web www.google.com, dovrebbe inviare una richiesta al nodo con l'indirizzo ip 172.217.168.196 indicando il port 80;
- Pertanto, un nodo può essere classificato non solo con l'indirizzo IP, ma anche dal servizio che espone agli altri nodi. Tra le varie tipologie possiamo distinguere nodi che:
  - ospitano informazioni o banche dati (cd. Web Server o http Server);
  - consento lo scambio dei messaggi di posta elettronica (cd. Email Server, POP

[21] Gli indirizzi IP privati, definiti nella RFC 1918, sono riservati alle reti locali allo scopo di ridurre le richieste di indirizzi pubblici. Sono suddivisi in classi: da 10.0.0.0 a 10.255.255.255, da 172.16.0.0 a 172.31.255.255, da 192.168.0.0 a 192.168.255.255.

Server, IMAP Server, SMTP Server);

- rendono fruibili file di vario genere (cd. FTP Server o Cloud File Server);
- inviano flussi audio e video (cd. Streaming Server);
- consentono le chiamate audio/video (VOIP Server, Video Conferencing Server).

Altri nodi sono destinati alla sicurezza delle comunicazioni, ovvero filtrano e monitorano il traffico di rete per evitare accessi abusi o malevoli alle informazioni contenute all'interno di una determina rete, oppure facilitano la disponibilità delle informazioni. Tra questi distinguiamo i Proxy Server, i Firewall, gli Intrusion Detection and Prevention Systems (IDPS), i Security Information and Event Management (SIEM), i Load Balancer Server, i nodi di una Content Delivery Network (CDN), ecc.

In sintesi, l'Internet Forensics rappresenta la branca della Digital Forensics specializzata nell'identificazione, raccolta, acquisizione, conservazione, analisi e interpretazione di quelle evidenze digitali generate, memorizzate e trasmesse dagli apparati connessi alla Rete Internet e, di conseguenza, consente di documentare fatti e/o eventi e/o azioni accaduti attraverso l'uso di queste tecnologie.

Il problema principale da affrontare in questa fattispecie di indagine digitale è rappresentato dall'acquisizione delle evidenze poiché, come è facilmente intuibile, è necessario individuare i nodi in cui sono memorizzate ed acquisirle in maniera diretta o indiretta tramite il gestore del nodo.

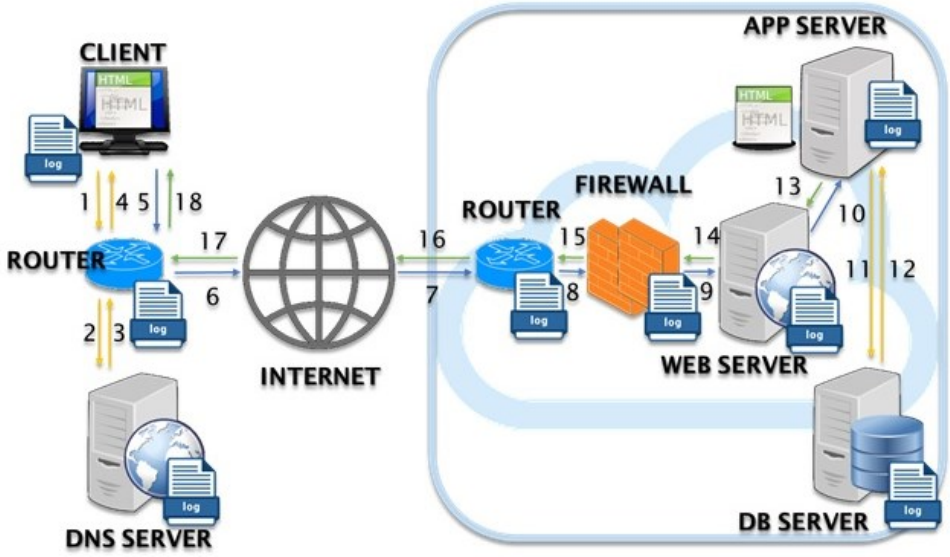


Fig. 5 – Schema semplificato della richiesta di una pagina web.

La figura illustra sinteticamente i nodi convolti nel processo di interrogazione di una pagina web, distinguiamo le richieste effettuate dal nodo "*client*" e le risposte rilasciate dai nodi "*server*". Quello che emerge dall'analisi di questo schema è che ogni freccia, che identifica univocamente una richiesta o una risposta, genera uno o più eventi ognuno dei quali lascia almeno una "*traccia*" digitale all'interno della memoria del nodo/dispositivo attivato. Queste "*tracce*" sono l'oggetto di interesse del processo di digital forensics applicato alle comunicazioni che hanno luogo attraverso la rete Internet.

2.2 Evidenze digitali dei servizi Internet

Il breve excursus tecnico (perdonate l'eccessiva semplificazione dei concetti) spero sia servito a chiarire ai non tecnici come avviene lo scambio dei dati attraverso la Rete Internet e che ciò implica il coinvolgimento di diversi componenti, tra i quali rammentiamo i principali:

- il nodo "*client*", ovvero colui che avvia la richiesta di dati e riceve la risposta dal "*server*",
- il nodo "*server*", ossia colui che riceve la richiesta di dati e genera la risposta al "*client*";
- i nodi "*router*", coloro che si occupano di recapitare i messaggi tra i vari nodi;
- i nodi "*ausiliari*", DNS, FIREWALL, ecc., che facilitano e rendono sicura la comunicazione.

Ognuno di questi nodi ha, ovviamente, delle peculiarità connesse al ruolo/servizio che svolge nell'ambito della trasmissione dei dati e alle caratteristiche tecniche che li contraddistinguono.

Le proprietà e le finalità dei nodi sono rilevanti perché ci consentono di individuare le tipologie di dati utili all'analisi forense. Distinguiamo:

- le informazioni concernenti le proprietà e la configurazione del singolo apparato;
- il dato memorizzato sul nodo "*server*" e il dato ricevuto dal nodo "*client*";
- il registro della comunicazione che ha coinvolto il nodo (cd. "*Log files"*)[22].

Le informazioni concernenti le proprietà e la configurazione del singolo apparato sono utili per comprenderne lo stato, la configurazione della rete e dei servizi; ed individuare eventuali errori

[22] Il Log file è letteralmente un registro digitale in cui sono memorizzate le informazioni connesse ad una determinata attività. Nel caso specifico, ovvero la trasmissione di dati, contiene le registrazioni delle richieste e delle risposte che transitano da un determinato nodo.

o anomalie accaduti durante lo scambio dei dati.

I dati, presenti sul server o sul client, costituiscono il contenuto informativo richiesto, trasmesso e ricevuto tra i due nodi della comunicazione.

I registri delle comunicazioni (cd. Log files) rappresentano il riscontro dello scambio dei dati.

I log files rivestono, spesso, un ruolo determinante nelle indagini riguardanti le transazioni online, perché consentono di ricostruire la comunicazione laddove non si conoscono i nodi principali, oppure non è possibile repertarli. Queste utili evidenze soffrono, sfortunatamente, di due criticità:

- il formato utilizzato per la loro memorizzazione non è standardizzato, di conseguenza il processo di ricostruzione della catena di comunicazione tra due o più nodi risulta particolarmente complesso poiché occorre preliminarmente trasformare il dato in un formato unico;
- lo spazio di memoria dedicato alla loro memorizzazione è spesso insufficiente o volatile, per cui si rischia di perdere informazioni storiche e non poter effettuare ricerche datate.

Inoltre, in alcuni casi è utile acquisire anche i log delle comunicazioni (cd. "*Tabulati*") direttamente dai gestori delle reti in quanto, attraverso l'incrocio dei dati riportanti, ci consentono di corroborare o confermare le informazioni riportate nei file di log degli apparati di rete.

2.3 Modalità di acquisizione

Come è già stato introdotto nel paragrafo precedente, l'acquisizione delle evidenze digitali prevede, dapprima, l'individuazione del supporto su cui è memorizzata l'informazione d'interesse e, successivamente, l'estrazione attraverso l'applicazione di metodologie e strumenti in grado di preservare il più possibile l'autenticità e l'integrità del dato originale.

Nel caso specifico dell'Internet Forensics, in cui il dato di interesse può memorizzato all'interno di più nodi distribuiti globalmente sulla Rete Internet, possono essere adottate due strategie:

1. *on-premise (in sede):* acquisire il dato direttamente dai vari Internet Service Provider, coloro che gestiscono il singolo servizio web, recandosi fisicamente presso il loro data center oppure delegando gli stessi ISP ad effettuare una copia per noi;
2. *off-premise (a distanza / online):* interrogare l'informazione tramite un dispositivo client

collegato alla rete e acquisirla dalla memoria dello stesso client. (si ricorda che un'interrogazione effettuata tramite la rete implica l'inoltro di una richiesta di dati dal client al server, un'elaborazione della risposta da parte del server e il trasferimento dell'informazione dal server al client – vedasi schema della figura precedente).

La modalità on-premise (in sede) consente di prelevare le evidenze direttamente dalla fonte, ma, spesso, questa ipotesi non è percorribile per una serie di fattori tra cui:

- il nodo/server non è agevolmente identificabile e raggiungibile. Si pensi, ad esempio, alle infrastrutture dei grandi Social Media o degli Operatori OTT – Over-The-Top[23],
- non siamo nelle condizioni giuridiche per chiedere ad un terzo la copia forense di un dato, anche se è pubblico, perché siamo in una fase di precontenzioso;
- il server si trova in uno stato estero per cui è necessaria una rogatoria internazionale di difficile attuazione;
- il dato d'interesse ha un alto grado di volatilità, si pensi ad un post pubblicato su un portale social, e pertanto si rischia di non trovarlo più disponibile;
- il tempo concesso per svolgere l'indagine non è compatibile con le tempistiche scandite da questa modalità di acquisizione.

Nel caso in cui ci si trova in una delle predette fattispecie si sfrutta l'altra modalità (cd. Off-premise / a distanza / online), ovvero acquisiamo il dato a distanza, o da remoto, attraverso l'interrogazione della fonte tramite una connessione alla rete Internet.

Gli esempi citati introducono un nuovo paradigma di acquisizione: non si deve più acquisire laddove il dato digitale effettivamente risiede, ma dove la stessa informazione viene visualizzata.

In questo scritto tratteremo quest'ultima metodologia perché è quella più affine alle indagini online su fonti aperte (OSINT/SOCMINT), per un approfondimento sulla prima modalità si consiglia la lettura dei testi indicati in nota[24].

La metodologia di acquisizione a distanza è stata oggetto di approfondimento giuridico e, a tal

---

[23] OTT (Over-The-Top): ci si riferisce agli Internet Service Provider che offrono contenuti a livello globale (p.e. Google, Facebook, Amazon, Apple) e, pertanto, dispongono di infrastrutture digitali distribuiti basate sul Cloud.
[24]. Cfr. E. CASEY, Digital Evidence and Computer Crime (Third Edition): Forensic Science, Computers, and the Internet, Academic Press, Cambridge, 2011. - Cfr. A. GHIRARDINI, G. FAGGIOLI, Digital Forensics, Apogeo, Milano, 2013.

riguardo, si rimanda alla lettura dell'art. 32 della Convenzione di Cybercrime sottoscritta a Budapest il 23 novembre 2011 e ratificata in Italia con la legge 48/2008 e delle relative considerazioni[25].

CONVENZIONE DEL CONSIGLIO D'EUROPA SULLA CRIMINALITÀ INFORMATICA

Articolo 32 – Accesso transfrontaliero a dati informatici immagazzinati con il consenso o quando pubblicamente disponibili

Una Parte può, senza l'autorizzazione di un'altra Parte:

a. accedere ai dati informatici immagazzinati disponibili al pubblico (fonti aperte), senza avere riguardo al luogo geografico in cui si trovano tali dati; o

b. accedere o ricevere, attraverso un sistema informatico nel proprio territorio, dati informatici immagazzinati situati in un altro Stato, se la Parte ottiene il consenso legale e volontario della persona legalmente autorizzata a divulgare i dati allo Stato attraverso tale sistema informatico.

