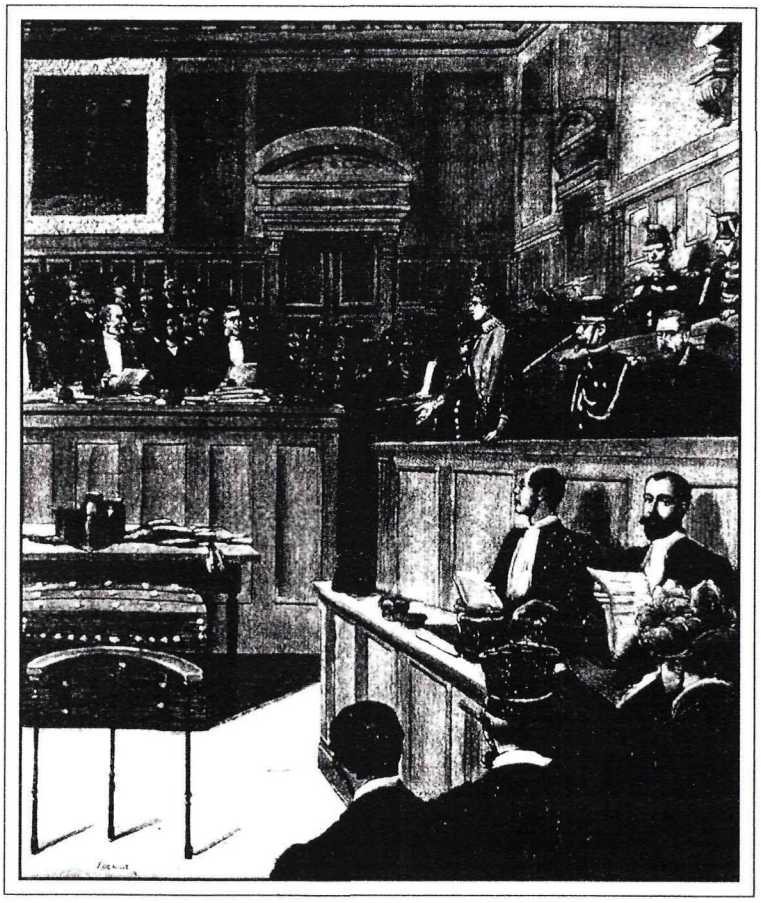
LA CORTE D'ASSISE

RIVISTA QUADRIMESTRALE
DI SCIENZE PENALISTICHE INTEGRATE



1-2/2012

Edizioni Scientifiche Italiane

La Corte d'Assise

Rivista quadrimestrale di scienze penalistiche integrate

Anno II – n. 1-2/2012

Direttore responsabile: Sergio Lorusso

Direzione scientifica: Antonio Laronga, Sostituto Procuratore della Repubblica presso il Tribunale di Foggia; Sergio Lorusso, Ordinario di Diritto processuale penale, Università di Foggia; Adelmo Manna, Ordinario di Diritto penale, Università di Foggia. **dircda@unifg.it**

La Rivista viene pubblicata con il contributo del Dipartimento delle Scienze giuridiche pubblicistiche, Università degli Studi di Foggia, fondi per la ricerca del Prof. Adelmo Manna; Camera Penale di Lucera; Centro Studi Avvocato Giovanni Scillitani; Comune di Lucera; Comune di Torremaggiore; Ordine degli Avvocati di Bari; Ordine degli Avvocati di Foggia; Ordine degli Avvocati di Lucera; Dipartimento di Scienze chirurgiche dell'Università degli Studi di Foggia.

