Digital Forensics dogmi o ragionamento?

IL REPERTAMENTO E L'ANALISI DELLA DIGITAL EVIDENCE NON DEVE ESSERE REGOLATO DA DOGMI E PROCEDURE MONOLITICHE, MA DA MODUS OPERANDI VALIDO SEMPRE, ANCHE PER LE SITUAZIONI INSOLITE

Si sa che le cosiddette "best practices"[1] (**SWGDE**, **NIJ**, la **ISO/IEC 27037**[2] [3]) regolano molti processi della digital forensics insieme ad alcune leggi e certificazioni internazionali che elencano una serie di accorgimenti ormai consolidati ed accettati dalla comunità dei digital forensics expert.

In Italia la legge 48/2008[3] [1] impone alcune cautele nell'analisi dei reperti digitali, proprio come avviene di solito con i reperti "classici", come le armi, le impronte digitali, ecc. ecc.

Le best practices internazionali indicano metodi ormai standardizzati ed accettati *de facto* dagli operatori del settore ma, a causa della costante evoluzione tecnologica, sia hardware sia software, spesso ci si trova ad affrontare situazioni nuove, strane, o a dover ragionare sul come agire e dover spiegare se la procedura adottata

1 https://www.swgde.org/documents/Current%20Documents/2014-09-05%20SWGDE%20Best%20Practices%20for%20Computer%20Forensics%20V3-1
2 http://www.iso.org/iso/catalogue_detail?csnumber=44381
3 http://www.parlamento.it/parlam/leggi/080481.htm

Nanni Bassetti è Laureato in Scienze dell'Informazione a Bari ed è libero professionista specializzato in informatica forense. Ha collaborato come free-lance con molte riviste informatiche nazionali e internazionali e come docente per molti corsi presso enti, scuole e università, ha inoltre scritto articoli divulgativi di programmazione, web usability, sicurezza informatica e digital forensics. Ha lavorato come ausiliario di Polizia Giudiziaria e per alcune Procure della Repubblica oltre che come CTU/CTP per molte analisi forensi informatiche civili e penali. Iscritto all'albo dei C.T.U. presso il Tribunale di Bari, è consulente di parte civile per alcuni casi di risonanza nazionale. Fondatore di CFI – Computer Forensics Italy – la più grande community di computer forensics italiana e Segretario di ONIF (Osservatorio Nazionale Informatica Forense). Project manager di Caine Linux Live Distro forense. Curatore del sito Scripts4cf dedicato a software per la computer forensics. Ha pubblicato "Internet Web Security – tutta la verità sulla sicurezza del web" nel 2004 con la Duke Editrice e il libro "Indagini Digitali". Fa parte del Comitato di Redazione della rivista "Sicurezza e Giustizia", su cui ha pubblicato diversi articoli.

sia corretta e che conseguenze porta sul reperto digitale.
Quindi, di fronte a degli eventi o situazioni non risolvibili con la "best practices", bisogna agire seguendo delle procedure che garantiscano un metodo ed una bibliografia scientifica e, laddove possibile, una ripetibilità dei risultati ottenuti.
L'applicazione delle procedure di digital forensics dovrebbe assicurare i requisiti di integrità, autenticità, veridicità, non ripudiabilità e completezza della fonte di prova ma, in quest'articolo, si vuole analizzare la casistica ispirata dal secondo principio dell'ACPO [5]:
Principio 2: In circostanze eccezionali, quando una persona si trova nella necessità di accedere ai dati originali conservati su un computer o su supporti di memorizzazione, bisogna che tale persona sia competente e che sia in grado di testimoniare e spiegare la rilevanza e le implicazioni delle proprie azioni.
Quindi, quando non si è nel dominio delle procedure standard che si usano usualmente, si dovrà ragionare e spiegare il perché il tipo di procedura o metodo adottato ha comunque valenza forense e scientifica.

