

Le indagini sui Reperti Virtuali “Digital Forensics”

Ing. Marco Mattiucci¹ - Anno 2011

1. Premessa

I computer, le reti di computer, Internet, gli embedded system (cellulari, smartphone, iPod, iPad, ecc.) e qualsiasi sistema di gestione automatica dei dati ad oggi in uso rappresentano, da un lato, una grande e rinnovata opportunità per le attività criminali e dall'altro, una insostituibile fonte di informazioni utili alle indagini di polizia giudiziaria. I tradizionali crimini come traffici illeciti, frodi, attentati, omicidi, ecc. vedono sempre più spesso la presenza di *"fonti di prova elettroniche e/o informatiche"* imprescindibili sia durante lo svolgimento delle indagini che in fase di dibattimento.

Lo scenario italiano vede tutte le FFPP (Forze di Polizia) affrontare un crescente volume di indagini che si riferiscono a sistemi elettronici digitali e ciò sta mettendo a dura prova le rispettive capacità di reazione agli aggiornamenti tecnologici. Gli stessi consulenti e periti privati che operano in dibattimento si sono federati in organizzazioni (es. IISFA²) al fine di ottenere una indispensabile circolarità informativa nel settore. Per finire, a livello internazionale un congruo numero di grandi comunità scientifiche e di polizia sta operando alacremente sempre nella stessa direzione (IOCE³, SWGDE⁴, ASCLD⁵, ENFSI-FIT-WG⁶, ISO-IEC⁷).

¹ <http://www.marcomattiucci.it>

² Italian Chapter of the International Information Systems Forensics Association <http://www.iisfa.it>

³ International Organization on Computer Evidence <http://www.ioce.org>

⁴ The Scientific Working Group on Digital Evidence <http://www.swgde.org/>

⁵ The American Society of Crime Laboratory Directors
<http://www.asclد.org/>

⁶ European Network of Forensic Science Institutes – Forensic Information Technology Working Group <http://www.enfsi.org>

Questo capitolo tenta di affrontare il citato problema dell'aggiornamento tecnico in questo delicato settore, anche in relazione alla scena del crimine dal punto di vista informatico ed elettronico. È evidente che a seguito della natura fortemente dinamica ed evolutiva della tecnologia digitale questo testo è soggetto a rapida obsolescenza.

2. Passato, Presente e Futuro possibile per la Digital Forensics

La DF (**Digital Forensics**) è una materia nata, in forma differente dalla presente, circa 40 anni or sono. È partita dalla “*computer forensics*” che si occupava prettamente di recupero dei dati persi o cancellati da file, data base, ecc.. Lo sforzo centrale è stato quello di adattare tali attività di recupero agli aspetti legali e quindi alla desiderata completa ripetibilità.

Gli anni **dal 1999 al 2007** si possono considerare come l’era in cui il DF è emerso con le sue enormi potenzialità [1]. Sono state, infatti, sviluppate tecniche, tool e teorie che hanno consentito di estrarre dati da sistemi digitali di incredibile importanza per le indagini ed in molti casi determinanti ai fini della colpevolezza degli indagati. In questo periodo le indagini dalle memorie di massa si sono allargate ad Internet e cellulari con numeri di grani proporzioni in ogni area del globo.

Dal 2008 ad oggi, il settore del DF ha continuato a guadagnare terreno fino a toccare punti di saturazione che dovranno essere affrontati dalla ricerca pena una difficoltà insormontabile nelle indagini. Il **futuro del DF**, infatti è verso i sistemi cloud⁸, verso memorie digitali di grandezze insperabili fino a qualche tempo fa, verso reti ad alta velocità, wireless e mobile, con protocolli sempre più performanti e sofisticati, verso forme di protezioni dei dati praticamente inattaccabili (crittazione forte).

Le frontiere della ricerca attuali inerenti il DF sono costituite da:

⁷ International Organization for Standardization - International Electrotechnical Commission <http://www.iso.org> - ISO/IEC CD 27037 “*Information technology -- Security techniques -- Guidelines for identification, collection, acquisition and preservation of digital evidence*”

⁸ Un “Cloud-System” è “*un insieme di tecnologie che permettono sia di memorizzare/archiviare dati che di elaborarli (con CPU o software) tramite l'utilizzo di risorse distribuite e virtualizzate in rete*” - http://it.wikipedia.org/wiki/Cloud_computing

- sviluppo di metodi e strumenti di investigazione che consentano di agire sul posto ed “a caldo” ossia su reperti ancora attivi durante o appena dopo il reato;
- realizzazione di strumenti di indagine tecnica che consentano non solo l’analisi (com’è vero attualmente) ma anche la correlazione tra i risultati delle analisi di reperti sostanzialmente diversi (cellulari, siti web, email, pc, log, ecc.);
- sviluppo di potenti reti di collegamento tra fondazioni, istituti privati e di polizia, università e centri di ricerca al fine di tenere allineato lo stato dell’arte su quello che è realmente possibile o meno in questo ambito di indagini⁹.

In definitiva uno degli elementi fondamentali che la ricerca dovrebbe introdurre è un set di standard a livello procedurale, strumentale ed addestrativo in grado di far interagire risorse provenienti da diverse realtà. Ad oggi questo è praticamente impossibile, ad esempio impiegare tool di diverse ditte in maniera integrata non a svolgere la stessa attività ma nel concorrere a risolvere lo stesso problema. Nello stesso modo ogni realtà operativa nel DF impiega personale con preparazione culturale veramente differente non esistendo una certificazione di natura universalmente accettata (o legalmente obbligata) nel settore.