INTRODUZIONE AL MONDO DEL *DIGITAL FORENSICS*

di Paolo Reale

1. *Introduzione*

1990. Analisi del computer utilizzato dalla vittima Simonetta Cesaroni: i consulenti tecnici della ditta fornitrice dei programmi (utilizzati su quel computer) svolsero una verifica facendo emergere che il computer aveva iniziato la sua attività alle 16:27 del 7 agosto 1990 ed era stato spento accidentalmente all'1:26 dell'8 agosto 1990, nel corso del sopralluogo di polizia giudiziaria, e proprio questo spegnimento accidentale aveva fatto sì che ci fosse ancora traccia delle attività svolte nel pomeriggio del 7 agosto, presumibilmente a partire dalle 16:27 (posto che in quei vecchi modelli di computer era l'operatore a dover indicare la data e l'ora di accensione dopo ogni spegnimento). Verso le 17:00-17:10 si era fermata poiché non riusciva ad inserire dei codici, e quindi chiamò telefonicamente per avere un aiuto. Il codice suggerito tuttavia non risultò mai inserito nel PC. In effetti fino alle 17:15 circa Simonetta era viva e stava lavorando come risulta dai riscontri telefonici[1].

Quanto sopra riportato è la più nota tra le prime effettive attività di *Digital Forensics* in Italia, ed è in sé esemplificativa della difficoltà di trattamento del dispositivo digitale (qui rintracciabile nello 'spegnimento accidentale', frutto di un'operatività improvvisata sulla scena del crimine, ma in questo caso provvidenziale), la difficoltà di ricostruire tutti i fatti avvenuti con certezza (l'orario del computer non sincronizzato in automatico), la difficoltà di interpretare i risultati (il significato del codice

[1] Vedi sentenza del proc. 399711/07 R.G.N.R., Corte di Assise di Roma, 26 gennaio 2011, 73-76.

ancora non inserito), ma soprattutto l'importanza di questo tassello nel ricomporre il quadro complessivo, inserendolo nel contesto delle altre prove raccolte.

Dal 1990 ad oggi, definire pervasive le tecnologie dell'informazione e delle telecomunicazioni (*Information and Communication Technology o ICT*), sia nell'ambito dei processi produttivi e industriali che nella vita quotidiana (attraverso l'uso di dispositivi e strumenti digitali), è un'osservazione banale ed ovvia. A tale rapidissima rivoluzione nelle abitudini quotidiane, non è corrisposta – parallelamente – analoga consapevolezza culturale su quali siano i limiti e le opportunità di queste tecnologie, spesso quasi confuse con la fantascienza, a volte guardate con sospetto, per non citare aneddoti e leggende metropolitane in cui sono considerate a livello di superstizione.

È altrettanto evidente, e per questo è un tema attualmente dibattuto, il problema del *digital divide*[2], non solo nell'accezione infrastrutturale del termine, ovvero le possibilità di accesso, ma anche nella diffusione e applicazione operativa dell'ICT nella gestione della pubblica amministrazione e nella vita del Paese, aspetto di cui si sta occupando l'Agenda Digitale Italiana recentemente istituita[3].

Necessariamente nel prossimo futuro saremo testimoni di un'evoluzione tecnologica e di un'informatizzazione capillare anche nell'amministrazione della Giustizia, con ciò non escludendo che già da qualche tempo la Giustizia civile e penale si stia confrontando con il mondo digitale attraverso la valutazione, nei procedimenti, delle evidenze provenienti da sorgenti digitali, frutto delle attività di *Digital Forensics* e delle sue diverse branche. A volte ciò avviene non senza difficoltà e contraddizioni: da un lato la ragionevole prudenza dei giuristi, che cercano di comprendere l'affidabilità e la validità di questa giovane disciplina 'al di là di ogni ragionevole dubbio', dall'altro lato i reparti scientifici della polizia giudiziaria, i consulenti e i periti, che spesso hanno operato in un contesto destrutturato, visto che solo recentemente (2008) è stato for-

[2] Il *digital divide*, o divario digitale, è il divario esistente tra chi ha accesso effettivo alle tecnologie dell'informazione (in particolare personal computer e internet) e chi ne è escluso, in modo parziale o totale. I motivi di esclusione comprendono diverse variabili: condizioni economiche, livello d'istruzione, qualità delle infrastrutture, differenze di età o di sesso, appartenenza a diversi gruppi etnici, provenienza geografica (fonte: Wikipedia).

[3] Si veda il sito istituzionale: *http://www.agenda-digitale.it/*.

malizzato e regolamentato in modo specifico l'approccio alla raccolta e gestione dell'evidenza digitale.