[25] Cfr. V. COLAROCCO, T. GROTTO, G. VACIAGO, op. cit.

3 Mapping delle ISO/IEC 27037 e 27042 all'Internet Forensics

3.1 Identificazione

In questa fase è necessario ricercare, individuare e documentare le potenziali prove digitali. Occorre, pertanto, stabilire qual è l'evidenza oggetto di analisi e descrivere gli elementi che la caratterizzano. Questa affermazione, che in un contesto generale potrebbe apparire poco rilevante o banale, è fondamentale nelle attività eseguite a distanza poiché non abbiamo la possibilità di repertare l'evidenza in sede e, soprattutto, abbiamo la necessità di assicurare i requisiti di verificabilità, ripetibilità, riproducibilità e giustificabilità precedentemente introdotti.

Per tale motivo si suggerisce di procedere alla raccolta delle informazioni, preferibilmente utilizzando una scheda informativa (cd. "*identification sheet*"), che descrive al meglio il canale di comunicazione e l'infrastruttura che ci consente di raggiungere, accedere ed estrapolare le evidenze di interesse.

In pratica, in questa fase occorre:

1. identificare e documentare le informazioni che permettono di descrivere le caratteristiche del server che ospita il dato di interesse (p.e. nome di dominio, dati di registrazione del nome di dominio, indirizzo IP, servizi disponibili, localizzazione del server, data e ora del server, etc.);
2. descrivere dettagliatamente quale tipologia di servizio Internet si sta interrogando: sito web, posta elettronica, streaming audio/video, social network, condivisione di file, cloud storage, e-commerce o marketplace, banking o payment online, etc.;
3. individuare e rappresentare la postazione, gli strumenti e la connessione che saranno utilizzati per interrogare e acquisire le evidenze oggetto di analisi.

IDENTIFICATION SHEET

IDENTIFICATIVO CASO:		COMMITTENTE:	
DATA E ORA:		COMPILATORE:	
DESCRIZIONE:			

Informazioni sul Target

NOME A DOMINIO:			
INFO REGISTRANTE:			
IP ADDRESSES:		NAMESERVERS:	
LOCALIZZAZIONE:		DATA E ORA:	
SERVIZI DISPOBINILI:			
SERVIZI DI INTERESSE:			

Informazioni sulla Connettività

INTERNET SERVICE PROVIDER:					
LOCALIZZAZIONE:		DATA E ORA:			
IP ADDRESS PUBLIC:		DNS SERVERS:			
PROXY SERVER:	NO / SI	URI:		PORT:	
INDIRIZZO:					

Informazioni sul Client di Acquisizione

SERVIZIO IN HOSTING:	NO / SI	URI:					
POSTAZIONE CLIENT:	NO / SI	IN VIRTUAL MACHINE:	NO / SI	IN CLOUD:	NO / SI		
LOCALIZZAZIONE:		DATA E ORA:					
CONFIGURAZIONE DI RETE:	INDIRIZZO IP		GATEWAY		DNS		
SISTEMA OPERATIVO:							
SOFTWARE UTILIZZATI:							
NOTE:							

Tab. 1 – Identification Sheet.

Le informazioni da riportare nella scheda informativa possono essere individuate attraverso alcuni portali e tools utilizzabili anche per l'analisi OSINT.

Per individuare le informazioni sul Target si suggerisce l'utilizzo di alcuni servizi web quali:

- **DOMAINTOOLS** (https://whois.domaintools.com/): un portale che ci consente di ottenere le informazioni sul nome di dominio, il proprietario, l'indirizzo del server, la localizzazione, ISP ed i suoi DNS di riferimento;
- **IPINFO.IO** (https://ipinfo.io/): consente di ottenere informazioni dettagliate sull'indirizzo IP;

DOMAINTOOLS PROFILE CONNECT MONITOR SUPPORT Whois Lookup

Home > Whois Lookup > VincenzoCalabro.it

Whois Record for VincenzoCalabro.it

Domain Profile

Registrar Status	ok
Dates	3,909 days old Created on 2010-02-04 Expires on 2021-02-04 Updated on 2020-02-20
Tech Contact	–
IP Address	104.27.144.204 - 562 other sites hosted on this server
IP Location	- California - San Francisco - Cloudflare Inc.
ASN	AS13335 CLOUDFLARENET, US (registered Jul 14, 2010)
Hosting History	1 change on 2 unique name servers over 3 years

Website

Website Title	Vincenzo Calabrò
Server Type	cloudflare
Response Code	200
Terms	386 (Unique: 245, Linked: 191)
Images	4 (Alt tags missing: 1)
Links	45 (Internal: 25, Outbound: 20)

Whois Record (last updated on 2020-10-18)

```
Domain:             vincenzocalabro.it
Status:             ok
Signed:             no
Created:            2010-02-04 19:32:30
Last Update:        2020-02-20 00:49:23
Expire Date:        2021-02-04

Registrant
  Organization:     Vincenzo Giovanni CalabrÃ²
  Address:          SS 18 IV tratto, 133
                    Catona
                    89135
                    RC
                    IT
  Created:          2010-02-04 19:32:28
  Last Update:      2010-02-04 19:32:28

Admin Contact
  Name:             Vincenzo Giovanni CalabrÃ²
  Organization:     Vincenzo Giovanni CalabrÃ²
  Address:          SS 18 IV tratto, 133
                    Catona
                    89135
                    RC
                    IT
  Created:          2010-02-04 19:32:28
  Last Update:      2010-02-04 19:32:28

Technical Contacts
  Name:             Staff Unitedhost
  Organization:     UnitedHost Servizi Internet srl
  Address:          Via Cefalonia 26
                    Brescia
                    25124
                    BS
                    IT
  Created:          2018-07-04 10:24:56
  Last Update:      2018-07-04 10:24:56

Registrar
  Organization:     Servizi Internet S.r.l.
  Name:             REGDOM-REG
  Web:              http://www.regdom.it/
  DNSSEC:           no

Nameservers
  paul.ns.cloudflare.com
  etta.ns.cloudflare.com
```

Fig. 6 - Risultato della ricerca effettuata su whois.domaintools.com

- **WAPPALYZER** (https://www.wappalyzer.com/): rileva le tecnologie in uso sul server;
- **SHODAN** (https://www.shodan.io/): un motore di ricerca dedicato alla ricerca dei dispositivi collegati ad Internet e ci consente di scoprirne anche le tecnologie impiegate.

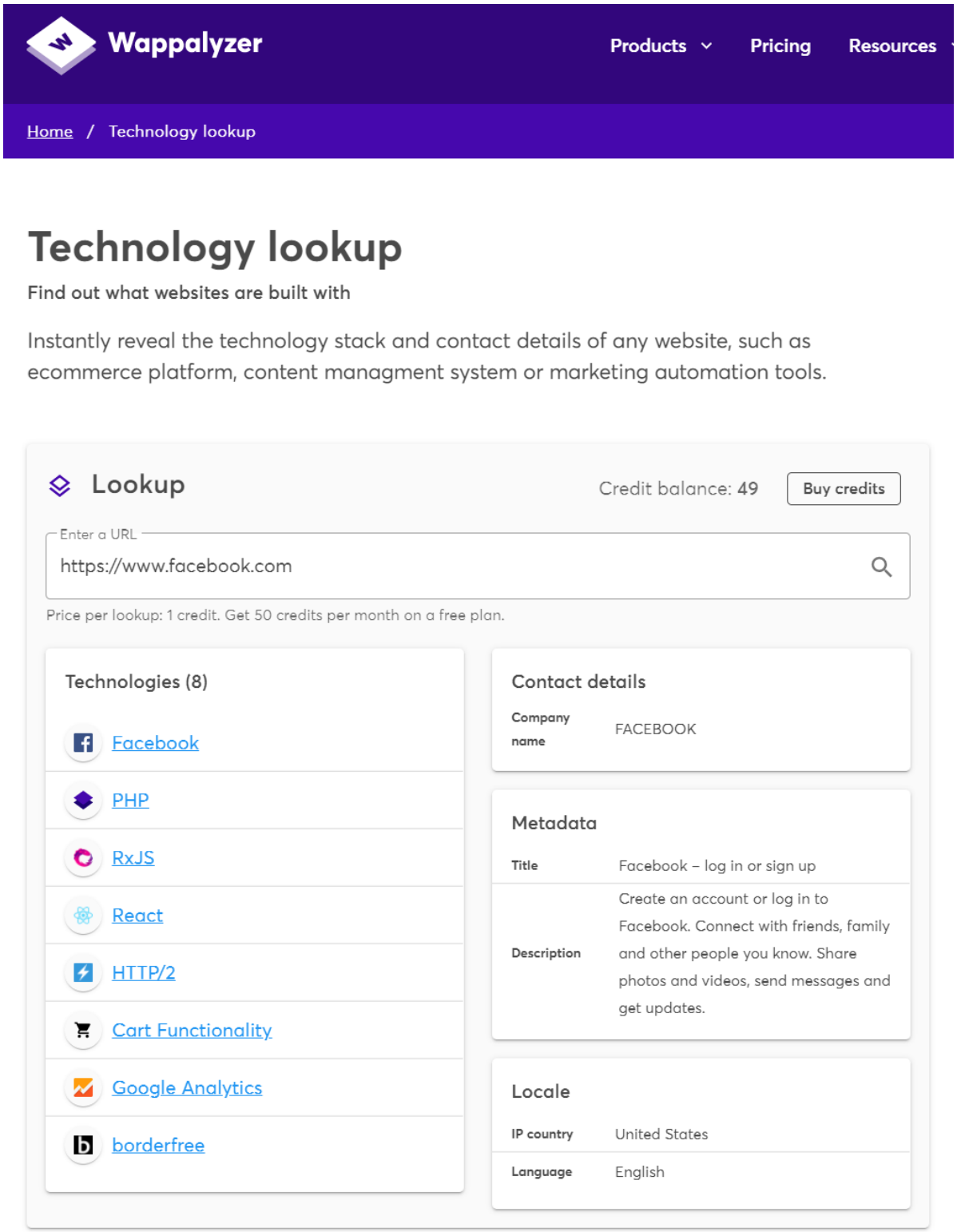


Fig. 7 - Risultato della ricerca effettuata su www.wappanalyzer.com

Per reperire le informazioni concernenti la **Connettività** e la postazione **Client** è sufficiente eseguire interrogare il sito:

- **IP Analyzer** (https://ipalyzer.com/) (inserendo il proprio indirizzo ip visibile in homepage)