3. La Digital Forensics in Italia

Sebbene l’attività tecnica tipica della DF abbia una tradizione consolidata di diversi decenni, la scienza della DF è da ritenersi di recente costituzione. Si trovano infatti, in ambito accademico, ancora variegata definizioni della stessa. Per completezza ed autorevolezza delle fonti definitorie a livello internazionale verrà, in questo lavoro, considerata la seguente: “*...the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal or helping to anticipate unauthorized actions...*” [2]. Una breve analisi di questa definizione è necessaria,

⁹ Il “CSI effect” [4] ha creato anche in professionisti (magistrati, FFPP, ecc.) delle aspettative enormi sulle possibilità del DF, talvolta anche di natura irreali. Quindi anche il solo conoscere cosa il DF può realmente fare allo stato dell’arte attuale è divenuto un elemento di fondamentale importanza.

soprattutto per chiarificare quale sia la situazione in Italia a riguardo di questo delicato settore.

Sembra scontato che si debbano impiegare **“metodi scientificamente derivati”** per svolgere esami di apparecchiature elettroniche digitali ma per anni (e forse molte volte ancora oggi) l’esperienza personale del consulente tecnico o perito ha (propriamente o impropriamente) sostituito l’applicazione di metodologie rigorose sia per la difficoltà che si ha nel settore informatico di delimitare i casi di studio che per la pretesa competenza dello stesso operatore (spesso solo auto-certificata).

In relazione al discorso che i **“metodi”** debbano essere **“provati, ossia dimostrati come scientificamente validi”** la situazione peggiora. Più studi del NIST¹⁰ hanno purtroppo dimostrato la quasi impossibilità di testare esaustivamente metodi e strumenti per le indagini tecniche elettronico/digitali. Va sottolineato comunque che il NIST si è sforzato di emanare diverse decine di documenti ufficiali sulle prove tecniche svolte al fine di creare dei riferimenti per gli specialisti nel settore.

Le **“fasi”** che, nella definizione, formano il DF sono: l’identificazione delle possibili fonti di prova elettronico/digitali (siano essi hardware o dati), la raccolta di tali fonti, la loro validazione tecnica e formale, la loro preservazione e protezione in fase di chiusura e sigillo, trasporto e successiva eventuale riapertura in laboratorio, l’analisi approfondita di laboratorio di quelli che ora possono chiamarsi reperti, la ricostruzione degli eventi investigativi tramite la scrittura di un referto giudiziario. In tutto questo **la fase di documentazione delle attività è fortemente trasversale** dovendo insinuarsi in ogni momento al fine di rendere il massimo delle attendibilità e delle garanzie nonché di determinare un’inattaccabile catena di custodia. Vi è infine da considerare l’ultima ma determinante fase della **“presentazione dibattimentale”** dei risultati ed anche quindi del referto.

È interessante notare come nella definizione la DF si occupi sempre e solo di attività **POST-MORTEM** ossia di azioni che si svolgono solo dopo che vi è stata una precisa notizia di reato. Talvolta si confondono digital forensics e digital investigation (prima, durante e dopo il fatto) per i tool impiegati. Questo fatto è non positivo se si pensa che i poteri legali delle due attività sono spesso sostanzialmente differenti.

¹⁰ National Institute of Standards and Technology (<http://www.nist.org>)

4. La Legge 48/2008 e la DF

La Legge 18 marzo 2008 n. 48 reca la ratifica della Convenzione del Consiglio d'Europa di Budapest sulla criminalità informatica del 23 novembre 2001. Seppur con un certo ritardo rispetto alle direttive europee ed a quanto attuato da diversi altri Paesi membri, il legislatore è intervenuto sul Codice Penale, sul Codice di Procedura Penale e sulla Legge sulla Privacy in relazione agli aspetti informatici. Elemento centrale della L.48/2008 è l'insieme delle modifiche del codice di procedura penale per quanto riguarda l'acquisizione delle fonti di prova da sistemi elettronici digitali, ossia proprio l'argomento di questo lavoro. Non si può quindi prescindere dallo studio (non certamente esaustivo ma pratico/operativo) di tali cambiamenti, questo anche considerando che il codice di procedura penale non aveva subito il benchè minimo allineamento alle innovazioni dell'informatica e telematica prima della L.48/2008; per cui il trattamento e reperimento di fonti di prova da sistemi digitali veniva trattato alla stregua delle altre fonti di prova scientifica. Questo in linea di massima potrebbe anche essere accettabile se non fosse che i sistemi digitali sono talmente pervasivi da aver determinato veri e propri nuovi metodi di indagine e nuove realtà con cui confrontarsi, spesso in concorrenza o sovrapposte alla realtà "reale".

La possibile virtualizzazione delle indagini in ambienti "non reali", intesi come ***"ambienti che esistono in ambito software ed hardware"*** è il centro dell'innovazione presentata dalla L.48/2008 per quanto riguarda il presente studio.

Modifica al C.P.P.	Commento
Art. 244 C.P.P. Casi e forme delle ispezioni vede inserita la <i>"...anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione."</i>	Ispezionare un sistema informatico o telematico è la realizzazione di quella che si può chiamare un' ispezione virtuale . "Persone, luoghi e cose" sono normalmente l'obiettivo dell'ispezione, ma ora si aggiunge l'ambiente determinato da un sistema software/hardware. L'ispezione virtuale dipende dal sistema e dalle possibilità di comprensione ed interpretazione di colui che ispeziona, ad ogni modo deve rimanere assolutamente <i>"non invasiva"</i> .

Modifica al C.P.P.	Commento
<p><i>Art. 247 C.P.P. Casi e forme delle perquisizioni vede l'inserimento di un intero comma: "1-bis. Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione."</i></p>	<p>Si definisce l'esistenza della perquisizione virtuale in maniera equivalente a quanto visto per l'ispezione.</p> <p>La perquisizione come tale può risultare anche parzialmente invasiva e questo si evidenzia parzialmente nel "<i>ancorché protetto da misure di sicurezza</i>".</p> <p>Sorvolando sulle problematiche che tale dicitura apre a livello legale è bene comprendere che ciò nonostante il comma termina con la solita indicazione "<i>adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione</i>".</p>

L'Art. 247 opera sulle "cose", mentre dal comma 1-bis, che la L. 48/2008 introduce, si nota che **la cosa pertinente il reato è invece un dato o un'informazione**¹¹ (che notoriamente NON sono cose!), anche magari nascosta in un sistema informatico/telematico (es. crittata) o protetta da password (in quello che è definito legalmente "domicilio informatico"). Anche questa attività è disposta con decreto motivato dell'Autorità Giudiziaria. Interessante è vedere i riflessi di questa modifica. Dato che la perquisizione è prodromica al sequestro e visto che si configura come un'azione di ricerca di informazioni utili anche in presenza di barriere di protezione, il sequestro che ne consegue non può che essere una copia di dati digitali¹² che determineranno quindi un **sequestro virtuale**.