Sono certamente molti i temi toccati in queste poche righe che meriterebbero adeguati approfondimenti, tuttavia l'obiettivo di questo articolo è molto più semplicemente di introdurre la scienza forense denominata '*Digital Forensics*' e le sue variegate sfaccettature, coerenti con l'esteso ambito dell'ICT, attraverso: la sua storia, la sua definizione, la sua peculiare differenza rispetto alle scienze forensi cosiddette 'classiche', la descrizione dell'approccio metodologico utilizzato e le differenti ramificazioni. In particolare l'obiettivo di questo articolo è di consentire un percorso di accesso al mondo della *Digital Forensics* non già nei suoi contenuti tecnologici, ma nelle sue potenzialità quale preziosa sorgente di evidenze di interesse per il procedimento giudiziario.

2. *Scienze forensi classiche e digitali*

Le scienze forensi possono essere suddivise in base al loro 'dominio' delle prove, ovvero il dominio da cui possono essere estratte le informazioni che hanno rilevanza probatoria: per le scienze forensi 'classiche' si tratta di rilevare tracce fisiche, mentre il dominio digitale è quello dei dati, che per loro natura sono sequenze di simboli (tipicamente in codice binario, '0' e '1'), memorizzati in formati differenti e su supporti di diversa natura e caratteristiche (magnetici, ottici, etc.). La *digital evidence* è definita come «*qualsiasi informazione, con valore probatorio, che sia memorizzata o trasmessa in un formato digitale*[4]».

Le scienze forensi classiche ricercano gli elementi di prova sulla base, sostanzialmente, di due principi: 1) il principio di divisibilità della materia[5], ovvero «la materia si divide in parti più piccole quando una forza sufficiente viene applicata» e queste parti mantengono le caratteristiche fisico-chimiche della porzione da cui provengono; 2) il principio di trasferimento (di Locard), ovvero «quando due oggetti entrano in contatto, ognuno lascia sull'altro qualcosa di sé; quindi un individuo che com-

[4] Definizione fornita dal '*Scientific Working Group on Digital Evidence*', nel 1999, all'interno del documento «*Digital Evidence: Standards and Principles*», *http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm.*

[5] Cfr. K. Inmana e N. Rudinb, *The origin of evidence*, in *Forensic Science International*, 126, 2002, 12.

mette un crimine lascia qualcosa di sé sulla scena del crimine e, parallelamente, qualcosa del luogo del delitto rimane sul reo.» È utile notare che il principio di trasferimento non si riduce alla scala microscopica, ma anche a quella macroscopica, come per esempio il trasferimento di impronte, quindi dei tratti, e non solo della materia.

Proprio in virtù dei medesimi principi, l'investigatore non è un elemento privilegiato sulla scena del crimine, e come parte interagente della stessa realtà necessariamente la perturberà, seguendo a livello macroscopico il principio di indeterminazione di Heisenberg. Per questo sono indispensabili le metodologie e le procedure, perfezionate nel corso degli anni, che definiscono i protocolli di azione sulla *scena criminis* e come trattare le prove fisiche.

Può sembrare che ciò non debba valere per la prova digitale, che è immateriale, di fatto astratta, ma per ciò stesso maggiormente fragile, ovvero facilmente modificabile laddove non venga gestita in modo corretto: es. se il dispositivo che contiene le informazioni di interesse viene manipolato (anche non dolosamente, semplicemente accendendolo o spegnendolo), facendo sì che il suo contenuto originale venga perso, o alterato, in modo totale o parziale, oppure se il contenuto di interesse si trova su internet, dove può essere modificato e/o rimosso. La prova digitale è del resto 'latente' e non può essere vista nel suo stato naturale, come ad esempio il DNA, in altre parole richiede un procedimento di identificazione ed interpretazione per renderla intellegibile.