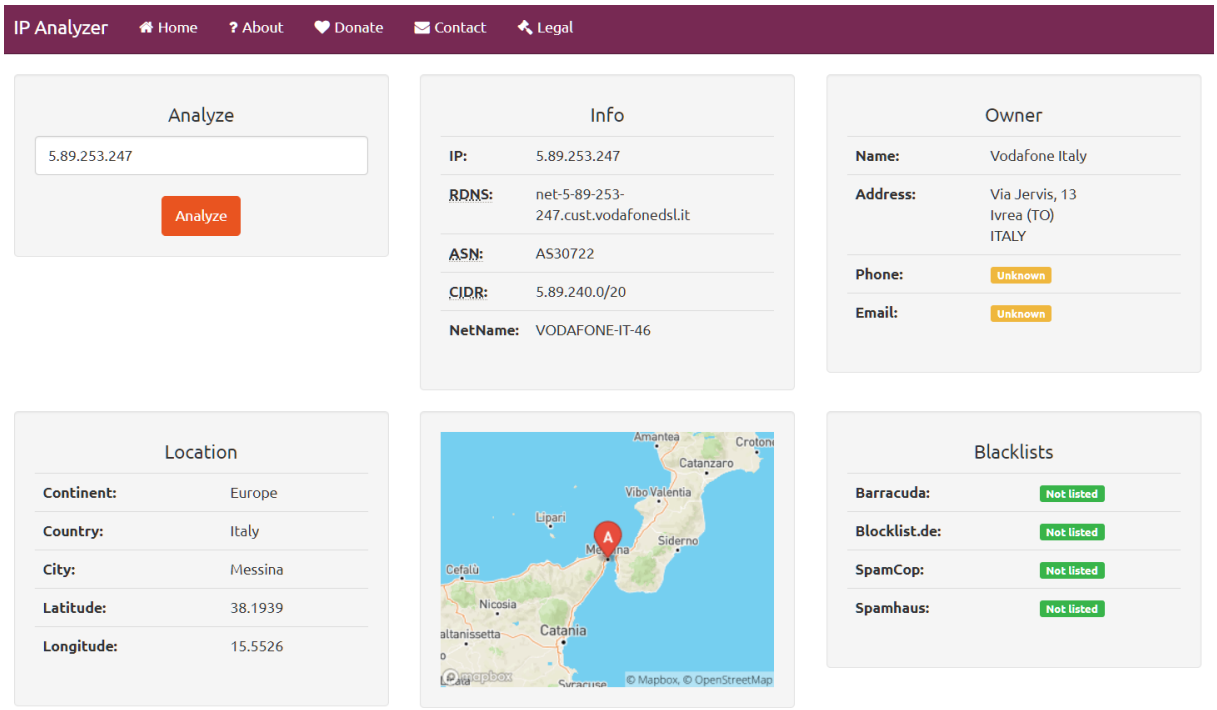


Fig. 8 – Risultato della ricerca effettuata su www.ipalyzer.com

ed eseguire il comando "**ipconfig /all**" dal prompt di Windows per ricavare le informazioni sulla configurazione di rete (indirizzo ip della postazione, router, dns server, proxy server).

```
C:\Users\mw>ipconfig /all

Configurazione IP di Windows

   Nome host . . . . . . . . . . . . . . : idea-PC
   Suffisso DNS primario . . . . . . . . :
   Tipo nodo . . . . . . . . . . . . . . : Ibrido
   Routing IP abilitato. . . . . . . . . : No
   Proxy WINS abilitato . . . . . . . . . : No
   Elenco di ricerca suffissi DNS. . . . : station

Scheda LAN wireless Wi-Fi:

   Suffisso DNS specifico per connessione: station
   Descrizione . . . . . . . . . . . . . : Realtek RTL8188EU Wireless LAN 802.11n USB 2.0 Network Adapter
   Indirizzo fisico. . . . . . . . . . . : F8-1A-67-19-F2-CB
   DHCP abilitato. . . . . . . . . . . . : Sì
   Configurazione automatica abilitata   : Sì
   Indirizzo IPv4. . . . . . . . . . . . : 172.16.1.147(Preferenziale)
   Subnet mask . . . . . . . . . . . . . : 255.255.255.0
   Lease ottenuto. . . . . . . . . . . . : domenica 18 ottobre 2020 09.55.27
   Scadenza lease . . . . . . . . . . .  : domenica 18 ottobre 2020 18.42.09
   Gateway predefinito . . . . . . . . . : 172.16.1.1
   Server DHCP . . . . . . . . . . . . . : 172.16.1.1
   Server DNS . . . . . . . . . . . . .  : 192.168.1.1
                                           172.16.1.1
   NetBIOS su TCP/IP . . . . . . . . . . : Attivato
```

Fig. 9 - Risultato del comando ipconfig

Successivamente, è necessario descrivere, attraverso un "*investigation planning*", il percorso che permette di raggiungere le informazioni di interesse (accesso diretto o interattivo[26]), lo stato della fonte (aperta o protetta da credenziali), inventariare le evidenze con un codice identificativo (cd. "*ID*") e la presenza di contenuti digitali da acquisire separatamente (per esempio: file, documenti, immagini, audio, video).

Di seguito è proposto un template di Investigation Planning in cui riportare tutte le informazioni utili ad identificare le evidenze di interesse e indicare le notizie utili durante la fase di acquisizione.

[26] Accesso diretto si utilizza quando è possibile richiamare una risorsa web direttamente dal suo indirizzo URI (p.e. https://www.facebook.com/photo/?fbid=1367613786767681), mentre Accesso Interattivo identifica un percorso di ricerca che inizia da un URI e, per poter proseguire, necessita dell'intervento dell'utente, come la selezione di un'opzione o l'inserimento di keyword, che non può essere automatizzato.

INVESTIGATION PLANNING

IDENTIFICATIVO CASO:		**COMMITTENTE:**	
DATA E ORA:		**COMPILATORE:**	
DESCRIZIONE:			

Caratteristiche del Target

FONTE APERTA indicare [SI]/[NO]	**SI** / **NO**	---> **indicare le modalità e le credenziali di accesso**	
ACCESSO DIRETTO: indicare l'url iniziale			
ACCESSO INTERATTIVO: indicare le keys utilizzate per raggiungere l'evidenza			

Storyboard

ID		EVIDENZA			
1	**Descrizione**				
	Autore		**Data e ora pubbl.**		
	URI da acquisire				
	FILE da acquisire				
	Note			**Acquisita**	
2	**Descrizione**				
	Autore		**Data e ora pubbl.**		
	URI da acquisire				
	FILE da acquisire				
	Note			**Acquisita**	
3	**Descrizione**				
	Autore		**Data e ora pubbl.**		
	URI da acquisire				
	FILE da acquisire				
	Note			**Acquisita**	
4	**Descrizione**				
	Autore		**Data e ora pubbl.**		
	URI da acquisire				
	FILE da acquisire				
	Note			**Acquisita**	
5	**Descrizione**				
	Autore		**Data e ora pubbl.**		
	URI da acquisire				
	FILE da acquisire				
	Note			**Acquisita**	

Tab. 2 – Investigation Planning.

In sintesi, l'obiettivo di questa fase è la ricerca, il riconoscimento e la documentazione delle potenziali fonti di prova digitali che saranno oggetto delle fasi successive.

3.2 Raccolta

La fase di raccolta (o sequestro) è un'attività posta in essere quando è necessario rimuovere o spostare la fonte di prova dal luogo di origine e, solitamente, viene disposta dall'Autorità Giudiziaria o da chi ne ha competenza. Nella fattispecie di indagine che stiamo analizzando, ovvero le investigazioni a distanza, questa operazione non può essere realizzata fisicamente, ma, se necessario, può essere portata a termine in uno dei seguenti modi:

- Se la risorsa è pubblica: si ordina all'Internet Service Provider di metterla off-line;
- Se la risorsa è protetta: si acquisiscono tutte le credenziali di accesso (dal proprietario o dall'ISP) e si modificano o disabilitano per renderla inaccessibile agli altri.

Come è facilmente deducibile, non si tratta di un sequestro definitivo, ma di un impedimento temporaneo che consente di posticipare le ulteriori attività o di effettuare le opportune valutazioni.

3.3 Acquisizione

L'acquisizione rappresenta il processo di creazione di una copia di un potenziale elemento di prova digitale e la stesura della documentazione riguardante i metodi utilizzati e le attività effettuate a tale scopo. In particolar modo, la documentazione prodotta dovrà permettere a chiunque di riprodurre e verificare tutto il processo di acquisizione.

Per realizzare una copia forense a distanza dobbiamo trasferire il dato digitale dalla sua origine, solitamente un server, alla postazione dell'operatore su cui si sta realizzando la duplicazione.

Questa operazione è facilmente attuabile perché ricalca, sostanzialmente, le azioni eseguite durante la consultazione della stessa fonte di prova. In altre parole, si effettua un'interrogazione delle stesse risorse web, richiamandole tramite la corrispondete URI[27], e si trasferiscono sulla postazione dell'operatore forense, per essere registrate su un'altra memoria di massa.

[27] Uniform Resource Identifier (in acronimo URI) è una sequenza di caratteri che identifica universalmente ed univocamente una risorsa, nel caso specifico l'indirizzo web. (p.e. http://www.sitoweb.it/pagina.html)

L’operatore incaricato di effettuare un’acquisizione di fonti prova online deve preliminarmente effettuare una serie di scelte tra le seguenti opzioni:

1. La modalità di acquisizione: automatica o interattiva;
2. Il luogo da cui effettuare l’acquisizione: hosted o client;
3. Gli strumenti e i comandi.

Cerchiamo di fornire gli elementi utili che consentono di selezionare la strategia migliore.

L’attività di acquisizione può essere eseguita in due modalità:

- **Automatica**, tramite un crawler[28]. In questo caso l’operatore indica un indirizzo URI al software selezionato (crawler) e quest’ultimo inizia a scaricare sequenzialmente e autonomamente tutte le risorse ad esso collegate individuabili dai “link” contenuti nelle stesse fonti di prova;
- **Interattiva**, tramite un browser[29]. In questa ipotesi l’operatore individua il percorso di interrogazione, tramite un apposito programma (browser), e seleziona le risorse da scaricare.

Negli ultimi anni la prassi delle acquisizioni a distanza è orientata verso il modello interattivo perché, sempre più spesso, i contenuti web non sono direttamente e facilmente identificabili a priori oppure sono connotati da un rapido dinamismo (basti pensare alle piattaforme social network) che non consente di rendere automatica l’acquisizione.

La produzione in giudizio dei singoli file che compongono una risorsa web (file HTML, fogli di stile CSS, contenuti multimediali, script, ecc.) forniscono certamente elementi ulteriori, quali ad esempio gli indirizzi da cui giungono oggetti esterni, ma non sono ancora sufficienti a dimostrare la genuinità del dato in quanto non vi è la dimostrazione che i file messi a disposizione siano stati ottenuti a seguito di una interrogazione sul World Wide Web, ne vi è

---

[28] Il crawler è un software che analizza i contenuti di una rete in un modo metodico e automatizzato, in genere per conto di un motore di ricerca. Nello specifico, un crawler è un tipo di bot (programma o script che automatizza delle operazioni), che solitamente acquisisce una copia testuale di tutti i documenti presenti in una o più pagine web creando un indice che ne permetta, successivamente, la ricerca e la visualizzazione. Durante l'analisi di una URL, identifica tutti i collegamenti ipertestuali presenti nel documento e li aggiunge alla lista di URL da visitare. Il processo può essere concluso manualmente o dopo che un determinato numero di collegamenti è stato seguito.

[29] Il browser è un'applicazione per l'acquisizione, la presentazione e la navigazione di risorse sul web. Il programma implementa da un lato le funzionalità di client per il protocollo HTTP, che regola lo scaricamento delle risorse dai server web a partire dal loro indirizzo URL; dall'altro quelle di visualizzazione dei contenuti ipertestuali (solitamente all'interno di documenti HTML) e di riproduzione di contenuti multimediali (rendering).

l'indicazione e la prova di quali siano i sistemi informatici remoti coinvolti nel processo di costruzione della pagina su cui vi sono i dati informatici di interesse, ovvero gli indirizzi Internet Protocol dei singoli server web da cui sono stati scaricati i file HTML, i fogli di stile, i contenuti multimediali, ecc.

Per rendere *forensically sound* un'acquisizione a distanza non basta quindi utilizzare solo un normale crawler o browser, ma è necessario catturare e registrare anche le seguenti informazioni:

1. **I contenuti digitali** richiesti e visualizzati sulla postazione forense per rendere l'acquisizione completa (codice html, documenti, file multimediali, certificati, script, ecc.);
2. **Il traffico di rete**, ovvero le richieste inviate dalla postazione client e le risposte ricevute dai server interrogati, per assicurare la conformità dei dati acquisiti a quelli originali e la loro verificabilità;
3. **I comandi impiegati** per realizzare l'intero processo di acquisizione, attraverso la registrazione del contenuto visualizzato a video, per garantire l'autenticità delle fonti di prova e la riproducibilità e ripetibilità del processo posto in essere.