¹¹ Questa è una palese contraddizione se si pensa che un dato informatico può al massimo essere assimilato ad un'informazione ma mai certamente ad una cosa.

¹² Più precisamente (ma questo non è stato approfondito dalla L.48/2008) la copia, per costituire sequestro di dati o sequestro virtuale dovrebbe essere "**forense**", ossia, secondo lo standard internazionale, dare garanzia di

Modifica al C.P.P.	Commento
<p>Art. 352 C.P.P. Perquisizioni, tratta la flagranza di reato e vede il comma aggiuntivo: <i>“1-bis. Nella flagranza del reato, ovvero nei casi di cui al comma 2 quando sussistono i presupposti e le altre condizioni ivi previsti, gli ufficiali di polizia giudiziaria, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l’alterazione, procedono altresì alla perquisizione di sistemi informatici o telematici, ancorché protetti da misure di sicurezza, quando hanno fondato motivo di ritenere che in questi si trovino occultati dati, informazioni, programmi informatici o tracce comunque pertinenti al reato che possono essere cancellati o dispersi.”</i></p>	<p>Si tratta della perquisizione virtuale in flagranza di reato. È bene in questo caso evidenziare il concetto di necessità dello svolgimento dell’attività espresso dalla postilla <i>“...tracce comunque pertinenti al reato che possono essere cancellati o dispersi”</i> (tale aspetto va spiegato e giustificato in un eventuale verbale di attività). Si noti poi che la responsabilità è della Polizia Giudiziaria che procede alla perquisizione dei sistemi informatici non supportata necessariamente da ausiliari tecnici e/o da consulenti tecnici. L’Autorità Giudiziaria non è menzionata in quanto il Pubblico Ministero non ha ancora assunto la direzione delle indagini, la responsabilità è degli investigatori classici, non necessariamente competenti in informatica, che si trovano a gestire la scena.</p>

La perquisizione virtuale in flagranza di reato ed il conseguente sequestro (copia forense) che ne può discendere (per improrogabile necessità) è una delle maggiori ragioni d’essere dell’esistenza di un preciso protocollo operativo cui gli investigatori non specialisti debbano almeno potersi riferire in queste attività d’urgenza.

autenticità sia a livello tecnico (con funzioni matematiche come hash, CRC, ecc.) che legale (presenza di appositi verbali).

Modifica al C.P.P.	Commento
<p>Art. 354 C.P.P. Accertamenti urgenti sui luoghi, sulle cose e sulle persone. Sequestro. Specifica l'impiego della copia quale strumento per effettuare un sequestro virtuale. È introdotta infatti la: “ <i>In relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, gli ufficiali della polizia giudiziaria adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità...</i> ”</p>	<p>Viene definita la copia (in senso generale e non forense) come sequestro virtuale “urgente”. L'urgenza è elemento centrale dell'articolo e vi è da dire che essa è ben acclarabile per i sistemi digitali, tanta è la criticità della loro possibilità di mantenere memorizzate le informazioni in maniera integra. Esso si rivolge alla Polizia Giudiziaria e la “<i>protegge</i>” consentendo anche direttamente una copia di dati evitando di repertare il dispositivo fisico che li contiene (fatto questo che nei prossimi anni dovrà divenire uno standard).</p>

È bene riflettere sul fatto che la **copia forense “sul posto” è un'operazione tecnica talvolta critica che taluni considerano un vero e proprio accertamento tecnico.**

Sequestro Fisico	Sequestro Virtuale
Agisce sull'oggetto fisico	Agisce sui dati informatici
L'oggetto viene sigillato e prelevato	Il dato viene copiato con garanzie
Equivale a privarne la disponibilità	Non equivale a privarne la disponibilità
Avviene in un ambiente fisico	Avviene su un software o hardware

Precauzioni per coloro che svolgono un sequestro virtuale in condizioni di urgenza:

- Quando viene effettuata la copia/sequestro è sostanziale **riportare dettagliatamente** tutto quanto svolto mediante verbale (magari anche coadiuvato da riprese video);
- Tenere presente che qualsiasi tipo di copia, anche se non perfettamente forense, in condizioni di (a) **urgenza** e (b) scrivendo sul verbale la frase ***“nei limiti delle conoscenze tecniche di chi opera, non potendo fare altrimenti pena la perdita definitiva della fonte”***, diviene accettabile alla luce della L.48/2008.

Data l'intrinseca irripetibilità dell'operazione dell'accertamento urgente svolto tramite la copia¹³, ciò che si ottiene dalla copia è a tutti gli effetti un **reperto virtuale**. Esso ha un valore che prescinde dall'originale ed anche dal supporto che lo conteneva e da quello che lo contiene.

Reperto Fisico Sequestrato	Reperto Virtuale Sequestrato
È un pacco sigillato	È un file sigillato elettronicamente
Non dipende dal suo imballo o sigillo	Non deve dipendere dal contenitore
L'imballo è fisico come il reperto	L'imballo è generalmente una memoria digitale (es. hard disk) quindi un oggetto fisico ma il reperto è immateriale perché è un file registrato al suo interno
Aprire l'imballo è un'operazione fisica di apertura sigilli	Per riavere il reperto virtuale è necessario copiare il file dal suo contenitore al momento del deposito, aprirlo con password se presente, decompattarlo se necessario, ecc.

¹³ L'irripetibilità dell'accertamento considerato (copia) non è tecnico ma è dovuto ad una serie di circostanze tecnico/legali. Fermo restando che la copia forense sia perfettamente ripetibile da un punto di vista tecnico, essa rimane infatti tale solo fino a quando il reperto fisico non viene ridato nelle disponibilità di un qualsiasi utente non esperto di DF.