APPLICANDO LE LEGGI SCIENTIFICHE ED IL RAGIONAMENTO LA DIGITAL FORENSICS PUÒ GARANTIRE LA SOLIDITÀ DI UN METODO ADOTTATO

NANNI BASSETTI

LA COPIA FORENSE

Nell'ambito della digital forensics, quando si pensa alla copia forense, subito si accosta il concetto di bit a bit dell'intero supporto di memoria, poi si pensa alla verifica del codice hash, ma si può definire co-

pia forense anche qualcosa che non è stata effettuata copiando dal primo bit all'ultimo bit di un reperto digitale?
La risposta è affermativa poiché per copia forense si intende una copia che abbia validità forense, ossia sia resistente in un Giudizio. Pertanto, anche una copia di una porzione di dati, se motivata e cristallizzata con una verifica di hash, può essere considerata una copia forense.

Esempi:
- Memoria di un telefono cellulare acquisita solo a livello logico o filesystem
- Casella di posta elettronica specifica, estratta da un hard disk di un server che non poteva essere duplicato per intero per vari motivi, legali o tecnici.
- Uno o più file appartenenti ad un computer che per qualche motivo tecnico o legale non poteva esser acquisito per intero.
- Un sito Internet acquisito da remoto.

Insomma, se per cause serie e solide si deve acquisire un elemento digitale in maniera parziale, bisogna spiegare il motivo per cui si è agito in quel modo, le cautele adottate per mantenere il più integro possibile il reperto, quali sono le conseguenze della procedura adottata e se si avevano i mezzi e le competenze per effettuarla.

Esempi:
- Per un motivo qualsiasi si deve acquisire una singola directory da un hard disk.
  Si spiega il motivo, si utilizza un software che permetta di copiarla mantenendo anche i metadati di file system come i timestamps, si calcola il codice hash per cristallizzarne l'identità digitale e garantirne l'autenticità nella catena di custodia.
- Per una limitazione tecnologica dello strumento in uso al consulente tecnico di un telefono cellulare si può acquisire solo il file system.
  Si spiega il motivo, si spiega cosa si perde, ossia la possibilità di recuperare le informazioni nello spazio non allocato (es. fotografie cancellate) e si calcola l'hash del dump ottenuto dallo strumento di mobile forensics adottato.

Questo primo "dogma" della copia bit-a-bit dell'intero dispositivo di memoria è facilmente superabile perché, laddove non è possibile effettuarla in quella modalità, il dato va raccolto diversamente, consapevoli delle informazioni di contorno che possono mancare ed adottando le maggiori cautele e garanzie possibili.

IL CONTENUTO DI UN HARD DISK

"*Il consulente acquisisca il contenuto degli hard disk*"
Cosa si intende per "*contenuto*" di un supporto di memoria di massa?
La risposta ovvia è lo strato dei dati memorizzati su di esso ed accessibili tramite software di analisi forense, ma se si volesse fare un ragionamento allargato si potrebbe pensare a qualsiasi cosa a partire dalle testine, i piattelli, firmwa-

re della PCB[4] [4] del disco rigido, ecc..
In questo caso si può ragionare per analogia con le leggi della Fisica. Infatti, se qualcuno chiede di misurare la velocità di un'automobile su un circuito di prova, tutti penseranno al sistema di riferimento inerziale relativo all'automobile sul circuito, tralasciando la rotazione terrestre, la curvatura, la rivoluzione planetaria, la rotazione del sistema solare, ecc. ecc..
Parametri che invece possono tornar utili ed importanti nel momento in cui si deve lanciare un razzo spaziale.
Per questo motivo, nel momento in cui si chiede l'acquisizione dei dati contenuti nell'hard disk, si dovrà pensare al sistema di riferimento "*dati dell'utenza umana*" e non ai dati contenuti nel firmware della PCB [4] del disco rigido, a meno che non vi sia una specifica necessità che può essere manifestata dal ponente il quesito o dall'analista stesso.
Ma perché è importante focalizzare quest'aspetto?
La risposta è nell'applicabilità del tipo di accertamento tecnico, se diviene ripetibile o se altera l'oggetto d'analisi.
Infatti, se consideriamo l'hard disk "in toto", quindi come oggetto fisico composto da varie componenti hardware e software, se il sistema di riferimento è questo, allora anche l'aver toccato l'oggetto, aver dato corrente elettrica, aver modificato alcuni parametri delle funzioni di SMART[5] [4] e mutato il tempo d'usura, implica che la semplice estrazione del disco e connessione al computer dell'analista, ha cagionato delle alterazioni al reperto.
Di contro, se il sistema di riferimento è il layer (strato) dei dati accessibili via software (file allocati, file non allocati e slackspace), allora quei dati, adeguatamente protetti dalla connessione del disco elettromeccanico ad un write blocker (hw o sw), rimangono gli stessi e forniranno lo stesso codice hash ogni volta che si estrarranno per effettuare copia forense, chiaramente ipotizzando un sistema ideale che non si rompa o corrompa nel tempo.
Pertanto è importante definire il dominio di repertazione al fine di giudicare se un tipo di accertamento tecnico, per sua natura, apporterà o meno modifiche sulle informazioni da acquisire.

