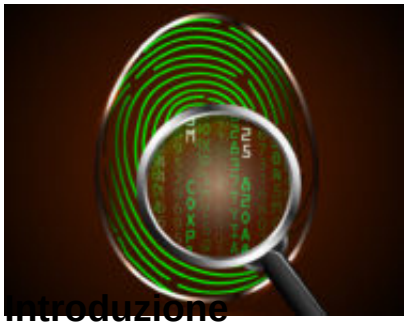
Framework dell’analisi digitale forense

Author : Francesco Costanzo

Date : 12 Ottobre 2020



Introduzione

Emersa a partire dai primi nei anni 80, quando i personal computer cominciavano ad essere più accessibili ai consumatori accrescendone però l'utilizzo in attività criminali, il campo dell’informatica forense è relativamente giovane rispetto ad altre scienze forensi.

Nonostante intervenga oramai in moltissimi procedimenti giudiziari come uno dei principali mezzi di investigazione legato a diversi crimini, di natura puramente informatica e non, non sempre si riesce a capire pienamente ciò che significa il termine **informatica forense** e quali siano le tecniche convolte. In particolare, sovente, vi è una mancanza di chiarezza per quanto riguarda la distinzione tra l'estrazione dei dati e l'analisi dei dati.

Il Cybercrime Lab in the Computer Crime and Intellectual Property Section (CCIPS) ha sviluppato un interessante *flow chart* che descrive nel dettaglio la metodologia di analisi forense digitale, disponibile sul sito web https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/03/26/forensics_chart.pdf. Tale *flow chart* è frutto della collaborazione di numerosi *computer forenser expert* operanti in diverse agenzie federali americane. Questo lo rende una valida guida durante le fasi dell’investigazione e aiuta a chiarire meglio le varie fasi del processo di analisi forense.

In questo articolo, sfruttando le caratteristiche di questo diagramma di flusso, si analizzerà e spiegherà la metodologia e i passi coinvolti in tale processo di analisi.

Panoramica della metodologia di analisi digitale forense

La definizione completa di informatica forense può essere espressa come: *"L'uso di metodi collaudati e scientifici per la raccolta, conservazione, validazione, identificazione, analisi, interpretazione, documentazione e presentazione di prove digitali provenienti da fonti digitali allo scopo di facilitare o promuovere la ricostruzione di eventi ritenuti criminosi o per aiutare ad identificare preventivamente azioni non autorizzate che si potrebbero dimostrare lesive o distruttive".*

La scienza dell’informatica forense si snoda in diversi settori della tecnologia al fine di permettere al perito informatico di acquisire e analizzare diverse tipologie di dispositivi e di dati.

Molti discutono se l’informatica forense sia **una scienza o un’arte**. Dati i numerosi modi in cui le informazioni vengono memorizzate su un dispositivo digitale, in maniera consapevole ed esplicita ad opera dell’utente o in maniera inconsapevole e nascosta ad opera dei sistemi e degli applicativi, la ricerca di tali dati può essere tanto un'arte quanto una scienza. La questione, tuttavia, non deve necessariamente porsi.

Gli strumenti e i metodi utilizzati sono scientifici e sono verificabili scientificamente. Il loro uso, però, richiede necessariamente il possesso, da parte di chi li utilizza, di competente specialistiche fortemente caratterizzanti ovvero abilità, giudizio e capacità di interpretazione. È proprio l’esercizio di tali competenze, la cui cognizione, specie da parte dei giuristi, è conquista degli ultimi anni, ad indurre gli osservatori a far trascendere il concetto di scienza o di metodo scientifico a favore del concetto di arte.

Ecco perché la parola "tecnica", in tutta la sua accezione, è spesso e volentieri usata per evitare l’annosa e improduttiva controversia tra scienza e arte in questo campo.

Alcuni **elementi chiave** dell’informatica forense sono elencati di seguito:

- uso di metodi scientifici;
- uso di *best practices*;
- collezione (o acquisizione) e conservazione;
- validazione;
- identificazione;
- analisi e interpretazione;
- documentazione e presentazione.

Il *flow chart* del Laboratorio di Cybercrime propone uno schema del processo investigativo molto intuitivo e confortevole, si veda la Figura 1.