Per quanto riguarda il sito da cui realizzare l'acquisizione, l'operatore può scegliere due alternative:

- **Hosted**: scegliendo questa opzione l'acquisizione è effettuata tramite un servizio web (in hosting o in cloud) che mette a disposizione dell'operatore una console da cui è possibile interrogare le risorse in rete e, terminata l'operazione, realizza una registrazione dell'intera sessione di navigazione, comprensiva dei contenuti web, del traffico di rete e del video-capture, che può essere successivamente scaricata per ottenere la copia in locale. Questa ipotesi è impiegata nel caso in cui non si ha a disposizione una postazione forense, in quanto, per realizzarla è sufficiente una postazione connessa alla rete internet, ed è preferita da chi non ha una conoscenza approfondita dell'information and communication technology;
- **Client**: scegliendo questa alternativa si realizza la copia direttamente sulla postazione dell'operatore opportunatamente configurata. In questo caso l'operatore è in grado di scegliere quali strumenti utilizzare ed ha il controllo completo del flusso di informazioni richieste ed acquisite. Questa ipotesi è scelta da coloro i quali hanno dimestichezza con gli strumenti dell'information and communication technology ed effettuano regolarmente

questo tipo di acquisizioni. Esiste la variante del Client virtuale**:** questa configurazione, molto simile alla precedente, si differenzia solo per la configurazione della postazione. Infatti, in questo caso la postazione dell'operatore è una macchina virtuale (eventualmente anche in cloud). Abitualmente, chi sfrutta questa modalità, utilizza una postazione bianca, cioè mai utilizzata prima, e, al termine dell'acquisizione, la macchina virtuale è aggiunta all'elenco di evidenze acquisite per rinforzare ulteriormente la verificabilità, la riproducibilità e la ripetibilità delle operazioni svolte. Ciò è riscontrabile generando la timeline delle operazioni del client virtuale.

Vediamo quali sono i passi che è opportuno seguire per ottenere le informazioni predette e, procedendo in maniera metodica, acquisire a distanza il maggior numero di elementi necessari per andare a costruire un quadro il più completo possibile:

A. Avviare la registrazione dell'output dello schermo,
B. Verificare la configurazione di rete e la sincronizzazione dell'orologio,
C. Cominciare a captare il traffico di rete e le chiavi di cifratura TLS,
D. Richiamare e memorizzare tutte le risorse web d'interesse,
E. Al termine, interrompere e memorizzare la captazione del traffico di rete e dei certificati,
F. Terminare e salvare la registrazione dell'output dello schermo.

Nell'esempio che si propone in questo testo si è optato per la soluzione interattiva e client. In particolare, è stato prescelto di impiegare una postazione in cui sono installati i seguenti software[30]:

- **OBS Studio** v29.1.3 (https://www.obsproject.com) per registrare la sessione di acquisizione;
- **Wireshark** v4.0.7 (https://www.wireshark.org) per catturare il traffico di rete;
- **Google Chrome** v115.0 (https://www.chromium.org) per acquisire i contenuti web.

Dopo aver recuperato le suddette applicazioni, dai rispettivi portali web, e averle installate con le loro configurazioni di default, procediamo a sviluppare le sei operazioni con un esempio.

[30] Esistono decine di applicazioni (open source, free e commerciali) in grado di fornire il risultato richiesto. La citata selezione dei software è stata orientata per coniugare tre caratteristiche: la qualità del risultato finale, la semplicità d'uso e la circostanza che fosse disponibile una versione compatibile con i principali sistemi operativi: Windows, MacOS e Linux.

A. Avviare la registrazione dell'output dello schermo.

Come prima attività si avvia la registrazione dell'output dello schermo, tramite il programma OBS Studio, per ottenere l'intera sessione di acquisizione da cui, successivamente, sarà possibile ricostruire la sequenza dei comandi utilizzati e dei relativi risultati ottenuti.

La prima volta che si esegue il programma OBS Studio è necessario configurare almeno una fonte di origine che, nel nostro caso, è lo schermo della postazione su cui stiamo operando. Pertanto, si seleziona l'icona **[+]** del Pannello **[Fonti]** e si aggiunge l'opzione **[Cattura lo schermo]** (nel caso in cui vi fosse più di uno schermo, selezionare quello che sarà utilizzato per la navigazione web) e, infine, si inizia la registrazione selezionando **[Avvia la Registrazione]**.

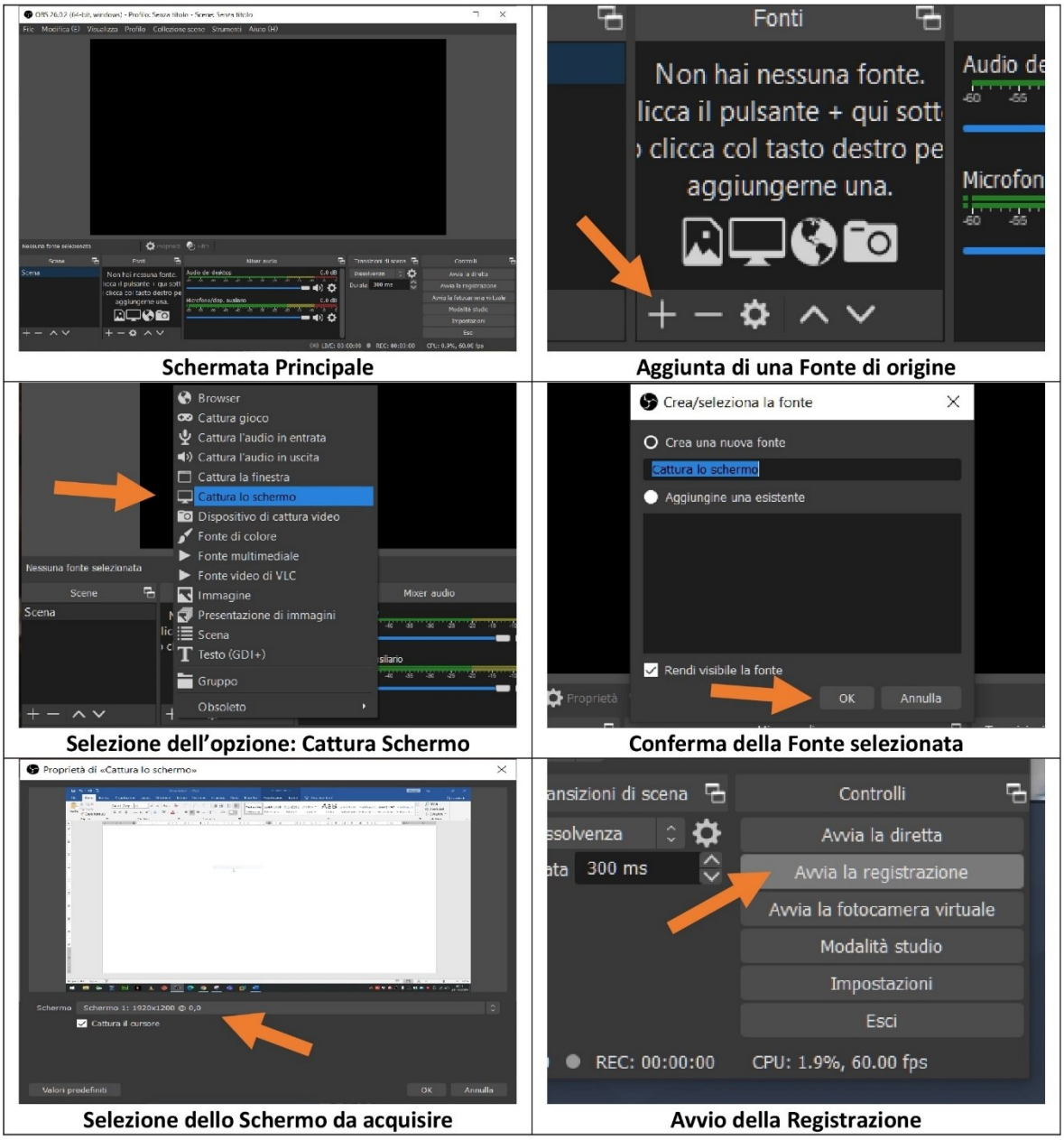


Fig. 10 - OBS Studio: configurazione e avvio.

B. Verificare la configurazione di rete e la sincronizzazione dell'orologio della postazione.

Il secondo step ci consente di interrogare e verificare la configurazione di rete della nostra

postazione[31], la raggiungibilità del target e la sincronizzazione dell'orologio di sistema[32]. Per realizzarla è sufficiente eseguire alcuni comandi, da prompt di sistema, come quelli indicati in figura.

```
C:\>echo %date% %time%

21/10/2020 23.04.31,71

C:\>ipconfig /all

Configurazione IP di Windows
   Nome host . . . . . . . . . . . . . . : PC
   Suffisso DNS primario . . . . . . . . :
   Tipo nodo . . . . . . . . . . . . . . : Ibrido
   Routing IP abilitato. . . . . . . . . : No
   Proxy WINS abilitato . . . . . . . . . : No
   Elenco di ricerca suffissi DNS. . . . : station
Scheda LAN wireless Wi-Fi:
   Suffisso DNS specifico per connessione: station
   Descrizione . . . . . . . . . . . . . : Realtek RTL8188EU Wireless LAN 802.11n Network Adapter
   Indirizzo fisico. . . . . . . . . . . : F8-1A-67-19-F2-CB
   DHCP abilitato. . . . . . . . . . . . : Sì
   Configurazione automatica abilitata   : Sì
   Indirizzo IPv4. . . . . . . . . . . . : 172.16.1.147(Preferenziale)
   Subnet mask . . . . . . . . . . . . . : 255.255.255.0
   Lease ottenuto. . . . . . . . . . . . : mercoledì 21 ottobre 2020 14.22.56
   Scadenza lease . . . . . . . . . . .  : mercoledì 21 ottobre 2020 23.52.54
   Gateway predefinito . . . . . . . . . : 172.16.1.1
   Server DHCP . . . . . . . . . . . . . : 172.16.1.1
   Server DNS . . . . . . . . . . . . .  : 8.8.8.8
                                           8.8.4.4
   NetBIOS su TCP/IP . . . . . . . . . . : Attivato

C:\>tracert -d facebook.com

Traccia instradamento verso facebook.com [185.60.216.35]
su un massimo di 30 punti di passaggio:

  1     2 ms     2 ms     3 ms  172.16.1.1
  2     5 ms     4 ms     3 ms  192.168.1.1
  3    22 ms    22 ms    22 ms  5.89.252.1
  4    33 ms    32 ms    33 ms  83.224.40.161
  5    32 ms    32 ms    32 ms  83.224.40.160
  6    34 ms    34 ms    33 ms  195.89.99.134
  7    42 ms    41 ms    41 ms  195.2.31.54
  8    65 ms    68 ms    55 ms  195.2.16.105
  9    53 ms    52 ms    52 ms  157.240.69.152
 10    99 ms    52 ms    52 ms  157.240.47.212
 11    53 ms    52 ms    51 ms  157.240.43.19
 12    50 ms    50 ms    49 ms  173.252.67.189
 13    56 ms    52 ms    51 ms  185.60.216.35

Traccia completata.
```

Fig. 11 – Verifica della configurazione della postazione.

[31] Per operare con una configurazione della connessione alla rete trasparente si consiglia di:
- impostare DNS server pubblici (p.e. Cloudflare DNS 1.1.1.1 oppure Google Public DNS 8.8.8.8),
- sincronizzare l'orologio di sistema con un NTP server pubblico (p.e. INRiM 193.204.114.105)
- non utilizzare server proxy per la navigazione in Internet.

[32] Le informazioni ricavate in questa fase sono utili a dimostrare l'autenticità della connessione alla rete Internet e della postazione e, pertanto, possono essere integrate con ulteriori che l'operatore ritiene opportuno per rinforzare la prova.