4 PCB: Printed Circuit Board
5 Self-Monitoring, Analysis, and Reporting Technology, o S.M.A.R.T., è un sistema di monitoraggio per dischi rigidi e per SSD, per rilevare e fornire diversi indicatori di affidabilità, nella speranza di anticipare i malfunzionamenti.
https://it.wikipedia.org/wiki/Self-Monitoring,_Analysis_and_Reporting_Technology
6 http://www.fawproject.com/

non c'entrano niente con l'indagine in corso, pertanto si utilizzano mezzi di repertazione remota, che permettono di acquisire le pagine target nel modo più completo possibile.
La complessità sta nel fatto che non basta un mero screenshot per cristallizzare una pagina web, poiché esso non è un documento attendibile, potrebbe esser stato creato con un qualsiasi strumento di fotoritocco ed inoltre è privo di qualsiasi altro metadato e codice sorgente, perciò andrebbero acquisiti più elementi:
- Codice sorgente della pagina e di tutti gli elementi che la compongono
- Sincronizzazione dell'orologio del computer utilizzato per acquisire con dei timestamp server internazionali
- Acquisizione dell'agent utilizzato
- Video della navigazione sul sito
- Screenshot del sito
- Hash di ogni elemento acquisito
- Pacchetti di rete transitati dalla macchina d'acquisizione verso il sito osservato
- Marca temporale
- Firma digitale

Queste operazioni si possono fare singolarmente o con software come FAW[6].
Tutto questo per garantire che il dato digitale è stato acquisito e riportato in digitale. Ma c'è sempre lo spettro che qualsiasi cosa digitale può esser artefatta e sicuramente, più elementi ci sono più diventa difficile ma comunque possibile.
Quindi si prospetta la possibilità che un garante terzo possa essere più attendibile di una serie di "cat-

IN CIRCOSTANZE ECCEZIONALI, QUANDO UNA PERSONA SI TROVA NELLA NECESSITÀ DI ACCEDERE AI DATI ORIGINALI CONSERVATI SU UN COMPUTER O SU SUPPORTI DI MEMORIZZAZIONE, BISOGNA CHE TALE PERSONA SIA COMPETENTE E CHE SIA IN GRADO DI TESTIMONIARE E SPIEGARE LA RILEVANZA E LE IMPLICAZIONI DELLE PROPRIE AZIONI

IL SITO INTERNET

Nel caso si debba repertare un sito Internet, per esempio una pagina web di un blog, di un forum, di una testata giornalistica online, di un social network, il concetto di copia bit-a-bit imporrebbe la copia totale dell'hard disk del server che ospita il suddetto sito, così da avere la maggior informazione possibile, come i database, i log file, le copie di backup, i codici sorgenti, ecc..
Chiaramente un'operazione simile è altamente invasiva, costosa e spesso irrealizzabile tecnicamente, si pensi ad una diffamazione su Facebook per esempio, o al fatto che acquisire un disco di un server che fa hosting implica un disservizio anche per tutti gli altri siti ospitati ed un problema di privacy ed altro ancora sui servizi e siti che