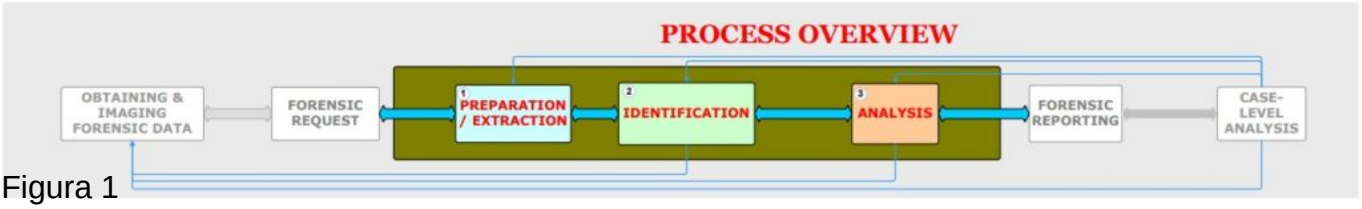


Figura 1

I tre passi, la preparazione/estrazione dei dati (1), l’identificazione (2) e l’analisi (3), sono i più importanti dell’intero processo di analisi.

Lo schema è potenzialmente iterativo, quindi si può anche decidere quante volte ripetere i passi. Infatti è di fondamentale importanza che si comprenda se un caso richiede l’esperimento di ogni singola fase o solamente la preparazione, l’estrazione e l'identificazione. Questo

perché, ad esempio, lo scopo di un'analisi forense può variare dal recupero di semplici informazioni alla ricostruzione di una serie di eventi.

Il punto di partenza è l’ottenimento di tutto il necessario per procedere, ovvero le immagini forensi dai dati da sottoporre alle analisi e una richiesta formale da parte dell’autorità giudiziaria o del privato. È proprio in questa prima fase che si effettua **un'analisi preliminare** del caso, si analizzano i quesiti, si stende un verbale e si predispone una catena di custodia. Essere meticolosi e precisi è particolarmente importante e il rispetto delle *best practices* lo è ancora di più. Ogni singola azione del processo investigativo che interviene nella metodologia forense adottata deve essere spiegata nel dettaglio.

Si procede, quindi, al vero e proprio accertamento tecnico che consiste nei tre passi evidenziati. Ognuno di questi tre passi, come si nota dallo schema, rappresenta un ipotetico nuovo punto di partenza. Questo perché potrebbe rendersi utile ripetere l’intero processo al fine di trovare ulteriori elementi ed evidenze digitali da studiare. Difatti potrebbero emergere elementi del tutto nuovi o che vadano ad agire come sussidiari alle prime rinvenute.

Preparazione ed Estrazione dei dati

Si inizia chiedendosi se vi sono sufficienti informazioni per procedere. Ci si assicura di avere una richiesta chiara e non equivoca in mano, sotto forma di quesiti, e che vi siano sufficienti dati per riuscire a rispondere in modo esaustivo. Se manca qualcosa, ci si confronta e coordina con il richiedente per determinare come proseguire.

In caso contrario, ovvero se gli elementi a disposizione risultano sufficienti, si continua a portare avanti il processo. Si veda la figura 2.

