# Framework dell'analisi digitale forense – parte II

*Segue dalla prima parte*

## Identificazione

Il processo di identificazione (da non confondere con la fase di identificazione, che solitamente si svolge in fase di perquisizione e sequestro) deve essere messo in atto per ogni elemento contenuto nell'elenco dei dati estratti.

In primo luogo, si determina la **natura** dell'elemento attenzionato. Se non è rilevante per rispondere ai quesiti posti, si contrassegna semplicemente come elaborato o processato e si va avanti. Proprio come in una ricerca fisica, se ci si imbatte in un elemento potenzialmente incriminante, ma al di fuori dell'ambito del mandato di ricerca originale, è consigliabile interrompere immediatamente tutte le attività, notificare l'evento ai soggetti appropriati (fatto salvo nei casi previsti dall'ordinamento o in caso di investigazione difensiva c.p.p. art. 334-bis), incluso il richiedente, e attendere ulteriori istruzioni.
Ad esempio, le forze dell'ordine potrebbero sequestrare un computer alla ricerca di prove per frode fiscale, ma ci si imbatte poi in un'immagine pedopornografica. L'approccio più prudente, nel caso in cui si rinvengono prove fuori dell'ambito di un mandato, è quello di fermare la ricerca e cercare di ampliare l'autorità di quel mandato o di ottenere un secondo mandato. Se un elemento, invece, è rilevante e pertinente ai fini dell'indagine viene documentato e inserito in un terzo elenco, l'elenco dei **dati pertinenti** (*"Relevant Data List"*). Questo elenco è una raccolta di dati rilevanti utili per rispondere al quesito o ai quesiti posti.

**Figura 1 – Identificazione**

In un caso di furto di identità, i dati rilevanti potrebbero includere tra le altre cose numeri di codice fiscale, numero di CI o patente, false immagini di identificazione o e-mail in cui si discute di furto di identità. È anche possibile che un elemento generi un altro oggetto (*"lead"*) che induca una nuova ricerca (*"Data Search Leads"*). Un'e-mail potrebbe rivelare che un target, oggetto di indagine, stava usando un altro nickname. Questo porterebbe a una nuova parola chiave da ricercare, ovvero quel nuovo nickname. Si può aggiungere questo nuovo elemento nella Lista di Elementi da ricercare (*"Data Search Lead List"*) in modo che ci si ricordi di indagare approfonditamente su di esso in seguito.

Un elemento può anche condurre a una nuova potenziale fonte di dati utili (*"New Source of Data"*) e che precedentemente non era stata considerata.
Ad esempio, si potrebbe trovare un nuovo account di posta elettronica utilizzato dal target. Si potrebbero anche trovare prove che indicano l'esistenza di file memorizzati su un'unità USB rimovibile e che le forze dell'ordine non hanno trovato al momento della perquisizione. In queste circostanze, le forze dell'ordine possono prendere in considerazione la possibilità di richiedere un nuovo mandato di perquisizione per cercare l'unità USB. Un'accurata **elaborazione forense** dei dati può portare alla luce molti tipi diversi di nuove prove. Tra questi si possono considerare i registri di sistema, i file di log, la creazione di registri di accesso o di eventi, recent files, lnk files, metadati, ecc. e cronologie di diversa natura, come ad esempio navigazione web e molti altri ancora.

Si documenta, quindi, tutto ciò e li si inserisce in un quarto elenco, la Lista di nuove fonti di dati (*"New Source of Data list"*). Dopo aver esaminato ed esaurito l'elenco dei dati estratti (*"Prepared/Extracted Data List"*), si esaminano tutti i nuovi lead sviluppati. Per tutti i nuovi lead di ricerca dei dati, può rendersi utile tornare alla fase di **Estrazione**

lavorando sull'immagine forense. Questo nell'eventualità in cui i dati a cui fanno riferimento i nuovi processi di ricerca non siano immediatamente disponibili, già estratti. Allo stesso modo, per qualsiasi nuova fonte di dati che potrebbe portare a nuove prove, sarà necessario tornare fino al processo di acquisizione e imaging dei nuovi dati forensi. Questo è il caso in cui, ad esempio, venisse rinvenuto un nuovo supporto di memorizzazione come l'unità USB di cui si parlava prima.

A questo punto delle indagini – e a seconda dei casi -, potrebbe essere consigliabile informare il richiedente dei risultati ottenuti. I dati pertinenti estratti e identificati possono già fornire informazioni sufficienti per portare avanti il caso. La conseguenza sarebbe non aver bisogno di effettuare ulteriori lavori. Infatti, in un caso di pedopornografia, se si recuperano un numero sufficiente e schiacciante di immagini pedopornografiche organizzate in *directory* create dall'utente e sussistono ulteriori condizioni necessarie anche di natura tecnica che permettano di accertare i fatti, un pubblico ministero potrebbe essere in grado di ottenere una sentenza di colpevolezza senza ulteriori analisi forensi.

Se invece i dati estratti e identificati "semplici" non sono sufficienti, la fase successiva è l'analisi.

## Analisi

Nella fase di analisi bisogna cercare di collegare tutti i punti e dipingere un quadro completo del caso.