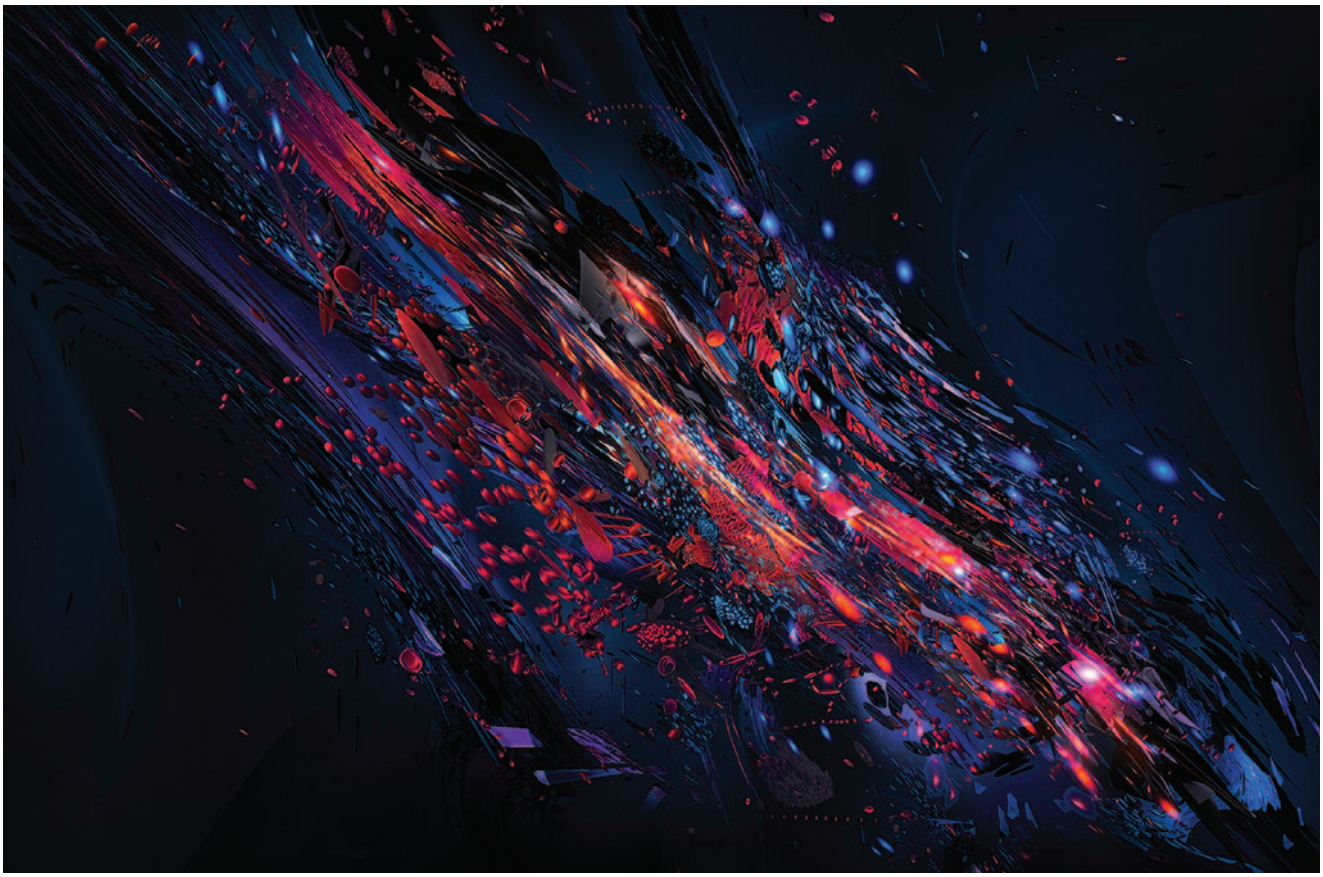
ture" effettuate con procedure software e, per creare il garante, si possono utilizzare siti d'archiviazione, come:
• archive.org
• archive.is
• freezepage.com
• hashbot.com
Questi siti inviano dei loro spider a leggere il contenuto della pagina target e provvedono ad archiviarla nei loro database, corredandola di data d'acquisizione.
Purtroppo questi servizi non funzionano sui siti che richiedono autenticazione (login e password) per esser consultati. In questi casi l'unico garante terzo sarebbe un pubblico ufficiale, per esempio un notaio, che dalla propria connessione, col proprio computer e browser, visualizzi e certifichi il contenuto nella pagina oggetto d'indagine.
Dunque, anche per l'acquisizione di un sito Internet non si possono utilizzare dei dogmi, ma ragionare sulla miglior strategia che abbia la maggior solidità scientifica, sia resistente il più possibile a contestazioni e redigere una spiegazione semplice e comprensibile.