5. Gli Standard Internazionali di riferimento

Questo lavoro si fonda su un'esperienza plurinennale in ambito di DF ma soprattutto su documenti internazionali nel settore di provato affidamento. In particolare si considerano:

- La ISO/IEC 27037 (*"Guidelines for identification, collection, acquisition, and preservation of digital evidence"*) in tutte le sue release tranne quella di pubblicazione definitiva in quanto dovrebbe avvenire tra il 2011 ed il 2012;
- La *"Guidelines for Best Practice in the Forensic Examination of Digital Technology"* prodotta dall'ENFSI-FIT-WG (v.6 2009);
- La *"Good Practice Guide for Computer-Based Electronic Evidence"* della ACPO (2011);
- La *"Best Practices for Seizing Computer evidence"* del U.S. Secret Service (2011);
- Il *"Model Standard Operating Procedures for computer forensics"* della SWGDE (2011).

I seguenti **4 principi** segnalati nei più autorevoli testi di DF e nella quasi totalità dei documenti precedenti, devono essere il punto di partenza di qualsiasi attività di sopralluogo e repertamento sulla scena del crimine in relazione a sistemi hardware o software digitali:

Nessuna azione deve essere svolta che possa cambiare dei dati direttamente o indirettamente e che possa successivamente essere segnalata come invalidante della fonte di prova in dibattimento
I dati sulla scena non dovrebbero mai essere acceduti direttamente ma se questo si rende indispensabile, pena la loro perdita definitiva, chi vi accede deve possedere la competenza tecnica e legale necessaria a spiegare in dettaglio i passi che ha svolto
Tutte le azioni sulla scena del crimine devono essere documentate . Nella migliore delle ipotesi una terza parte indipendente dovrebbe essere in grado non solo di valutarle ma anche di ripeterle con i medesimi risultati
Colui che è incaricato delle indagini è anche responsabile per il rispetto dei precedenti tre principi.

Queste considerazioni costituiscono di fatto l'idealità massima di intervento sulla scena del crimine per un esperto di DF. Che siano sempre rispettabili è utopia ma che debbano sempre essere tenuti presenti per evitare errori eclatanti è determinante.

Un altro elemento in comune tra i documenti precedenti la seguente coppia di definizioni:

Digital Evidence First Responder (DEFR): la persona fisica o il team autorizzato e qualificato ad agire per primo sulla scena del crimine in relazione alla raccolta ed eventuale acquisizione di fonti di prova elettroniche e digitali

Digital Evidence Specialist (DES): la persona fisica o il team che oltre a poter eseguire la funzione di DEFR ha conoscenze tecniche e legali nel DF di natura superiore che può consentirgli di svolgere l'intera sequenza di lavoro sui reperti digitali, dal repertamento all'analisi e refertazione

In relazione al DEFR, in Italia attualmente è possibile al massimo parlare del **first responder**, inteso come l'ufficiale di polizia giudiziaria e/o altro funzionario di pubblica sicurezza (con al massimo degli ausiliari) che arriva per primo sul luogo del reato. Questi nel migliore dei casi ha conoscenze di intervento forense generalizzato. Il DES italiano è il consulente specialista che il più delle volte prende in consegna dei reperti già prelevati ed imballati per svolgere soprattutto l'operazione di analisi e refertazione nonché spesso la presentazione dibattimentale.

Il presente lavoro si occupa soprattutto di definire e regolare l'operato del DEFR mentre è lasciato a successivi sviluppi di natura altamente tecnica la creazione di procedure per il DES. Il DEFR opera in un ambiente per definizione non protetto e non preparato, dal punto di vista tecnico si può sicuramente affermare che, in tal senso, **la scena del crimine si deve considerare come un'area non di laboratorio** per cui ad essa non possono essere applicati gli stessi protocolli dell'analisi forense di laboratorio. In generale quindi si vanno qui a studiare le **SOP¹⁴ sulla scena del crimine** relative alle fonti di prova digitali e non quelle interne al laboratorio o agenzia forense.

6. Ciclo di vita di un reperto digitale (hardware/software)

Le *"prove elettroniche"*¹⁵ sono sostanzialmente dati o informazioni memorizzate in un dispositivo elettronico di interesse per il caso investigativo. Le "prove elettroniche" non sono evidenti, nel senso che non si possono acquisire tramite la semplice osservazione visiva, ma possono

¹⁴ Standard Operating Procedure(s)

¹⁵ Traduzione piuttosto impropria di "digital evidence"

essere ricavate esclusivamente mediante un processo informatico di natura certificata che determina una specifica elaborazione. In questo senso, la "ripetibilità" di tale processo è un elemento determinante che caratterizza la bontà dell'attività e la competenza tecnica di chi la svolge.

Un dato digitale, e quindi una possibile fonte di prova elettronica, è per sua natura soggetto ad essere modificato, alterato o distrutto con estrema facilità. La preservazione più o meno sicura di tali dati è quindi fondamentale anche per la successiva indispensabile analisi a scopo di indagine. L'interpretazione dei dati elettronici presenti in un computer è poi altrettanto importante quanto la loro individuazione questo perché un dato male interpretato genera informazioni sbagliate.

I dati elettronici, al fine di essere ammissibili in dibattimento, devono essere ottenuti mediante procedure corrette, legalmente certificate e documentate. Si possono individuare almeno **"4 fasi pratiche"** che portano a determinare "fonti di prova digitali" [3]: repertamento/imballaggio, copia, analisi e relazione finale. Questo è il ciclo di vita del reperto digitale (che può terminare anche con restituzione/distruzione).