L'indagine di un dispositivo digitale è quindi molto più vicina di quanto non sembri all'investigazione sulla scena del crimine: una situazione reale può svelare molti elementi fisici (tracce di sangue, impronte, istante in cui si è svolto il crimine etc.) che possono consentire l'individuazione del responsabile, così come un dispositivo digitale, per esempio un telefonino, che di per sé è un elemento fisico, può contenere migliaia di informazioni e prove informatiche che possono consentire di identificare il responsabile di un'attività e la sequenza pregressa delle interazioni uomo-dispositivo. Peraltro la possibilità di rilevare le tracce digitali, i cosiddetti 'artefatti', prodotti dall'utilizzo del sistema informatico e/o degli applicativi, appare come un'analogia del principio di trasferimento, in cui l'utilizzatore del dispositivo 'lascia' l'impronta della sua attività. Per questo la letteratura tecnica suggerisce l'adozione degli stessi protocolli e metodi utilizzati nelle scienze forensi classiche, con gli opportuni adeguamenti, considerando il singolo PC, o dispositivo digi-

tale, come se fosse in sé e per sé una 'scena del crimine', ovviamente digitale[6]. E come quella fisica può essere facilmente contaminata, se non si adottano le opportune procedure. Si noti, incidentalmente, il fatto che il dispositivo digitale non è assimilato alla prova classica, ma alla *scena criminis* contente al suo interno tracce da interpretare ed eventualmente promuovere a prove.

La fondamentale differenza della prova digitale è che l'oggetto dell'analisi può essere reso teoricamente eterno, in quanto duplicabile perfettamente senza introdurre errori. Inoltre, in linea teorica, la manipolabilità pressoché totale di un dispositivo digitale porta alla conclusione che sia possibile costruire artificialmente una traccia digitale non generata da un'attività reale, o –per contro- l'eliminazione perfetta delle evidenze di quanto realmente accaduto all'interno del dispositivo[7].

3. *Definizione di* Digital Forensics

Una completa definizione della *Digital Forensic Science* proposta dal *Digital Forensic Research Workshop*[8] (DFRWS) è la seguente: «L'uso di metodi derivati e verificati scientificamente per la conservazione, la raccolta, la convalida, l'identificazione, l'analisi, l'interpretazione, la documentazione e la presentazione di prove digitali derivate dalle fonti digitali allo scopo di facilitare o permettere la ricostruzione degli eventi criminali, o contribuire a prevenire le azioni non autorizzate che potrebbero essere pericolose e potenzialmente distruttive rispetto alle operazioni pianificate (ndr in un sistema informativo).»

Citando quanto proposto da Ziccardi[9]: «Per *computer forensics* si intende quella scienza che studia il valore che un dato correlato a un sistema informatico o telematico può avere in ambito giuridico, o legale che dir si voglia», dove il valore eÃ inteso come la capacità di resistenza ad eventuali contestazioni e capacità di convincimento del giudice e delle parti processuali in ordine alla genuinità, non ripudiabilità, imputabilità

[6] Si veda B. Carrier e E.H. Spafford, *Getting Physical with the Digital Investigation Process*, in *International Journal of Digital Evidence*, II, 2, 2003, 5.

[7] Cfr. R. Bohme e altri, *Multimedia Forensics is not Computer Forensics*, 2009, 4.

[8] Cfr. *A Road Map for Digital Forensic Research, DFRWS Technical Report From the First Digital Forensic Research Workshop* (DFRWS), Agosto 2001.

[9] Cfr. G. Ziccardi, *Digital Forensics*, in *Informatica Giuridica*, Milano, 2008.

e integrità del dato stesso e dei fatti dallo stesso dimostrati». Si noti come viene qui utilizzato il termine *Computer forensics*, in questo caso nella medesima accezione della *Digital forensics*. Da un punto di vista più formale la prima costituisce un sottoinsieme, sostanzialmente il più importante, della *Digital forensics*, in quanto quest'ultima si riferisce in senso più esteso a tutti i contesti in cui il dato è disponibile nel formato digitale.

Il riferimento normativo italiano in cui viene coinvolta l'informatica forense è principalmente la legge 18 marzo 2008, n. 48, in ratifica alla Convenzione di Budapest del Consiglio d'Europa del 2001. Al suo interno sono contenute importanti modifiche al Codice penale, al Codice di procedura penale e al cd. Codice Privacy e sono trattati i metodi investigativi sulle *digital evidence*. Sono inoltre fornite le indicazioni metodologiche sulle procedure per la loro acquisizione, attraverso l'adozione di «misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione», e in altri casi «l'adozione di procedure che assicurino la conformità dei dati acquisiti a quelli originali e la loro immodificabilità».