È fortemente consigliato identificare tutti i nodi tra il target e il client utilizzando il comando:

> **tracert -d** ***[nome_target]*** (p.e. www.google.com)

Gli operatori più paranoici possono aggiungere ulteriori artefatti che conferiscono attendibilità anche agli altri e quindi all'acquisizione stessa. Per esempio possono memorizzare l'intero stato della postazione forense (la memoria, i processi, le connessioni di rete, i file di registro, i file di logs, ecc.) prima e dopo l'acquisizione; oppure utilizzare direttamente una macchina virtuale che, al termine delle operazioni, aggiungono all'elenco delle evidenze da conservare e che risulterà coerente, ad un'eventuale analisi, con gli altri artefatti acquisiti.

C. Cominciare a captare il traffico di rete e le chiavi di cifratura TLS.

La terza operazione è diretta alla captazione di tutto il traffico di rete, entrante e uscente dalla postazione, generato dall'operatore durante l'interrogazione delle fonti di prova (target).

Le informazioni memorizzate consentono, ad un livello più tecnico, di ricostruire l'intera sessione, composta da richieste e risposte, e rendere verificabile l'intero processo.

Poiché la maggior dei servizi internet utilizza protocolli di trasmissione che adoperano la cifratura TLS, il traffico di rete generato risulta cifrato e incomprensibile. Per rendere intelligibile, e quindi verificabile, questi contenuti è necessario catturare, oltre al traffico di rete, anche le chiavi di sessione generate dal client e scambiate con il server durante la navigazione in modo tale che possano essere utilizzate per decifrare il traffico di rete captato[33].

Un metodo per memorizzare le chiavi di sessione sui sistemi operativi Windows consiste nell'impostare una variabile di ambiente denominata: **SSLKEYLOGFILE=C:\case\keylogfile.txt** utilizzando l'utility **[Impostazioni di sistema avanzate]** come visualizzato in figura.

[33] Poiché la maggior dei servizi internet utilizza protocolli di trasmissione che adoperano la cifratura TLS, il traffico di rete generato risulta cifrato e incomprensibile. Per rendere in chiaro, e quindi verificabile, questa tipologia di contenuti è necessario catturare, oltre al traffico di rete, anche le chiavi di sessione scambiate tra il server e il client e utilizzarle per decifrare il traffico di rete captato durante la navigazione. Per apprendere le modalità di estrazione delle chiavi per la decrittazione del traffico di rete, si rimanda a questa breve guida: https://gitlab.com/wireshark/wireshark/-/wikis/TLS

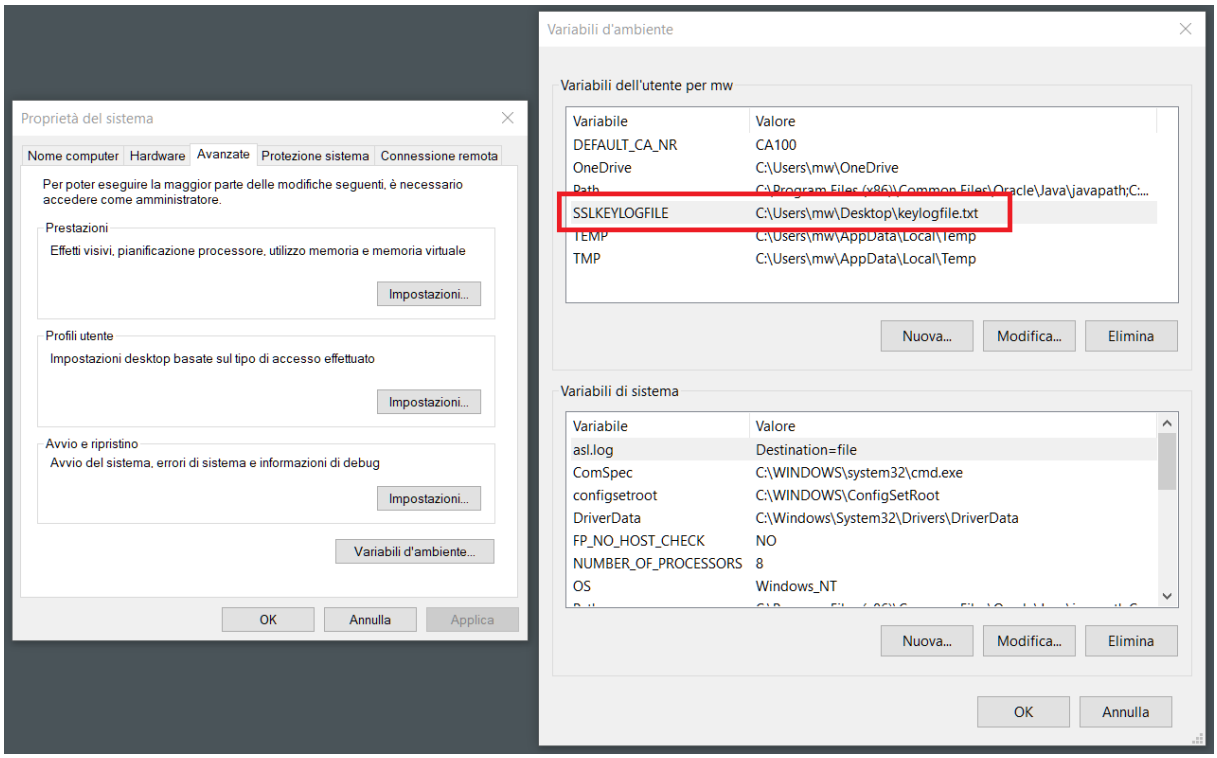


Fig. 12 - Impostare la variabile di ambiente SSLKEYLOGFILE

Per avviare la registrazione del traffico di rete, si avvia il programma Wireshark, si seleziona la scheda di rete che collega la postazione alla rete Internet e si **[Avvia la cattura dei pacchetti] (icona Blu) o [CTRL+E]** come indicato in figura.

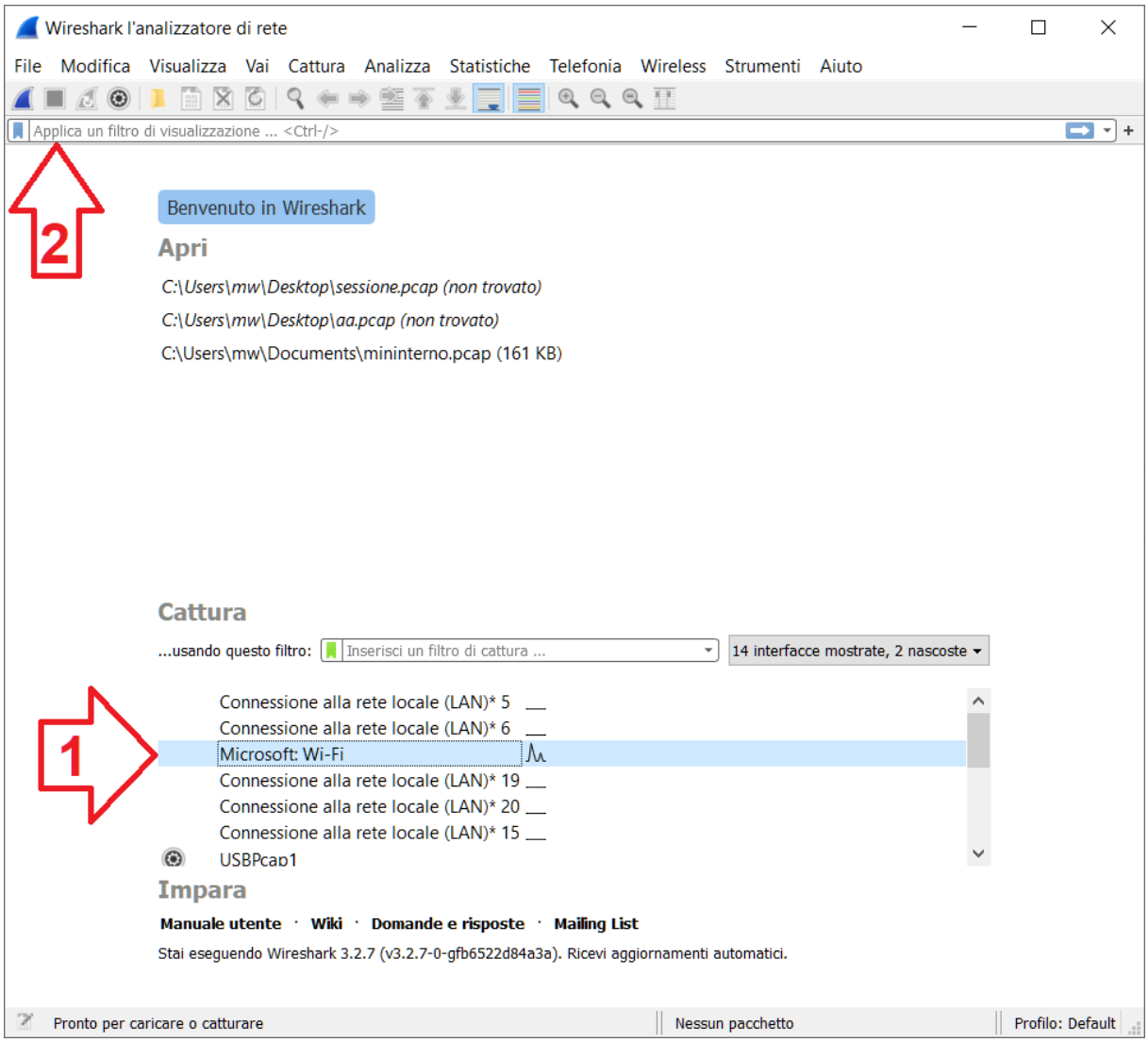


Fig. 13 - Wireshark: configurazione e avvio.

D. Richiamare e memorizzare tutte le risorse web d'interesse.

La quarta attiva permette all'operatore di richiamare le fonti di prova, precedentemente identificate, e trasferirle sulla memoria del dispositivo client.

Per realizzare la copia di un contenuto web con il browser Google Chrome è sufficiente richiamare la pagina e selezionare dal menu **[Altri strumenti: Salva pagina con nome]** o premere **CTRL+S.**

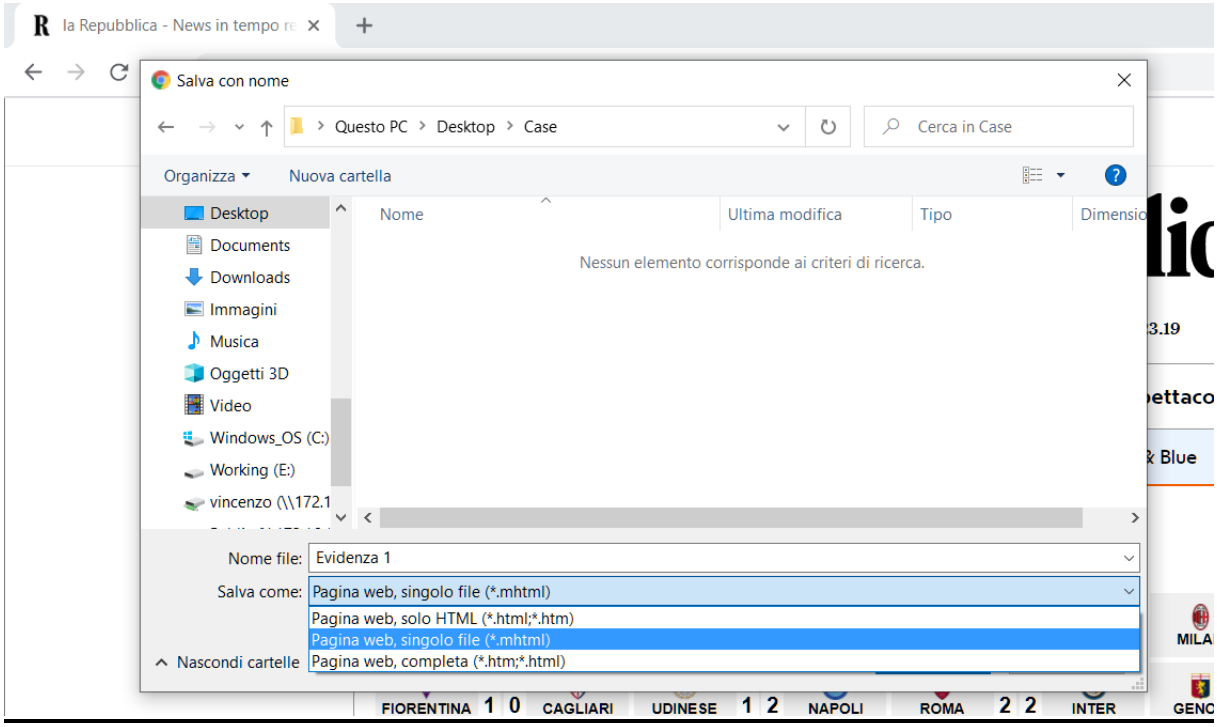


Fig. 14 – Come salvare un pagina web

È opportuno nominare le pagine con lo stesso numero **ID** utilizzato nell'*Investigation Planning*. Questa operazione deve necessariamente essere ripetuta ad ogni nuova interrogazione.