HASH DI VERIFICA

Durante la copia forense di un hard disk viene calcolato il codice hash del supporto originale. Quando la copia termina si ottiene un file immagine rappresentante il disco copiato. Normalmente si effettua anche il calcolo dell'hash di questo file al fine di verificare se copia ed originale siano identici matematicamente.
Si potrebbe invece calcolare solo l'hash dell'originale e poi in un secondo tempo calcolare l'hash del file immagine, per ragioni di mancanza di tempo?
Anche qui si necessita di un ragionamento. In una situazione ideale il calcolo dell'hash dell'immagine, in un secondo momento, non dovrebbe comportare problemi ma, se si pensa che quest'operazione si chiama "verifica", si capisce che in quanto tale serve a verificare, appunto, quindi non vi è la certezza che "tanto l'hash sarà uguale a quello dell'originale" perché, se fosse una cosa così deterministica, non si avrebbe la necessità della verifica.
Quindi, quando si opera in questo modo, bisogna tenere in conto che la verifica in differita potrebbe non tornare e, se non sia ha più accesso al disco originale, si potrebbe essere in possesso di un file immagine non conforme, con i relativi problemi tecnico-scientifici e legali che ne comporterebbe.
Quindi, non essere dogmatici, ma sempre consapevoli di cosa possono cagionare le procedure che si adottano.

CONCLUSIONI

Si può concludere che per avere sempre delle procedure attendibili e resistenti alle contestazioni, ci si dovrà attenere al metodo scientifico, alla tracciabilità di ogni operazione compiuta, alla bibliografia ufficiale e/o affidabile, agli stru-



menti hardware e software accettati dalla comunità degli specialisti di digital forensics oppure a strumenti verificabili da terzi, se vi è una sperimentazione va documentata passo per passo sempre ai fini di verificabilità e ripetibilità.
Quindi bisogna abbracciare un concetto più largo di "best practices", dato che nel vasto panorama delle casistiche eterogenee, non si potrà mai avere sempre un elenco esaustivo che suggerisca cosa utilizzare, come e perché, ma ci si potrà trovare di fronte a dei problemi risolvibili solo con la ricerca, la sperimentazione e la costruzione di un'ipotesi e procedura.
Se si utilizzeranno metodi alternativi ai "dogmi" consolidati, si dovranno fornire tutti gli strumenti adoperati, anche quelli auto-costruiti e descrivere ogni passo effettuato e le conseguenze che possono aver arrecato sui reperti digitali.
Si deve dare sempre la possibilità a chiunque di comprendere completamente le procedure, i metodi, i software e quant'altro adottato nello svolgimento di un'operazione di digital forensics, altrimenti si genererebbero degli atti di fede dogmatica, ma i dogmi non sono scientifici. ■

SUGGERIMENTI BIBLIOGRAFICI

[1] http://www.parlamento.it/parlam/leggi/080481.htm
[2] https://it.wikipedia.org/wiki/Metodo_scientifico Open Source Digital Forensics Tools:
The Legal Argument - Brian Carrier http://home.eng.iastate.edu/~guan/course/backup/CprE-592-YG-Fall-2002/paper/atstake_open-source_forensics.pdf CERIAS Tech Report 2006-06 A HYPOTHESIS-BASED APPROACH TO DIGITAL FORENSIC INVESTIGATIONS - Brian Carrier - https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2006-06.pdf Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet - Eoghan Casey
[3] http://www.iso.org/iso/catalogue_detail?csnumber=44381
[4] SelfMonitoring, Analysis, and Reporting Technology, o S.M.A.R.T., è un sistema di monitoraggio per dischi rigidi e per SSD, per rilevare e fornire diversi indicatori di affidabilità, nella speranza di anticipare i malfunzionamenti.
https://it.wikipedia.org/wiki/Self-Monitoring,_Analysis_and_Reporting_Technology
[5] http://www.digital detective.net/digitalforensics documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf
[6] https://en.wikipedia.org/ wiki/Daubert_standard
[7] http://www.digitalevidence.org/papers/opensrc_legal.pdf Digital forensics with open source tools – C. Altheide, H. Carvery – Syngress
[8] https://www.swgde.org/documents/Current%20Documents/2014-09-05%20SWGDE%20Best%20Practices%20for%20Computer%20Forensics%20V3-1