Repertamento ➔ Copia ➔ Analisi di laboratorio ➔ Refertazione
--

1. Il **"repertamento"** dei dispositivi elettronici e dei dati sulla scena coinvolge aspetti quali la capacità di individuare gli oggetti e le informazioni, raccogliarli ed imballarli correttamente, evitare modifiche dello stato per poi scrivere un verbale completo e legalmente inattaccabile.
2. Il procedimento di **"copia"** è generalmente indispensabile al fine di preservare i dati rilevati e garantire la ripetibilità della successiva fase di analisi. La copia a scopo forense è complessa e deve essere svolta solo da strumenti hardware/software adeguati e riconosciuti per l'impiego a scopo forense.
3. L'**"analisi"** è la più complessa delle fasi e richiede competenze tecniche molto approfondite e notevole esperienza nelle indagini. E' bene tenere presente che l'esperienza nel settore informatico non coincide con quella nel settore informatico forense.
4. La costruzione della **"relazione finale"** da presentare agli investigatori e/o alla magistratura richiede una notevole schematicità di rappresentazione dei fatti, una discreta capacità di sintesi e la capacità di descrivere i risultati con parole semplici. La relazione deve essere completa nel senso che deve includere non solo i risultati ma anche la descrizione puntuale delle procedure.

LA PROCEDURA

1. Titolo

Identificazione, raccolta, acquisizione e preservazione, a partire dalla scena del crimine, di tutti i reperti costituiti da sistemi elettronici e/o digitali nonché da reperti virtuali (immateriali) costituiti da soli dati digitali.

2. Approvazione ed Ufficialità

La procedura indicata è fortemente orientata alla ISO-IEC 27037 *"Information technology -- Security techniques -- Guidelines for identification, collection, acquisition and preservation of digital evidence"* documento standard approvato a livello mondiale per la specifica attività di repertamento nel DF.

Essa risulta poi compatibile con i documenti standard internazionali indicati nel paragrafo sugli Standard Internazionali di riferimento.

3. Indice

- 3.1 Verifica delle autorizzazioni legali
- 3.2 Identificazione delle possibili fonti di prova digitali/elettroniche
- 3.3 Raccolta dei reperti
- 3.4 Acquisizione digitale dei reperti
- 3.5 Preservazione dei reperti acquisiti
- 3.6 Verifica della documentazione e della catena di custodia

4. Introduzione

Dispositivi elettronici digitali sono ormai presenti in ogni aspetto della vita e del lavoro e possiedono potenzialmente una enorme quantità di evidenze per le indagini di polizia giudiziaria. Computer, reti e sistemi elettronici digitali speciali, oltre a contenere informazioni su fatti possono essere essi stessi usati per commettere crimini (computer e cyber crime).

Risulta di fondamentale importanza, quindi, il trattamento dei reperti che potenzialmente possono fungere da fonti di prova di natura elettronica.

Le SOP di questo lavoro sono state realizzate proprio a tale scopo e sono contestualizzate alla realtà legale italiana. Merita a questo proposito un breve cenno il problema dell'individuazione e responsabilizzazione del *"manager della scena del crimine"*, questione ancora oggi fortemente

dibattuta ed irrisolta in Italia ed in diverse nazioni europee. Resta il fatto che nella maggioranza dei casi il "responsabile" per l'individuazione, raccolta, preservazione e trasporto dei reperti elettronici è il team di investigazione classico che non è tenuto ad essere specificamente preparato nel settore scientifico forense. L'ideale, come avviene in paesi quali il Giappone e gli USA, sarebbe avere squadre di intervento forensi h24 a livello locale, con specialisti in ognuno dei settori scientifici forensi ed aventi istituzionalmente le prerogative necessarie a chiudere e preservare scena del crimine ed i correlati reperti.

Nell'attesa che ciò venga recepito dalle competenti autorità italiane, il "*first responder*" rimane generalmente l'investigatore classico che è intervenuto per primo sulla scena, da cui l'utilità del presente lavoro (si deve assolutamente tenere presente la "*fragilità*" dei dispositivi elettronici e da essa valutare con quanta facilità è possibile perdere dati che potrebbero risultare determinanti per le indagini e il successivo dibattito).

5. Scopo della procedura

Questa procedura ha lo scopo di fornire un riferimento pratico e diretto per DEFR e DES, ossia coloro che, a vario titolo, devono agire sulla scena del crimine per trattare Identificazione, raccolta, acquisizione e preservazione di tutti i reperti costituiti da sistemi elettronici e/o digitali nonché da reperti virtuali (immateriali) fatti di soli dati digitali. Ciò nell'ambito italiano e considerando che l'operatore coinvolto deve poter eseguire la procedura in maniera sistematica, imparziale e documentata così da preservare l'integrità probatoria e l'autenticità delle fonti di prova determinate.

6. Termini, simboli, acronimi e sigle

Access Token: In Windows NT, rappresenta una scheda di sicurezza interna che è generata quando gli utenti si connettono. Contiene l'ID di sicurezza (SIDs) per l'utente e tutti i gruppi a cui l'utente appartiene. Una copia del token di accesso è assegnato a ogni processo avviato dall'utente.

AVI: Audio Video Interleave (formato video)

BIOS (Basic Input Output System): L'insieme di routine memorizzate in una ROM (memoria di sola lettura) che permette a un computer di avviare il sistema operativo e di

comunicare con i diversi dispositivi del sistema come unità disco, tastiera, monitor, stampante e porte di comunicazione.

Buffer: Un'area di memoria, spesso indicata come una "cache", utilizzata per velocizzare gli accessi alle periferiche. È utilizzato per la memorizzazione temporanea di dati letti da una periferica o in attesa di essere inviato a un dispositivo, come un disco fisso, un CD-ROM, una stampante o un'unità nastro.

Campi elettromagnetici: Il campo di forza associato alla carica elettrica in movimento avente componenti sia elettriche che magnetiche e contenente una quantità definita di energia elettromagnetica. Esempi di dispositivi che producono campi elettromagnetici sono gli altoparlanti e i trasmettitori radiofonici che si trovano frequentemente sulle autovetture di servizio.

CCTV: Closed Circuit Television

CD-R (Compact disk - recordable): Un disco ottico su cui i dati possono essere scritti ma non cancellati.