Per quanto riguarda la scelta del formato di memorizzazione è stato preferito MHTML (MIME encapsulation of aggregate HTML documents) perché è molto semplice da utilizzare. Si tratta di un formato di archiviazione di pagine web aperto, distribuito come RFC 2557[34], e utilizzato per combinare in un unico file il codice HTML e tutte le risorse complementari (come le immagini, le animazioni Flash, le Java applet, i file audio e video, e gli script) rappresentate da collegamenti ipertestuali esterne al codice HTML della pagina web d'origine richiamata. L'acquisizione in formato MHTML è gestita da Google Chrome, e da tutti i browser Chromium-based, attraverso il motore Chrome Blink[35]. L'intestazione di un file MHTML così generato contiene alcuni metadati che possono essere utilizzati durante la validazione del risultato:

```
From: <Saved by Blink>
Snapshot-Content-Location: https://www.facebook.com
```

[34] Request for Comments: 2557 - MIME Encapsulation of Aggregate Documents, such as HTML (MHTML) (https://tools.ietf.org/html/rfc2557).
[35] The Chromium Projects - Blink (Rendering Engine) (https://www.chromium.org/blink).

```
    Subject: Facebook - Log In or Sign Up
    Date: Mon, 11 Gen 2021 15:47:07 -0000
    MIME-Version: 1.0
    Content-Type: multipart/related;
        type="text/html";
        boundary="-MultipartBoundary-
wqL3OhPd46E2L20Gy6hFTMUyH5DxHzbEkglKVzKx24-"
```

Il campo [Date] rappresenta il timestamp in formato UTC del momento in cui Chrome memorizza la pagina web.

È possibile utilizzare anche altri formati di archiviazione, come il formato WARC (Web Archive file format) definito nello standard ISO 28500:2017[36], che richiedono plug-in o software specifici[37] da installare sulla postazione forense. Il formato WARC ha il vantaggio di incorporare nello stessa file sia la richiesta che la risposta in formato HTML. Anche se esistono pochi tools specifici per l'acquisizione in questo formato, è quello utilizzato dalle principali Biblioteche Digitali.

Spesso è necessario catturare singolarmente i contenuti digitali collegati (tramite URL) o inseriti all'interno della pagina web visualizzata per effettuare successivamente un'analisi più accurata.

Si riportano alcuni esempi:

- *memorizzare un'immagine visualizzata in una pagina web*: posizionarsi sull'immagine d'interesse, premere il tasto destro del mouse, selezionare **[Salva immagine con come]** e memorizzarla in una directory riconducibile tramite numero ID alla pagina di origine;
- *memorizzare un file collegato ad una pagina web*: posizionarsi sul collegamento (link) d'interesse, premere il tasto destro del mouse, selezionare **[Salva link con come]** e memorizzarlo in una directory riconducibile tramite numero ID alla pagina di origine;
- *memorizzare un video da un social media:* i video ospitati su siti Web sono generalmente forniti all'utente finale in formato MP4 o WebM. Ciò si realizza tramite il codice embedded che incorpora il contenuto del video nell'interfaccia visibile all'utente

[36] ISO 28500:2017 Information and documentation — WARC file format (https://www.iso.org/standard/68004.html).
[37] Per un approfondimento sui tools che supportano il formato WARC si consiglia di consultare il progetto "Webrecorder" (https://webrecorder.net).

e, solitamente, non consente il salvataggio diretto tramite il tasto destro del mouse. Tuttavia, il fatto che il contenuto venga riprodotto significa che esso deve essere referenziato da una fonte d'origine, di solito tramite una rete di distribuzione dei contenuti (CDN).

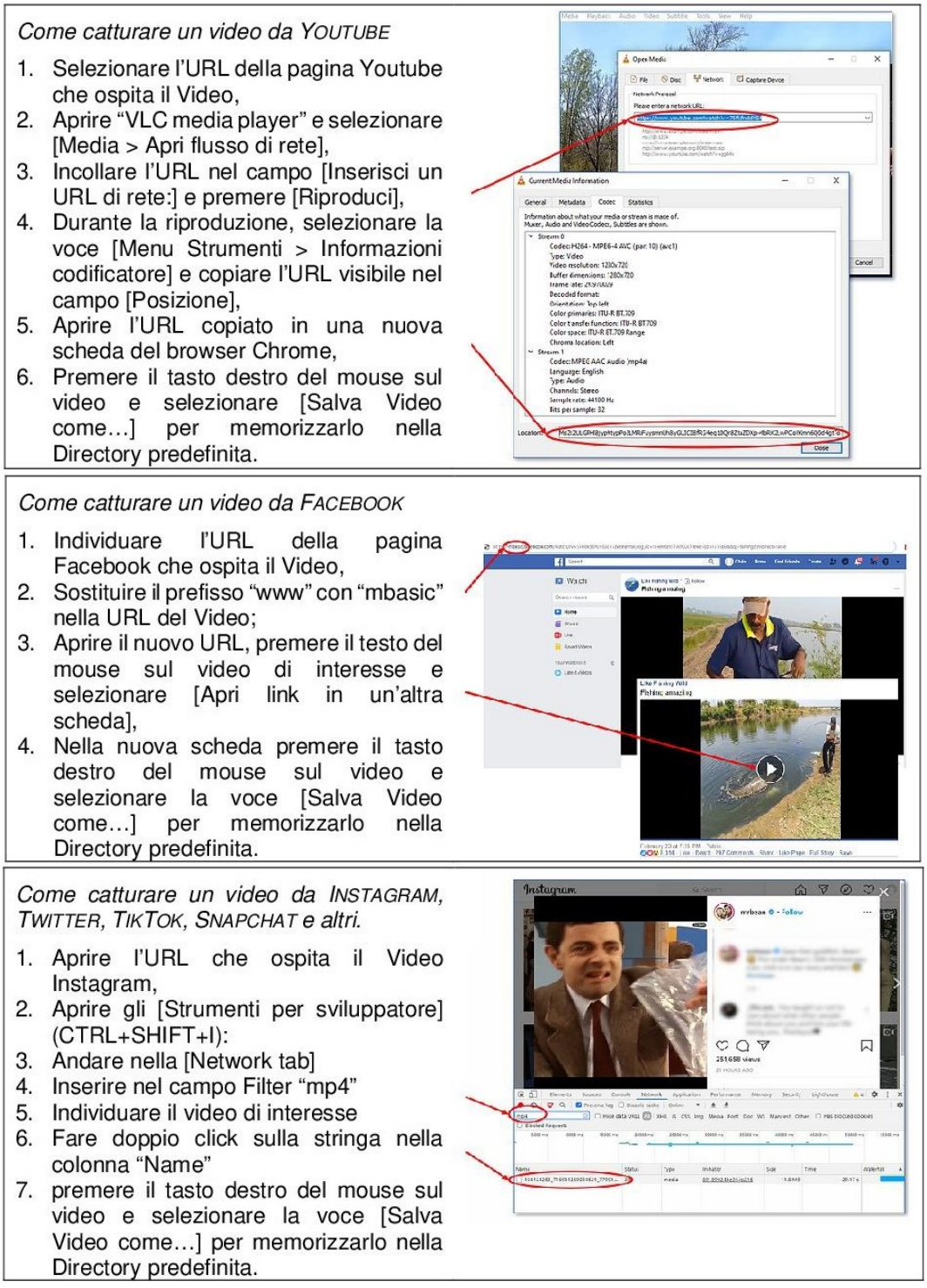


Fig. 15 - Esempi di memorizzazione video dalle Piattaforme di Social Network.

Spesso, in presenza di profili di Social Network (Facebook, Instagram, Twitter o Linkedin), è richiesto di acquisire l'intero profilo utente. Questa funzionalità, grazie all'entrata in vigore del GDPR, è disponibile sulle principali piattaforme Social e consente di realizzare un'esportazione completa dei dati utente. Questa opzione può essere sfruttata se si conoscono le credenziali dell'utente e viene gestita dall'operatore con le stesse procedure di una normale acquisizione da remoto.

L'acquisizione può riguardare anche informazioni cancellate o rimosse. Per tentare di effettuare il recupero di tali informazioni occorre spostare il target di acquisizione:

- Google Cache,
- Wayback Machine.

Google Cache (Google.com) è una funzione del noto motore di ricerca che consente di memorizzare il contenuto di una determinata pagina in una memoria cache. La copia di ciascuna pagina viene immagazzinata da Google al fine di ridurre le richieste da inoltrare al server e alla Main Memory. Una memoria del genere consente all'utente di recuperare facilmente ogni pagina e a Google di elaborare al meglio le pagine visitate. Questa opzione consente nel breve periodo, ovvero prima che il motore di ricerca non visiti il sito web, di recuperare la versione precedente di una determina risorsa rimossa o modificata.

Per visionare la copia cache di Google, è possibile mettere in pratica tre tecniche differenti:

- In primo luogo, si può cliccare sulla freccia verso il basso dell'URL per visionare la SERP di Google. Dopo aver fatto clic sulla relativa opzione per copiare la cache, la pagina memorizzata si apre in automatico. L'indirizzo risulta diverso rispetto all'URL della pagina perché la cache visualizzata si trova sul server di Google.
- Il secondo metodo riguarda la possibilità di utilizzare l'operatore "cache:", seguito dall'URL della pagina desiderata. (p.e. scrivere su Google "cache: www.repubblica.it")
- Il terzo sistema, invece, prevede il download di un plugin che consente di visualizzare la cache e la storia di una determinata pagina. Sui vari browser Web, esistono diverse estensioni che possono assolvere tale compito.

Wayback Machine (Archive.org) è un progetto universale per la creazione di una biblioteca digitale dei contenuti reperibili online. Il progetto, avviato nel 1996, contiene miliardi di pagine web e di altri contenuti digitali. (negli anni successivi sono stati avviati diversi progetti con finalità e tecnologie simili tra i quali si segnala quello europeo raggiungibile all'url:

Archive.eu). Il vantaggio di questa tipologia di archivi è quello di memorizzare più versione della stessa risorsa in istanti diversi. Per cui è possibile sfruttarlo per effettuare la ricerca in periodi anche distanti dal presente. L'archivio può essere alimentato in due modalità: automaticamente, ovvero il crawel del sistema acquisisce periodicamente nuovi contenuti oppure una nuova versione dei contenuti già indicizzati; manualmente o on-demand, chiunque può richiedere al portale di indicizzare una risorsa e creare una "fotografia" di quel contenuto ad un determinato istante (anche in maniera non pubblica).

Queste funzionalità, in ambito forense, consentono di ottenere due benefici:

- Ricavare informazioni non più visibili, rimosse o cancellate;
- Creare una copia dei contenuti.