Va comunque evidenziato che detto quadro legislativo, pur costituendo un fondamentale passo avanti, ancora non esaurisce i dubbi e le questioni emergenti nelle casistiche reali. A ciò si aggiunge che, da un punto di vista più strettamente tecnico, la realtà italiana non offre un riferimento riconosciuto (*best practice*) in merito alle metodologie di acquisizione, repertamento e analisi dei dispositivi digitali, per quanto siano molti gli esperti in questo campo che forniscano in rete, o tramite associazioni, pregevoli suggerimenti e indicazioni. Tutto ciò, necessariamente, non rende più agevole la comprensione ai 'non addetti ai lavori'.

4. *Principali branche della* Digital Forensics

In base a quanto precedentemente descritto, dovunque esista un dato digitale che possa avere un valore probatorio, si può parlare di DF. Tuttavia, le peculiarità dei dispositivi oggetto di analisi, o delle modalità di raccolta delle informazioni, o degli obiettivi dell'indagine, fanno sì che la DF possa articolarsi in un certo numero di branche, la cui composizione può aggiornarsi nel tempo, in base agli sviluppi della tecnologia e delle abitudini di utilizzo della stessa. Di seguito si fornirà quindi un elenco dei filoni considerati principali dallo scrivente.

5. Computer Forensics

Si tratta della principale branca della DF, anche da un punto di vista storico. Per questo non è insolito che in molti testi ed articoli i riferimenti alla CF siano in realtà intesi nella veste più ampia della DF. I primi casi in cui sono stati coinvolti i computer risalgono agli anni settanta, in prevalenza per frodi finanziarie, e nel 1978 in Florida viene emanato il primo «*Computer Crime Act*» che contempla le frodi tramite computer e le intrusioni telematiche, a cui fanno seguito altre leggi (negli Stati Uniti) per l'estensione ai reati legati al *copyright*, la *privacy* e la pornografia minorile.

A partire dagli anni ottanta cresce la consapevolezza che per alcuni crimini le evidenze possano essere trovate solo sui computer, e vengono quindi attuati dei programmi di formazione di gruppi specializzati, appartenenti alle forze dell'ordine (USA). Negli anni novanta si formano le prime organizzazioni internazionali, per definire e sviluppare metodi e strumenti utili alle investigazioni, e –sebbene informalmente già utilizzata- la locuzione CF compare anche in ambito accademico[10].

A partire dal 2000 emerge in modo prepotente la necessità di definire standard, linee guida, regole e procedure, al fine di conseguire un livello di attendibilità adeguato ad un'aula di tribunale, attraverso una forte interazione con ricercatori accademici, operatori del campo, ed esperti legali[11]. Il Dipartimento di Giustizia americano ha dunque pubblicato diverse guide, destinate prevalentemente alle forze dell'ordine, per l'analisi forense delle prove digitali e per la salvaguardia della scena del crimine digitale, mettendo anche a disposizione strumenti specifici[12].

L'analisi del computer può seguire finalità investigative differenti in funzione del «ruolo» assunto dal computer stesso, in quanto può costituire parte «attiva» dell'azione criminale, ed è quindi uno *strumento* (es. un'intrusione nelle reti di computer), oppure «passiva» in quanto è l'*oggetto*, l'obiettivo degli atti criminali (es. alterazione o distruzione di con-

[10] Cfr. P.A.Collier e B.J. Spaul, *A forensic methodology for countering computer crime*, *Computers and Law* (Intellect Books), 1992.

[11] Cfr. G.L. Palmer, *Forensic Analysis in the Digital World*, *International Journal of Digital Evidence*, 2002, 6.

[12] Si veda il sito nel National Institute of Justice: *http://www.nij.gov/topics/forensics/evidence/digital/welcome.htm*

tenuti, spionaggio), infine può essere semplicemente il contenitore delle prove, quindi *soggetto* (es. pirateria *software*, pornografia minorile).