CD-RW (Compact disk – rewritable): Un disco ottico su cui i dati possono essere scritti e cancellati.

Clík!™ : Un'unità disco portatile, conosciuta anche come un disco Pocket Zip. L'unità esterna si collega al computer tramite la porta USB o una PC card.

Clone della prova digitale: Un clone è un'accurata riproduzione digitale di tutti i dati contenuti sul supporto fisico originale.

Compressed File (file compresso): Un file la cui dimensione è stata ridotta attraverso uno algoritmo di compressione per economizzare spazio su disco. La compressione di un file lo renderà non leggibile per la maggior parte dei programmi fino a quando esso non sarà decompresso.

Cookies: Piccoli file di testo memorizzati su un computer mentre l'utente naviga in Internet. Essi memorizzano informazioni come identificativi di posta elettronica, password e cronologia delle pagine che l'utente ha visitato.

CPU (Central Processing Unit): Unità di calcolo e controllo di un computer. Essa è il "cervello" del computer che esegue tutte le funzioni aritmetiche, logiche e di controllo.

Crittazione: Qualsiasi procedura utilizzata in crittografia per convertire testo chiaro in testo crittato per scongiurare che qualcuno, ma non il destinatario, possa leggere quei dati.

Deleted files (file cancellati): Se un soggetto sa che su un computer ci sono file incriminati, li potrebbe cancellare, nella speranza di eliminare la prova. Molti utenti di computer pensano che ciò in effetti elimini le informazioni; tuttavia, a seconda di come i file sono stati cancellati, in molti casi un ispettore forense è in grado di recuperare tutto o parte dei dati originali.

Digital evidence (prova digitale): Le informazioni memorizzate o trasmesse in forma binaria che possono essere utilizzate in tribunale

Dispositivi periferici: Un qualsiasi dispositivo ausiliario come una stampante, un modem o un sistema di memorizzazione dati, che funziona insieme a un computer.

Docking station: Dispositivo al quale un computer portatile può essere collegato per essere utilizzato come un computer desktop, dotato di solito di un connettore per i dispositivi esterni connessi, come dischi fissi, scanner, tastiere, monitor e stampanti.

Documentazione: Appunti scritti, audio/videotape, moduli stampati, schemi e/o fotografie che formano un resoconto dettagliato del luogo, prove recuperate e attività eseguite durante il sopralluogo.

Dongle: Detto anche “chiave hardware”, un dongle è un dispositivo di protezione dalla copia, fornito unitamente a un software, che si collega ad una porta del computer, di solito la porta parallela. Il software invia un codice a quella porta e la chiave hardware risponde con il suo numero seriale, che viene verificato dal programma. La chiave hardware impedisce la duplicazione del software perché ad ogni copia del programma è associato un numero univoco, difficile da ottenere, e la chiave hardware deve essere programmata con quel numero.

DSL (Digital subscriber line): Protocolli progettati per permettere comunicazioni dati ad alta velocità sulle linee telefoniche esistenti tra utenti finali e società telefoniche.

DVD (Digital versatile/video disk): Simile nell'aspetto a un CD, può però memorizzare maggiore quantità di dati.

Electronic device (dispositivo elettronico): Dispositivo che opera su principi che governano il comportamento degli elettroni. Esempi sono i sistemi di computer, gli scanner, le stampanti, ecc..

ESN: Electronic Serial Number

File con nome alterato e file con estensione modificata: Un semplice modo per camuffare il contenuto di un file è modificarne il nome con qualcosa di innocuo. Ad esempio, se un investigatore esamina dei fogli elettronici cercando una particolare estensione dei file, come “.XLS”, un file la cui estensione sia stata modificata dall'utente in “.DOC” non verrebbe visualizzato a seguito della ricerca. Gli ispettori forensi utilizzano tecniche speciali per individuare eventuali alterazioni, attività questa di cui l'utente medio non è consapevole.

First responder: L'ufficiale di polizia giudiziaria e/o altro funzionario di pubblica sicurezza che arriva per primo sul luogo del reato.

GPS: Global Positioning System

GSM: Global System for Mobile Communication

Hidden data (dati nascosti): Molti sistemi informatici includono un'opzione per proteggere le informazioni dall'utente non autorizzato, nascondendole. Un utente inesperto, con un esame superficiale, potrebbe non visualizzare file nascosti, directory o partizioni. Un esame forense documenterà invece la presenza di questo tipo di informazioni.

IMEI: International Mobile Equipment Identity

IP: Internet Protocol

ISDN (Integrated Services Digital Network) : Linea telefonica digitale ad alta velocità per connessioni di rete ad alta velocità.

ISP (Internet Service Provider): Organizzazione che fornisce accesso a Internet. I piccoli provider Internet forniscono servizi via modem e ISDN, mentre quelli più grandi offrono anche linee private hookups (per esempio, T1, T1 ripartita).

Jaz@: Un tipo di disco fisso rimovibile ad alta capacità.

LAN: Local Area Network (rete locale).

Latent (nascosto): Esistente, sebbene non visibile, ma capace di diventare visibile.

LS-120: Il Laser Servo 120 è un tipo di floppy disk della capacità di 120MB. L'unità LS-120 utilizza una testina dual-gap, che legge e scrive i dischi da 120MB oltre ai floppy standard da 1.44MB e 720KB.

MD5: Message-Digest Algorithm 5

Memoria volatile: Memoria che perde il suo contenuto quando è disconnessa dall'alimentazione.

Modem: Un dispositivo utilizzato da computer per comunicare sopra linee telefoniche. È riconosciuto da collegamento a una linea di telefono.

MP3: MPEG Audio Layer 3 (formato audio).

MPEG: Moving Picture Experts Group (formato multimedia).

NAS: Network Attached Storage (archivio di rete).

Network (rete): Un gruppo di computer collegati l'uno all'altro per condividere informazioni e risorse.

Networked system: Computer collegato a una rete.

ORB: Un disco fisso rimovibile ad alta capacità. Le unità ORB utilizzano testine con tecnologia di lettura/scrittura magnetoresistenti (MR).