Quest'ultima opzione, attivabile anche in area riservata dagli utenti registrati, è particolarmente utile nel caso in cui l'operatore non può procedere all'acquisizione con altri strumenti.

L'Internet Archive è stato ampiamente sfruttato nelle aule di Tribunale in quanto è universalmente riconosciuto come una fonte attendibile di copie di pagine o siti web basato sull'autorevolezza accademica e giuridica e la terzietà che hanno acquisito con il tempo l'ente e il sistema stesso.

L'utilizzo dei due sistemi di ricerca proposti presuppone la conoscenza dell'URI di partenza, oppure l'impiego degli operatori logici messi a disposizione dai motori di ricerca.

E. Al termine, interrompere e memorizzare la captazione del traffico di rete e dei certificati.

Dopo aver terminato l'acquisizione di tutte le fonti di prova, è necessario interrompere le attività precedentemente avviate. Per cui, dapprima si chiude il browser, poi si passa all'applicazione Wireshark, si **[Ferma la cattura dei pacchetti] (icona rossa) o [CTRL+E]** e si memorizza il traffico catturato **[CTRL+S]** assegnandogli un nome significativo (p.e. "NumeroCaso_data"). Per la captazione dei certificati è sufficiente eliminare la variabile di ambiente **SSLKEYLOGFILE=C:\case\keylogfile.txt** e salvare il file prodotto nella directory del caso.

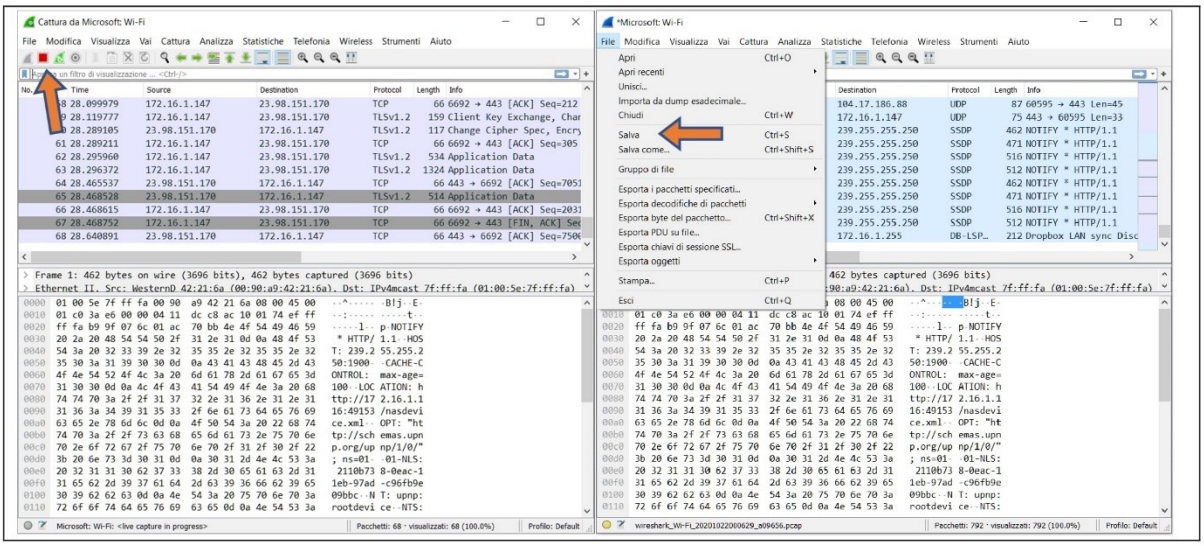


Fig. 16 – Come interrompere Wireshark e memorizzare il traffico captato.

F. Terminare e salvare la registrazione dell'output dello schermo.

Ugualmente, è necessario terminare la registrazione dell'output dello schermo. Per realizzare quest'ultima operazione di acquisizione è sufficiente passare all'applicazione OBS Studio e selezionare la voce **[Termina la registrazione]** dal pannello **[Controlli]**. Il file video prodotto è solitamente memorizzato nella directory utente "Video" e nominato con una stringa che indica il giorno e l'ora di avvio della registrazione. Per cui, ci si posiziona nella predetta directory, si seleziona il file appena creato e lo si sposta all'interno della directory del caso.

Di seguito si propone uno schema di directory per la memorizzazione delle evidenze raccolte:

Fig. 17 – Sistema di Directory.

3.4 Conservazione

Uno dei requisiti fondamentali nel trattamento delle fonti di prova digitale, stabilito anche dall'ordinamento europeo ed italiano, prevede che tutte le attività probatorie siano disposte attraverso tecniche idonee ad assicurare la conservazione dei dati originali ed impedirne l'alterazione.

La conservazione rappresenta la protezione dell'integrità delle fonti di prova digitale. Questo obiettivo è rilevante poiché, come ampiamente dichiarato in precedenza, le evidenze digitali si contraddistinguono per l'immaterialità, la dispersione, la promiscuità e la congenita modificabilità.

In altri termini, le fonti di prova digitali sono fortemente alterabili e/o modificabili e, pertanto, la loro conservazione (o preservazione) richiede protocolli specifici che consentano, in qualsiasi fase del procedimento, di verificare l'integrità del dato.

I principali strumenti con cui è possibile ottenere questo risultato sono:

1. la catena di custodia dei reperti e delle copie,
2. l'impronta hash dei file copiati o generati,
3. la memorizzazione dei file su supporti durevoli.

Analizziamoli nel dettaglio.

La catena di custodia è un registro in grado di garantire la tracciabilità del reperto contenente le fonti di prova digitali. La catena di custodia di un reperto è ordinariamente creata nella fase di identificazione e segue il reperto in tutte le fasi successive. Tutte le volte che un reperto viene gestito dal forenser, tali attività devono essere evidenziate, attraverso una registrazione documentale, sulla catena di custodia in modo tale che chiunque possa agevolmente individuare:

- i dati identificativi del reperto,
- la data e l'ora di prelievo e di conservazione del reperto,
- il motivo dell'interazione,
- il nome di chi ha interagito con il reperto,
- il luogo di conservazione,
- lo stato del reperto prima e dopo l'evento.

Il calcolo dell'impronta hash dei file copiati o generati è una funzionalità che consente di garantire l'integrità delle fonti di prova digitali.

Gli algoritmi di hash sono utilizzati nell'ambito dell'informatica forense per validare e in qualche modo "firmare" digitalmente i dati acquisiti, tipicamente le copie forensi. L'algoritmo elabora qualunque mole di bit. Si tratta di una famiglia di algoritmi utilizzata anche nella digital forensics poiché soddisfa i seguenti requisiti sfruttati per verificare l'integrità di un file:

- l'algoritmo di hash restituisce una stringa di numeri e lettere a partire da un qualsiasi flusso di bit di qualsiasi dimensione (può essere un file, ma anche una stringa). L'output è detto "*digest"*,
- l'algoritmo non è invertibile, ossia non è possibile ricostruire il documento originale a partire dalla stringa che viene restituita in output ovvero è una funzione unidirezionale.

Tramite i codici hash è possibile in ogni momento verificare che quanto repertato sia rimasto immutato nel tempo. Se i codici hash corrispondono per entrambe le parti, originale e copia, si ha la ragionevole certezza di lavorare sulla stessa versione dei reperti, garantendo quindi un'uniformità di analisi e in genere di risultati. I risultati dei codici hash vengono ormai calcolati di default dalla maggioranza dei software per acquisizione forense e allegati alle copie forensi salvate.

Un software indicato per questa funzione è: **HashMyFiles v2.37** (http://www.nirsoft.net).

Tramite l'interfaccia grafica è possibile selezionare una directory di partenza (File – Add Folder o F3), comprendendo tutte le sub directory, ed avviare il calcolo dei digest in vari formati (MD5, SHA1, CRC32, SHA-256, SHA-512, SHA-384) di tutti i file presenti all'interno del percorso selezionato.

Al termine della funzione di calcolo, si selezionano tutte le righe (CTRL+A) e si salvano nella directory del caso in formato testo. Al file riepilogativo, che contiene le impronte digitali di tutti i file inclusi nel pacchetto di evidenza forense, sono apposti una marca temporale e una firma digitale per garantire la data certa, in cui è stata completata l'operazione di creazione della copia forense, l'integrità e l'inalterabilità della prova digitale e, infine, le generalità dell'operatore forense.

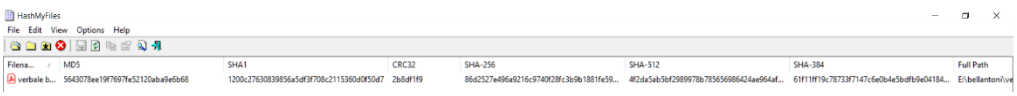


Fig. 18 – Schermata di HashMyFiles per il calcolo dell'impronta hash.

L'ultimo step riguarda il trasferimento di tutte le evidenze su un supporto di memoria durevole. Generalmente si prediligono i supporti ottici, come i Compact Disc (CD), i Digital Versatile Disc (DVD) o i Blu-ray Disc (DB), in alternativa possono essere utilizzati anche supporti di massa magnetici. Poiché il concetto "durevole", ovvero la capacità di conservare in modo duraturo le informazioni nel medio-lungo termine, non è una caratteristica definita in maniera scientifica per nessun tipo di memoria di massa, si sfruttano le peculiarità della "ridondanza". A tal riguardo, la prassi forense prevede che si realizzino almeno due o tre copie delle evidenze in modo tale che, in caso di deterioramento di una copia, sia possibile recuperare le evidenze da una delle altre copie.

3.5 Analisi

Spesso la digital forensics non si limita all'acquisizione delle fonti di prova, ma richiede anche un'attività di valutazione delle potenziali fonti di prova al fine di accertarne la rilevanza per l'indagine in corso, rispondere a determinati quesiti o ricercare ed estrarre specifiche informazioni.

Solitamente, se presente, è la fase più laboriosa ed estesa dell'intero processo di digital forensics.

L'attività di analisi può servire ad identificare e recuperare le informazioni d'interesse che, nell'ambito dell'Internet Forensics, possono riguardare le seguenti fattispecie:

- L'identità e/o l'autenticità dell'identità dell'autore della fonte di prova,
- La datazione della fonte di prova e/o la sua attendibilità,
- L'estrazione dei metadati e/o di ulteriori informazioni correlate alla fonte di prova.

L'identità e/o l'autenticità dell'identità dell'autore della fonte di prova.

Per verificare l'identità e l'autenticità dell'autore della fonte di prova è spesso necessario estendere il target dell'investigazione perché le informazioni acquisite potrebbero non essere sufficienti, oppure potrebbero essere oggetto di falsificazione o contestazione (p.e. falsi profili, sostituzione di identità). Al fine di consentire di avvalorare l'identità dell'autore è opportuno cercare ed acquisire ulteriori informazioni, anche al di fuori del contesto, come: i dati identificati del proprietario del server o del servizio online, i dati indentificati dell'autore dell'informazione, la data e l'ora di pubblicazione, i riferimenti, se presenti, ad altre fonti

informative che ci consentano di corroborare le informazioni di interesse nella fase di analisi (p.e. indicare se il contenuto sia stato condiviso o ripubblicato su altri server e/o da altri soggetti, oppure se il contenuto sia stato commentato o "linkato" su altri server e/o da altri soggetti), analizzare i metadati, verificare che lo stesso soggetto pubblica altrove oppure gestisce altre risorse web, ecc.

La datazione della fonte di prova e/o la sua attendibilità.

Per quanto riguarda la datazione di una fonte di prova si può fare ricorso a varie risorse:

- catturare la data restituita nell'header delle risposte HTTP relativa alle richieste di risorse web statiche quali: pagine html, immagini, documenti e qualsiasi altro file (cd. "Carbon dating"[38]),
- analizzare le date presenti nel corpo della pagina (le date dei commenti, dei post, dei collegamenti esterni, delle notizie, ecc.),
- estrarre le date dai metadati delle immagini, dei file audio e video e degli altri file connessi,
- effettuare una ricerca della risorsa sugli Internet Archive[39].