6. Mobile Forensics

La MF si occupa dell'analisi dei dispositivi mobili: più precisamente si divide nella SIM *card forensics*, in cui l'oggetto analizzato è il contenuto della scheda SIM, *Mobile Handset Forensics* (citata anche come *Cell Phones Forensics*), in cui l'oggetto analizzato è il contenuto del dispositivo mobile (Mobile Equipment, o ME), e la *Memory Card Forensics* (anche *Removable Media Forensics*), in cui l'oggetto analizzato, con tecniche del tutto analoghe a quelle adottate nella CF, è la memoria su scheda utilizzata dal cellulare come spazio di memorizzazione.

È sempre piuttosto elevata l'attenzione posta dalla Polizia giudiziaria sui dispositivi mobili, in quanto preziosissime fonti di informazione. Ciò deriva non solo dalla loro impressionante diffusione, ma anche dalle caratteristiche dei terminali di ultima generazione, i cosiddetti '*smartphone*', evoluti in termini di funzionalità, perfettamente integrati con internet e con i suoi servizi (posta elettronica, *social network*, etc.)

Anche se non rientrano strettamente nell'abito della DF, è comunque opportuno menzionare, in correlazione con i terminali mobili, la *Cellsite Analysis*, che studia come utilizzare le informazioni, tracciate dall'operatore di rete mobile, allo scopo di individuare la posizione (in senso probabilistico) di un cellulare in un dato momento («a posteriori» rispetto all'evento), e l'analisi dei tabulati di traffico telefonico.

7. Network Forensics

Questa branca di DF, per ragioni storiche spesso accomunata alla CF, ha anche molti elementi in comune con la sicurezza informatica. Del resto la definizione comunemente accettata, ovvero «il prelievo, la memorizzazione e l'analisi degli eventi di rete al fine di identificare la sorgente degli attacchi alla sicurezza o l'origine di altri problemi del sistema di rete[13]» si presta certamente ad una doppia interpretazione.

[13] Cfr. M. Ranum, *Network Forensics and Traffic Monitoring*, in *Computer Security Journal*, Vol. XII, 2 novembre 1997.

La linea di demarcazione, suggerita da Ziccardi, è che «se al centro dell'attenzione c'è la sicurezza del sistema e il suo buon funzionamento ci si trova nel campo della security», altrimenti se il presupposto è la «consapevolezza che il dato raccolto è destinato ad un contesto non informatico ma giuridico[14]» allora si è in presenza della disciplina forense.

In estrema sintesi, una rete di calcolatori è una struttura composta da nodi (es. computer, *switch*, etc.), collegati tra di loro secondo topologie articolate, in cui le informazioni transitano seguendo percorsi differenti, tra sorgenti e destinatari diversi (a volte anche senza raggiungersi). Si tratta dunque di un ambiente distribuito che varia col tempo in modo fortemente dinamico, scambiando notevoli quantità di dati. Già intuitivamente si può comprendere la difficoltà tecnica legata all'acquisizione, ovvero la 'cristallizzazione' della prova: nella maggior parte dei casi le macchine non possono neppure essere spente, pena il malfunzionamento della rete complessiva. Anche per l'attuale tendenza evolutiva del mercato informatico, che sta muovendosi verso soluzioni applicative, dei servizi e di memorizzazione dei dati distribuite in rete (*cloud computing*), la NF è certamente una delle branche più complesse e sfidanti della *Digital forensics*.

8. Multimedia Forensics

La nostra epoca è certamente caratterizzata dalla multimedialità, in cui immagini e video hanno una grande importanza, tuttavia fino a poco tempo fa attribuivamo un certo grado di fiducia all'integrità di queste rappresentazioni: la tecnologia digitale ha necessariamente eroso questa fiducia[15].

La *Multimedia forensic* si distingue[16] in modo netto dalle altre branche della DF, poiché opera su oggetti che sono rappresentazioni digitali di oggetti reali (es. immagini, video), la cui costruzione si avvale della presenza di sensori, i quali – a loro volta – introducono un ulteriore grado di complessità (e di alterazione). A ciò deve aggiungersi la semplicità con cui è possibile oggi la manipolazione di queste rappresenta-

[14] Cfr. G. Ziccardi, *Informatica Giuridica*, cit., 318.