Password-protected file (file protetti da password): Molti software includono la possibilità di proteggere un file utilizzando una password. Un tipo di protezione da password è detto talvolta "negazione di accesso": in questa modalità, i dati saranno presenti sul disco in modo normale, ma il software non aprirà o non visualizzerà il file se l'utente non avrà immesso la password. In molti casi, gli ispettori forensi sono in grado di aggirare questa protezione.

PDA: Personal Digital Assistant

PED: Personal Electronic Device

Phreaking: Hacking telefonico.

PIN: Personal Identification Number

Porta: Interfaccia attraverso la quale un computer comunica con un altro dispositivo o sistema. I personal computer hanno diversi tipi di porte: internamente, ci sono varie porte per il collegamento delle unità disco, video e tastiere; esternamente, vi sono porte per il collegamento di modem, stampanti, mouse e altri dispositivi periferici.

Printer spool file: Lavori che non vengono stampati direttamente ma vengono memorizzati in spool file sul disco.

Prova elettronica: La prova elettronica è rappresentata dalle informazioni e dai dati di valore investigativo che sono memorizzati o trasmessi da un dispositivo elettronico.

Prova elettronica originale: Elementi fisici e dati ad essi associati al momento del sequestro.

Proxy anonimo: Server che adempie alle richieste dei client senza inoltrare l'indirizzo IP che li identifica, permettendo quindi ad essi un assoluto anonimato sul web. Ciò è possibile poiché lo stesso proxy inoltra le richieste dei client con il suo identificativo, restituendo i dati acquisiti dalla rete ai richiedenti. Sul proxy, l'IP del client è presente per il tempo strettamente necessario a garantire il servizio

PUK PIN: Unlock Key

RAID: Redundant Array of Independent Disks (protocollo hardware/software nonché attributo di sistemi di archiviazione come hard disk, batterie di hard disk, ecc.).

RAM: Random Access Memory

Replicatore di porte: Dispositivo dotato delle comuni porte di un PC (seriali, parallele e di rete) che si collega ad un computer portatile. Un replicatore di porte è simile a una "docking station", la quale normalmente fornisce possibilità di espansione alle schede madri.

RFID: Radio Frequency Identification

SAN: Storage Area Network

Screen saver (salvaschermo): Un programma di utilità che evita al monitor di essere danneggiato da un'immagine immutabile. Può anche fungere da controllo sugli accessi.

Seizure disk (disco di acquisizione): Un floppy disk speciale progettato per proteggere il computer dalle modifiche accidentali di dati.

Server: Computer che fornisce vari servizio ad altri computer ad esso collegati tramite una rete.

SHA1: Secure Hash Algorithm 1

SIM: Subscriber Identity Module (modulo utente per i telefoni cellulari – chip).

Sleep mode: Modalità di attesa che sospende le attività del disco fisso e del monitor, restituendo una schermata video nera/vuota, al fine di ridurre il consumo energetico. Talvolta è indicato come “modalità di sospensione”.

Stand-alone computer (computer indipendente): Computer non collegato ad una rete o ad altri computer.

Steganography (stenografia): L'arte e la scienza di comunicare in modo da nascondere l'esistenza della comunicazione. È utilizzata per nascondere file dentro altri file. Ad esempio, un'immagine pedo-pornografica può essere nascosta dentro un altro file di immagine, dentro un file audio o dentro un file di un altro formato.

Supporto magnetico: Un disco, un nastro, una cartuccia, un dischetto o una cassetta utilizzata per memorizzare magneticamente i dati.

Supporto rimovibile: Elementi (per esempio, floppy disk, CD, DVD, cartucce, nastri) che memorizzano dati e possono essere facilmente rimossi.

System administrator (amministratore di sistema): Colui che legittimamente ha il compito di supervisore in un sistema di computer. L'amministratore gestisce l'accesso al sistema al livello più alto. E' conosciuto anche come sysop, sysadmin e system operator.

Temporary and swap files (file temporanei e di scambio): Molti computer utilizzano sistemi operativi e applicazioni che memorizzano temporaneamente i dati sul disco fisso; questi file, che sono generalmente nascosti e inaccessibili, possono contenere informazioni che l'investigatore trova utili.

Tunneling: Sistema di trasmissione dati mediante Internet che permette a coloro che sono coinvolti nella comunicazione di avere una specie di canale dedicato, detto “tunnel”, che risulta del tutto trasparente agli altri utenti del web. Tutto ciò avviene mediante specifici protocolli di comunicazione che incapsulano i pacchetti di trasmissione all'interno di altri

pacchetti regolati dal protocollo specifico di tunneling: in tal modo l'investigatore potrà accertare che è avvenuta una comunicazione tra due utenti, ma non potrà mai risalire all'informazione oggetto della stessa. Uno dei protocolli più noti è il PPTP (Point to Point Tunneling Protocol)

UPS: Uninterruptible Power Supply

USB (universal serial bus 1.0, 2.0 e 3.0): Interfaccia hardware per periferiche a bassa velocità come tastiera, mouse, joystick, scanner, stampante e telefoni.

USIM: Universal Subscriber Identity Module

Zip®: Unità disco rimovibile da 3.5 pollici. Tale unità è fornita con un software che può catalogare i dischi e bloccare i file per motivi di sicurezza.

7. Sicurezza

Personale: se la o le persone indagate sono presenti sulla scena del crimine bisogna tenere conto che potrebbero divenire violente e quindi vanno allontanate o, qualora risulti indispensabile, possono rimanere presenti opportunamente controllate.

Il personale specializzato in informatica ed elettronica deve spesso rimanere per ore sulla scena del crimine ed operarvi in maniera molto intensa dal punto di vista intellettuale avendo scarso contatto con la realtà (data l'immersione nei sistemi digitali), risulta quindi importante quanto segue.

Armi: qualora siano presenti armi sulla scena del crimine devono essere rimosse da personale specializzato e non permanere durante le attività di sopralluogo e repertamento informatico/elettronico.