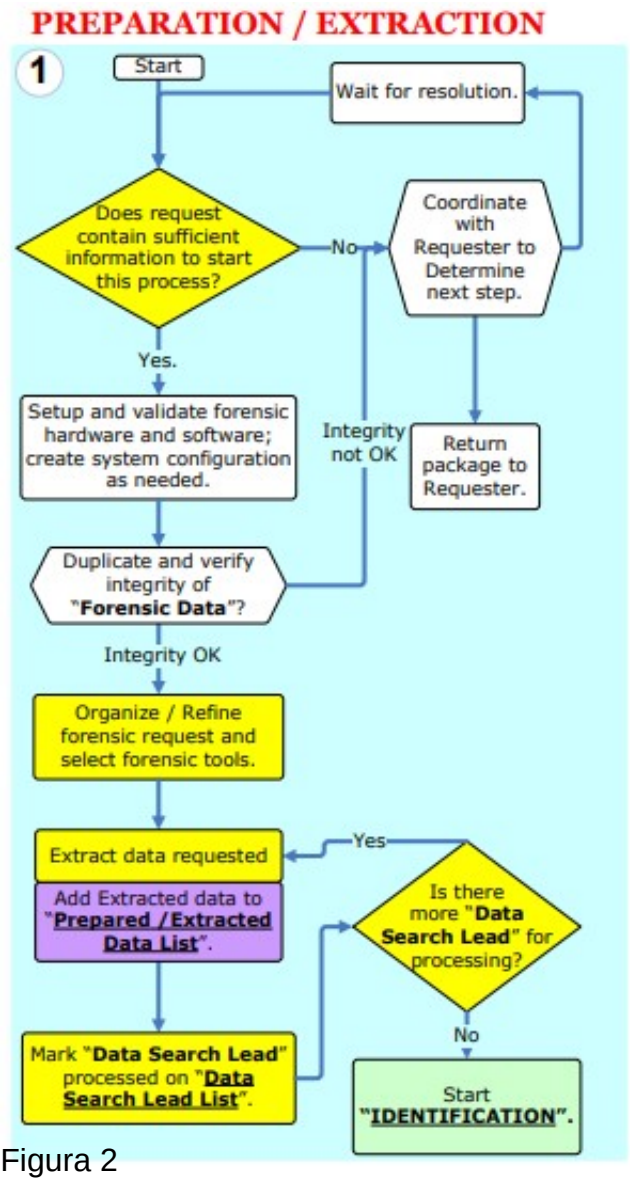


Figura 2

Il primo passo, di natura tecnica, in qualsiasi processo forense è la convalida di tutto l'hardware e il software, per garantire che funzionino correttamente. Potrebbe rendersi necessario aggiornare i *firmware*, verificare che non sia state rinvenuti falle o più semplicemente che gli strumenti a disposizione non siano danneggiati o compromessi da usi incauti. Anche in questo caso una approfondita analisi a livello del "caso" è quanto mai consigliata. Non sempre gli strumenti validi per un caso lo sono anche per quello in esame, e non sempre gli strumenti utilizzati producono i risultati attesi. **Flessibilità, adattabilità e apertura mentale** sono altri requisiti fondamentali. Non sono pochi i casi risolti usando semplicemente dei piccoli *tool* gratuiti od *open source*. L'affidabilità di quest'ultimi è se non altro garantita, senza difficolta alcuna, dal codice aperto e dalla comunità dei *peer reviewer.* Tutti gli strumenti dovrebbe essere ritestati anche dopo ogni aggiornamento o riconfigurazione.

Quando la *workstation* forense è pronta, si duplicano i dati forensi forniti e se ne verifica

l'integrità.

Questa attività presuppone che si siano già ottenuti i dati attraverso un processo legale e metodico che abbia condotto a creare **un'immagine forense**. Un'immagine forense è una copia bit-a-bit dei dati che sono memorizzati sul supporto originale, senza aggiunte o eliminazioni o in definitiva modificazioni. Si presuppone inoltre che l'esaminatore forense abbia ricevuto una copia di lavoro dei dati, ovvero una copia dell'immagine forense originale. Se gli esaminatori ottengono, invece, direttamente le prove originali, hanno bisogno di fare una copia di lavoro e custodire l'originale con una opportuna catena di custodia. Bisogna assicurarsi che la copia in possesso sia intatta e inalterata.

A tal fine, si procede verificando l'*hash*, o impronta digitale, delle prove. Se sono presenti problemi, incongruenze o atro ci si consulta con il richiedente per determinare come si intendere procedere. Registrare tutto su verbale è il minimo.

Dopo aver verificato l'integrità dei dati da analizzare, viene sviluppato un piano per **estrarre i dati** di interesse. Si organizza, quindi, e raffina la comprensione della richiesta del cliente in relazione ai quesiti posti per determinare come pervenire alla risposta attesa.

Vengono individuati gli strumenti che consentono di rispondere a questi quesiti. Già dalle prime battute, in genere, si hanno delle idee di massima su cosa cercare, sulla base della richiesta. A questi elementi si aggiunge poi una *"Search Lead List"*, ovvero una lista di ricerche specifiche da condurre che funge da guida per indirizzare l'attenzione dell'esaminatore sul caso in esame.

Ad esempio, la richiesta potrebbe vertere su provvedere indizi utili per dimostrare una "ricerca di materiale pedopornografico." La lista li guiderà in maniera specifica a concentrare le ricerche su elementi attinenti alla richiesta. Man mano che emergono nuovi indizi vengono aggiunti alla lista come elementi di approfondimento. Mentre viene elaborata ogni singola ricerca, questi sono segnati come "processato" o "fatto" realizzando di fatto una vera e propria *"to do list".*

Per ogni ricerca condotta, si estraggono i dati pertinenti e si contrassegnano anch'essi come processati. Tutti questi vanno a comporre un secondo elenco chiamato "Elenco dei dati estratti".

La fase successiva è l'identificazione.

Riferimenti

https://www.justice.gov/criminal-ccips
https://it.wikipedia.org/wiki/Informatica_forense
A Road Map for Digital Forensic Research, Report from the First Digital Forensic Research Workshop (DFRWS), available at http://www.dfrws.org/sites/default/files/session-files/a_road_map_for_digital_forensic_research.pdf.

The Need for Digital Forensic Investigative Framework, at https://www.researchgate.net/publication/266794518_THE_NEED_FOR_DIGITAL_FORENSIC_INVESTIGATIE_FRAMEWORK

Articolo a cura di **Francesco Costanzo**