[15] Cfr. H. Farid, *Image Forgery Detection-A survey*, in *Ieee Signal Processing Magazine*, 2009.

[16] Cfr. R. Bohme *et alii*, *Multimedia Forensics is not Computer Forensics*, 2009.

zioni digitali, attraverso *software* accessibili che consentono di ottenere risultati di elevata qualità con minimo sforzo.

L'obiettivo principale della *Multimedia Forensics* non è quello di analizzare la semantica dei contenuti digitali, ma quello di verificare l'autenticità e la provenienza delle evidenze: es. 1) determinare se una specifica immagine è stata oggetto di contraffazione e 2) determinare se è stata ripresa con uno specifico dispositivo.

9. Embedded System Forensics

A causa dell'estrema diversificazione degli apparati analizzati, l'*Embedded System Forensics* non ha una sua dimensione ben circostanziata come le altre sopra citate: questa branca si occupa di affrontare l'analisi forense dei sistemi digitali non classificabili nelle precedenti categorie. Sono infatti sempre più numerosi gli strumenti digitali specializzati per le più diverse attività e per il fatto che possono contenere dati e informazioni, anche storiche (ovvero potenziali tracce), meritano l'interesse degli investigatori. Parliamo quindi di analisi delle *gamebox* (PS3, Xbox, etc.), dei computer per immersioni subacquee, delle centraline per la gestione degli allarmi, dei dispositivi per la riproduzione musicale mp3 (*ipod*, etc.), delle 'scatole nere' che registrano i dati di navigazione (aerea, navale, etc.), e così via.

La difficoltà di questi sistemi è generalmente l'elevato livello di 'personalizzazione' del prodotto, per cui non è agevole trovare disponibilità di informazioni in merito al funzionamento, alle modalità di gestione dei dati, e alle possibilità di interfacciamento che consentano di non alterare il dato originale.

10. *L'errore nella* digital forensics

Per le nuove prove scientifiche, negli Stati Uniti viene adottato lo standard definito dalla sentenza 'Daubert', in cui il giudice deve valutare criticamente l'affidabilità dei metodi e delle procedure adottate dall'esperto, rispetto a: *a)* l'accettazione da parte degli studiosi della materia; *b)* il grado di controllabilità o falsificabilità del metodo scientifico; *c)* l'indicazione da parte del perito del margine di errore conosciuto nel caso di specie: cioè qual è il grado di probabilità della prova.

In particolare, per l'ultimo punto, va ricordato che le scienze forensi classiche adottano comunemente – nel contesto giuridico – la valutazione del 'rapporto di verosimiglianza', che esprime in modo efficace il livello di fiducia[17], in senso probabilistico, della prova scientifica: detto rapporto si misura con il supporto dell'approccio statistico bayesiano[18] (*inferenza bayesiana*).

Nelle indagini sulle prove digitali non è, purtroppo, prassi adottata quella di esprimere un indice di errore, in alcuni casi non viene neppure presa in considerazione la dizione 'ipotesi' quando sarebbe opportuno farlo. È infatti inevitabile che sussista sempre un relativo grado di errore: es. la corretta sincronizzazione degli eventi temporali, la mancanza di dati (persi e/o non ricostruibili) può dare una rappresentazione incompleta di quanto accaduto, o peggio fuorviante. Addirittura, come in precedenza affermato, è possibile che un'informazione digitale sia stata prodotta artificialmente, appositamente per depistare gli investigatori[19].

L'applicazione rigorosa del metodo scientifico può comunque ridurre i possibili errori nell'analisi e nell'interpretazione: è fondamentale quindi che l'esperto forense adotti il principio di falsificabilità, esplorando sempre tutte le ipotesi possibili in modo da poterle eventualmente eliminare, e rispondendo a tutte le domande, in modo da sviluppare una teoria che possa spiegare ogni elemento rilevato.