L'estrazione dei metadati e/o di ulteriori informazioni correlate alla fonte di prova.

Infine, può essere chiesto di estrarre ed analizzare i metadati della fonte di prova, in special modo se trattasi di contenuto multimediale, oppure le informazioni ad esso collegate tramite link esterni o ricerche sul web correlate.

In presenza di molti dati possono essere utilizzate metodologie di big data analysis che aiutano a correlare tra di loro le molteplici fonti di prova e ricostruire un determinato evento.

L'elenco riportato rappresenta una sintesi dei principali quesiti posti nelle indagini online e, ovviamente, non è esaustivo di tante altre fattispecie che possono scaturire dall'uso di Internet.

3.6 Interpretazione

Dopo aver completato le precedenti fasi tecniche, occorre predisporre una sintesi dell'intero

---

[38] Tool per il Carbon Dating: per estrarre le date degli elementi statici di una pagina https://github.com/Lazza/Carbon14, per trovare la risorsa sui siti archive http://carbondate.cs.odu.edu

[39] Un Internet Archive è una biblioteca digitale che ha lo scopo di creare una banca dati pubblica delle risorse digitali. Essa offre uno spazio digitale permanente per l'accesso a vari tipi di risorse: ad esempio, siti web, audio, immagini in movimento (video) e libri. La più famosa, Wayback Machine (https://archive.org), fu fondata da Brewster Kahle nel 1996 e fa parte della IIPC (International Internet Preservation Consortium).

processo tramite l'esposizione, entro i limiti concordati, delle informazioni fattuali ricavate dalle prove e dall'insieme di esami ed analisi che hanno costituito l'indagine. Questo obiettivo si concretizza attraverso la redazione di un elaborato o report da cui sia possibile ricavare:

- l'origine delle fonti di prova digitale,
- la metodologia utilizzata per la gestione delle fonti di prova,
- la tecnologia adoperata per il trattamento delle fonti di prova,
- la procedura eseguita per giungere ai risultati conseguiti,
- i risultati ottenuti (anche sottoforma di allegati multimediali),
- la risposta al quesito.

Un metodo suggerito per la stesura della relazione finale consiste nello sviluppare e strutturare la presentazione seguendo lo stesso ordine delle fasi ISO descritte nei paragrafi precedenti.

La presentazione dei risultati è l'elemento con cui si valuta tutta l'attività svolta. Per cui, durante la stesura, è fortemente consigliato tener conto delle seguenti indicazioni:

- occorre essere semplici e chiari,
- i risultati devono essere esposti in una forma facilmente comprensibile a tutti,
- i destinatari non hanno di solito competenze informatiche,
- molto probabilmente la relazione sarà esaminata da un tecnico della controparte,
- non bisogna essere approssimativi o esprimere giudizi che non siano corroborati dai dati.

Nell'ordinamento giuridico italiano, il risultato di un processo di digital forensics si può concretizzare in una perizia o in una consulenza tecnica. Sono i due mezzi di prova attraverso i quali fa ingresso nel processo il sapere tecnico, scientifico e artistico. Entrambe si sostanziano, alternativamente o cumulativamente, nello svolgimento di indagini, nell'acquisizione di dati o nell'effettuazione di valutazioni che richiedono per la loro natura particolari competenze tecniche, scientifiche o artistiche.

Nel processo penale distinguiamo:

- La perizia (artt. 220 e ss. c.p.p.) che costituisce il mezzo di prova "neutro" (essendone affidato l'espletamento ad un soggetto terzo, quindi imparziale, nominato dal giudice) ed essenzialmente discrezionale (essendo rimessa al giudice la valutazione sul requisito della sua "occorrenza"). Oltre che a richiesta di parte, può essere disposta anche d'ufficio.
- La consulenza tecnica, invece, può esperirsi: nell'ambito di una perizia già disposta,

concedendo alle parti facoltà di nominare propri consulenti che possono partecipare alle operazioni peritali al fine di realizzare il contraddittorio nella formazione della prova (art. 225 c.p.p.).

Nel processo civile il Giudice può nominare un Consulente tecnico per svolgere determinate indagini (art. 195 c.p.p.). Se l'attività è svolta in presenza del giudice istruttorio, il CTU deve trasferire i risultati in un processo verbale redatto dal cancelliere, mentre negli altri casi deve redigere una relazione scritta. La relazione deve essere trasmessa dal consulente alle parti costituite nel termine stabilito dal giudice con ordinanza resa all'udienza di giuramento. Anche nel processo amministrativo il Giudice può disporre una consulenza tecnica d'ufficio ai sensi dell'art. 67 c.p.a.

Per gli approfondimenti su questi ultimi aspetti si rimanda alla lettura dei testi indicati in bibliografia.

5 Conclusioni

Negli ultimi anni la prova informatica ha assunto un ruolo sempre più importante nell'ambito delle investigazioni giudiziarie e, pertanto, "l'introduzione delle tecnologie dell'informazione nel mondo criminale, anche se relativamente recente, ha avuto un'immediata propagazione a tutti i livelli, dal singolo alle organizzazioni più sofisticate"[40].

Quello che spesso rende l'attività complessa è il fatto che si deve acquisire qualcosa che risiede altrove, il cui controllo può non essere diretto e la cui presenza potrebbe variare nel tempo.

La scelta delle soluzioni tecnologiche proposte nel testo è stata deliberatamente orientata su prodotti open source per consentire un'immediata realizzabilità. In commercio sono disponibili diverse soluzioni alternative, in versione client (Hunchly, OSIRT, FAW, Magnet Web Page Saver) o hosted (PageFrezeer, LegalEye, Hanzo, Cliens Prova Digitale) che consentono di raggiungere gli stessi risultati in maniera più semplice e rapida, ma con la stessa efficacia giuridica.

L'esposizione dei contenuti di questo lavoro è orientata principalmente all'enunciazione dei principi della digital forensics e all'illustrazione di una metodologia scientificamente riconosciuta per il trattamento delle fonti di prova online.

A tal riguardo è opportuno sottolineare che "l'analista forense delle evidenze digitali ha l'onere di fornire in maniera puntuale e con l'avallo del metodo scientifico una connotazione spazio temporale dell'evento investigato definendo fatti, confutando alibi, correlando elementi o accadimenti"[41]. Di fondamentale importanza nell'analisi della digital evidence è la correlazione di fatti, elementi, indizi che, travalicando la mera disamina di stampo ingegneristico o peritale di un elemento repertato, ne caratterizza la formazione di elementi probatori.

Il biologo forense, che analizza un frammento di codice genetico, può scientificamente dimostrare la presenza di un soggetto sulla scena del crimine; tale circostanza, nell'ambito del processo investigativo, dovrà essere correlata ad altri elementi, tipicamente acquisiti nell'attività d'indagine, al fine di ottenere una linea temporale che definisca quando, come e

---

[40] Cfr. G. MAROTTA, Tecnologie dell'Informazione e processi di Vittimizzazione, in "Rivista di Criminologia, Vittimologia e Sicurezza", n. 2, Bologna, 2012, p. 94.
[41] M. TONELOTTO, Evidenza informatica, computer forensics e best practies, in "Rivista di Criminologia, Vittimologia e Sicurezza", n. 2, Bologna, 2014, p. 101.

perché quel soggetto, quella traccia, quell'elemento fosse stato presente in quel determinato luogo.

In ambito digitale questa correlazione spetta invece all'investigatore informatico, che deve necessariamente interagire con il fatto investigato, assumendo elementi anche non di carattere informatico, esaminando le tracce, non per forza digitali e correlando gli aspetti assunti nelle evidenze acquisite. Tali attività dovranno necessariamente essere compiute con perizia, scienza e coscienza, al fine di poter assumere l'elemento digitale come prova e proporla nelle opportune sedi giudiziarie.

La legge, seppur lacunosa nelle specifiche procedure tecniche da adottare, ha comunque affermato i principi fondamentali della conservazione, dell'integrità e della non alterabilità della prova informatica anche in situazioni emergenti, prevedendo l'applicazione di corrette procedure al fine di evitare l'alterazione dell'elemento digitale.

È indubbio come l'investigatore moderno debba sempre più frequentemente confrontarsi con le nuove tecnologie al fine di poter fornire una risposta certa, precisa e minuziosa al fatto investigato. Per questo motivo, e per le caratteristiche dell'ambiente virtuale sempre più interconnesso con quello reale, dovrà operare in base a procedure codificate e non esclusivamente sulla scorta dell'intuito personale, dell'improvvisazione o dell'esperienza. Tali elementi certamente necessari, fondamentali ed indispensabili all'attività investigativa, non rappresentano più condizioni sufficienti per un approccio moderno alle scienze criminali.

6. Bibliografia

F. CARNELUTTI, Teoria generale del diritto, in “Società del Foro italiano”, 1951, Roma.

E. CASEY, Digital Evidence and Computer Crime (Third Edition): Forensic Science, Computers, and the Internet, Academic Press, Cambridge, 2011.

E. CASEY, Trust in digital evidence, in “Forensic Science International: Digital Investigation”, F. 31 (2019) 200898, Elsevier, Amsterdam, 2019.

V. COLAROCCO, T. GROTTO, G. VACIAGO, La prova digitale, Giuffrè Francis Lefebvre, Milano, 2020.

V. COLAROCCO, M. FERRAZZANO, La pagina web come prova digitale nel processo civile, in “Questioni di informatica forense”, Aracne editrice, Roma, 2015.

A. GHIRARDINI, G. FAGGIOLI, Digital Forensics, Apogeo, Milano, 2013.

L. LUPARIA, G. ZICCARDI, Investigazione penale e tecnologia informatica, Giuffrè, Milano, 2007.

C. MAIOLI, Dar voce alle prove: elementi di informatica forense, in “La sicurezza preventiva dell’informazione e della comunicazione” (a cura di P. Pozzi), Bologna, 2004.

G. MAROTTA, Tecnologie dell’Informazione e processi di Vittimizzazione, in “Rivista di Criminologia, Vittimologia e Sicurezza”, n. 2, Bologna, 2012, p. 94.

S. MASON, Electronic Evidence. Discovery and Admissibility, LexisNexis Butterworths, London, 2007.

A. S. TANENBAUM, D. J. WETHERALL, Fondamenti di reti di calcolatori, Pearson, Milano, 2013.

M. TONELOTTO, Evidenza informatica, computer forensics e best practies, in “Rivista di Criminologia, Vittimologia e Sicurezza”, n. 2, Bologna, 2014, p. 101.

ISO/IEC 27043:2015 Information technology — Security techniques — Incident investigation principles and processes (https://www.iso.org/standard/44407.html).

ISO/IEC 27035-1:2016 Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management (https://www.iso.org/standard/60803.html).

ISO/IEC 27035-2:2016 Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response (https://www.iso.org/standard/62071.html).

ISO/IEC 27035-3:2020 Information technology — Information security incident management — Part 3: Guidelines for ICT incident response operations (https://www.iso.org/standard/74033.html).

ISO/IEC 27037:2012 Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence (https://www.iso.org/standard/44381.html).

ISO/IEC 27042:2015 Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence (https://www.iso.org/standard/44406.html).

ISO/IEC 27041:2015 Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative method (https://www.iso.org/standard/44405.html).

ISO 28500:2017 Information and documentation — WARC file format (https://www.iso.org/standard/68004.html).

Request for Comments: 2557 - MIME Encapsulation of Aggregate Documents, such as HTML (MHTML) (https://tools.ietf.org/html/rfc2557)

Internet Archive (https://web.archive.org/).

The Chromium Projects - Blink (Rendering Engine) (https://www.chromium.org/blink).

The Webrecorder Projects (https://webrecorder.net/).