Per ogni elemento dell'elenco dei dati pertinenti, è appropriato rispondere a domande come chi, cosa, quando, dove e come. Bisogna cercare di spiegare quale utente o applicazione ha creato, modificato, ricevuto o inviato ogni elemento e come esso ha avuto origine. È importante spiegare e documentare anche dove vengono trovati questi elementi. Ancora

più importante, spiegare perché tutte queste informazioni sono significative e cosa significano per il caso in esame.

Spesso gli esperti possono rendere l'analisi più preziosa e meticolosa osservando tecnicamente quando sono avvenute le cose e producendo una **linea temporale** (*timeline*) che racconti una storia coerente. Per ogni elemento pertinente, si illustra quando è stato creato, acceduto, modificato, ricevuto, inviato, visualizzato, eliminato e avviato. Si osservano e spiegano sequenze di eventi, mettendo in evidenza e in relazione quali eventi sono accaduti nello stesso momento o periodo temporale.



**Figura 2 – Analisi**

Si deve documentare adeguatamente tutte le analisi svolte e altre informazioni rilevanti per la richiesta forense da soddisfare e aggiungere tutto in un quinto e ultimo elenco, l'**"Elenco dei risultati dell'analisi"** (*"Analysis results list"*). Questo è un elenco di tutti i dati significativi che rispondono a chi, cosa, quando, dove, come e altre domande. Le informazioni contenute in questo elenco devono soddisfare la richiesta e i questi sottoposti all'analista forense dal richiedente. Anche in questa fase avanzata del processo, qualcosa potrebbe generare nuovi *lead* di ricerca dei dati o anche una nuova fonte di dati: in questo caso, questi verranno aggiunti agli elenchi appropriati per poi valutare la possibilità di tornare indietro per esaminarli approfonditamente.

Infine, dopo avere effettuato questi passaggi un numero sufficiente di volte e quando si è certi dei risultati ottenuti, si può rispondere compiutamente alla richiesta formulata dal richiedente, redigendo la necessaria relazione tecnica. A questa fa seguito la preparazione di una adeguata presentazione. Questo è il passaggio in cui bisogna

documentare con adeguato registro i risultati, in modo che il richiedente o autorità giudiziaria possa comprenderli e utilizzarli nel procedimento.

La **relazione finale** è il modo migliore per comunicare i risultati al richiedente. La presentazione, ancor di più, è importante perché l'intero processo forense diventa valido e utilizzabile, nelle opportune sedi, in funzione della capacità di trasmettere correttamente tutte le informazioni al richiedente, qualsiasi esso sia. Dopo la presentazione, il richiedente esegue un'analisi a livello di caso in cui egli (eventualmente con gli esperti) interpreta i risultati nel contesto dell'intero caso giudiziario.

## Conclusioni

Mentre esperti e richiedenti si destreggiano attraverso questo tutto questo processo, è doveroso pensare al ritorno economico dell'investimento profuso in termini di tempo, competenze e risorse. Vi è anche un tema molto dibattuto sulla proporzionalità delle vacazioni e il corretto riconoscimento delle competenze in questo settore. Oltretutto, durante un'azione investigativa, le fasi del processo possono essere ripetute più volte determinando ulteriore dispendio. Tutti coloro che sono coinvolti nel caso devono determinare quando possa essere utile fermarsi. Una volta ottenute le prove, il valore dell'identificazione e dell'analisi aggiuntive tende inevitabilmente a diminuire.

Si spera che questo articolo possa essere un'utile introduzione alla informatica forense e alla metodologia di analisi digitale forense; il diagramma di flusso può servire come strumento utile per guidare le analisi.

## Riferimenti

https://www.altalex.com/documents/news/2013/12/18/notizia-di-reato

https://www.sicurezzaegiustizia.com/giustizia-ed-informatica-forense-particolarita-ed-eccezioni/

Articolo a cura di **Francesco Costanzo**



Ho conseguito la laurea in Ingegneria Informatica presso l'Università della Calabria.

Mi sono specializzato in digital forensics e investigazioni digitali attraverso un master in digital forensics e cyber security presso l'ISF College Corporate University (Milano). In seguito perfezionato in Criminalità Informatica e Investigazioni Digitali presso l'Università Statale di Milano.

Sono membro dell'Associazione Nazionale Criminologi e Criminalisti (Elenco del Ministero dello Sviluppo Economico, legge 14 gennaio 2013, n. 4). Iscritto al n. 00148/2020/PRO Sett. B Criminalisti in qualità di Criminalista esperto.

In possesso dell'Attestato di Qualità e Qualificazione Professionale dei Servizi prestati ai sensi degli artt. 4, 7 e 8 della legge 14 gennaio 2013, n. 4 (Attestato approvato Ministero dello Sviluppo Economico) rilasciato dall'Associazione Nazionale Criminologi e Criminalisti.

Presso l'Istituto di Scienze Forensi ricopro la figura di Investigatore tecnico forense.

Sono docente titolare degli insegnamenti di "Digital e computer forensics" presso l'ISF College Corporate University di Corsico (MI).



https://www.ictsecuritymagazine.com/articoli/framework-dellanalisi-digitale-forense-parte-ii/