Non può essere sottovalutato neppure il fatto che ogni sistema operativo, o applicativo, presenti delle falle, o degli errori, in alcuni casi introdotti anche volontariamente dai programmatori, così come nei sistemi complessi certe peculiari situazioni possono determinare risultati imprevisti, che possono portare anche a comportamenti anomali (i.e.: non documentati) del sistema, dipendenti dalla sua particolare configurazione e dalle specifiche versioni del software ivi installato, sino ad arrivare alla perdita dei dati o a catastrofici *crash*[20]. Per quanto complesso nella realtà investigativa, in un approccio ideale deve sempre essere tenuta in considerazione l'affidabilità e la ripetibilità del sistema, e del processo, che genera i dati analizzati.

[17] Per esempio «*si valuta che l'ipotesi accusatoria sia un milione di volte più verosimile di quella difensiva*».

[18] Si veda P. Agnoli, *Il teorema di Bayes: una introduzione critica*, 2002.

[19] Si veda E. Casey, *Error, Uncertainty, and Loss in Digital Evidence*, in *International Journal of Digital Evidence*, I, 2, 2002.

[20] Si veda sempre E. Casey, *Error, Uncertainty, and Loss in Digital Evidence*, cit.

11. *Conclusioni*

Il progresso tecnologico che coinvolge complessivamente l'ICT è caratterizzato da elevata velocità di cambiamento, rilevante impatto sulle abitudini di vita, elevata numerosità dei dispositivi, enorme capacità di memorizzazione delle informazioni, e tutto ciò si riflette inevitabilmente come difficoltà per chi deve acquisire, preservare, analizzare, interpretare e presentare i risultati dell'indagine scientifica svolta sugli apparati digitali.

Oltre a quanto sopra descritto, occorre evidenziare che a condizionare lo sviluppo e la corretta percezione dell'importanza della DF, insieme alle altre scienze forensi di recente sviluppo, ci sono fattori legati alle regole stesse del procedimento giudiziario, in cui, per esempio la stessa figura dell'esperto forense manca, in Italia, di una precisa caratterizzazione formale, così come si dibatte, attualmente, sul contraddittorio tecnico, in tema di perizie. A tutto ciò si aggiunge l'oggettiva difficoltà intrinseca delle materie tecniche, che devono trovare posto nell'ambito di un procedimento giuridico in modo 'semplice', e comprensibile, operazione non agevole e dai risultati a volte opposti.

Il percorso seguito da questa introduzione alla *Digital Forensic Science*, evidentemente non esaustivo di tutti i suoi contenuti, fornisce comunque gli elementi necessari a comprendere l'importanza e la complessità di questa disciplina in continua evoluzione sui suoi diversi fronti.

giudice: «[...] voi siete professori universitari, fate convegni, fate siti protetti e mandate le cose ai Consulenti Tecnici di Parte, ovviamente è tutto un modo giustissimo ed efficientissimo di fare. Noi purtroppo siamo nella giustizia italiana, che si basa a parte su regole formali e poi si basa ancora prevalentemente sul cartaceo. [...] forse noi fra 300 anni ci arriveremo, però tenete presente che noi siamo in un processo che si basa anche sul cartaceo [...] se avete tabelle riassuntive, se ce la buttate sul cartaceo, lo so siamo nella preistoria, però noi preistorici abbiamo bisogno anche del cartaceo»[21].

Abstract

Il presente lavoro introduce la scienza forense denominata '*Digital Forensics*' e le sue variegate sfaccettature, coerenti con l'esteso ambito dell'ICT, at-

[21] Verbale di Udienza, 2009.

traverso: la sua storia, la sua definizione, la sua peculiare differenza rispetto alle scienze forensi cosiddette 'classiche', la descrizione dell'approccio metodologico utilizzato e le differenti ramificazioni. In particolare l'obiettivo di questo articolo è di consentire un percorso di accesso al mondo della *Digital Forensics* non già nei suoi contenuti tecnologici, ma nelle sue potenzialità quale preziosa sorgente di evidenze di interesse per il procedimento giudiziario.

This work introduces forensic science called 'Digital Forensics' and its various facets, consistent with the extensive field of ICT, through: its history, its definition, its distinctive difference from the forensic science so-called 'classical', the description of the methodology used and the different branches. In particular, the objective of this paper is to provide an access path to the world of Digital Forensics is not already in its content and technology, but in its potential as a valuable source of evidence relevant to the proceedings.