Pericoli meccanici, chimici ed elettrici: sempre il personale specializzato deve provvedere a rimuovere oggetti e sistemi atti a costituire pericolo meccanico (es. oggetti in precaria condizione di equilibrio), chimici (es. acidi), elettrici (es. fili di collegamento elettrico alla corrente alternata di rete in precaria condizione di isolamento).

Pericoli psicologici: materiale informatico e dati possono costituire problema psicologico per il personale operante qualora si riferisca a situazioni inerenti pedopornografia, violenza, terrorismo, ecc. In tali casi bisogna sempre seguire la regola di interagire il meno possibile con macchine e dati al fine di realizzare sul posto esclusivamente quanto indispensabile per preservare la maggioranza delle fonti di prova e proseguire quindi le analisi in laboratorio. Il personale tecnico soggetto a tali

pericoli psicologici dovrebbe essere sottoposto a controlli periodici dello stato mentale (es. 6 mesi).

Pericoli biologici: il materiale informatico ed elettronico (es. frequente del cellulare su una scena di omicidio) potrebbe essere immerso, coperto o comunque raccogliere quantità variabili di liquidi o materiali biologici come sangue, liquidi seminali, ecc. Data la possibilità che ciò comporti trasmissione di malattie al personale operante si deve scegliere che il repertamento in specie sia effettuato da personale specializzato in biologia lasciando eventuali ispezioni informatiche ad un passo successivo della procedura.

Indicazioni cui attenersi in generale: l'operatore informatico ed elettronico forense, sulla scena del crimine, deve avere la prevista vestizione integrale per evitare qualsiasi forma di inquinamento delle fonti di prova (quindi almeno tuta, protezione delle calzature e guanti). A ciò va aggiunto l'impiego di:

- strumenti per l'apertura ed il trattamento di circuiti elettrici ed elettronici (pinzette, giraviti, ecc.) che risultino compatibili con le direttive sull'isolamento elettrico stabilite dal laboratorio di appartenenza;
- kit antistatici soprattutto nel trattamento di sistemi digitali micro-elettronici;
- calzature isolanti secondo lo standard stabilito dal laboratorio di appartenenza.

8. Equipaggiamento tecnico

Si deve partire questo paragrafo considerando tutte le possibilità che un sistema elettronico digitale ha di interfacciarsi con l'esterno. Questo in quanto proprio tali "porte" costituiranno elemento centrale di indagine per colui che interviene sulla scena del crimine.

- Tastiera e Monitor
- Interruttori ON/OFF/STANDBY
- Ethernet port
- Phone/Fax port
- VGA port
- HDMI port
- USB port
- CD/DVD drive
- Serial port

- DVI port
- Parallel Port
- PS/2 port
- Firewire port
- Compact Flash
- Thunderbolt port
- Interfacce proprietarie

In base a tali eventualità di interfacciamento bisogna essere pronti con dei tool specifici sul posto:

- 1) **Workstation forense portatile** dotata del maggior numero possibile di porte di interfacciamento e con installato il software per repertamento ed analisi forense di dati
- 2) **Copia a basso livello del contenuto dell'hard disk della workstation** pronta per l'eventuale ripristino dell'apparato qualora durante il repertamento siano avvenute alterazioni incontrollate
- 3) **Collegamento ad Internet della Workstation forense** al fine di rendere possibili ricerche scientifiche e di nomi, fatti, ecc. Questo collegamento può essere via satellite o chiavetta mobile
- 4) **Lettore di SIM card** e software installato (sul workstation portatile) di analisi
- 5) Sistema di repertamento ed analisi dei dati di terminali radiomobili di cellulari ivi comprendendo una **gabbia di Faraday** campale
- 6) **Buste schermate** elettromagneticamente e elettrostaticamente per imballare i reperti ed **etichette**
- 7) **Tester multifunzione** tarato precedentemente all'intervento
- 8) Un **alimentatore** che generi corrente continua da alternata o da batteria con una tensione regolabile
- 9) **Set di hard disk** (già sottoposti a wiping, funzionanti e pronti per ospitare dati) di sufficiente capacità di memoria per eventuali copie sul posto
- 10) **Skimmer** per la lettura eventuale di carte di credito
- 11) **Hard disk forensic imager** per realizzare l'eventuale copia forense sul posto del contenuto di hard disk
- 12) **Chip forensic imager**: sistema di lettura campale di chip di memoria flash
- 13) **Set di giraviti** e strumenti di montaggio/smontaggio case

- 14) Set di software di **NFAT** (Network Forensic Analysis Tools) per affrontare attività di repertamento, analisi e tracciamento in rete
- 15) Set di **software per la “live analysis”** dei sistemi e delle memorie di massa che per la loro peculiare attività possono risiedere su CD/DVD o su chiavetta USB
- 16) Set di software di cracking per abbattere eventualmente password e protezioni sui dati e programmi
- 17) **Connettori** per telefoni cellulari
- 18) **Connettori** standard per PC e Mac

In tutto questo va ricordata la regola generale che sulla scena del crimine non è positivo effettuare l'analisi e quindi spingersi molto nell'attività forense. Lo scopo deve rimanere il prelievo del reperto virtuale e/o reale sapendo che in laboratorio continueranno le attività.

9. Ruoli e Responsabilità

Sulla scena del crimine sono ipotizzabili le seguenti funzioni, talvolta svolte da un numero di persone non necessariamente coincidente:

- **Responsabile per la scena:** colui che mantiene il controllo degli accessi e che genera un report finale dei movimenti di persone e raccolta di reperti sulla scena stessa (non necessariamente si tratta di uno specialista in tecniche scientifiche forensi);
- **Team leader:** il capo della squadra multidisciplinare di intervento della scientifica, colui che, dotato di notevole esperienza in interventi sulla scena, individua il piano da adottare e le materie forensi da coinvolgere nell'attività, tenendo i contatti con l'Autorità Giudiziaria, la Polizia Giudiziaria ed i media, inoltre è responsabile per la creazione della catena di custodia e quindi per l'iniziale integrità (prima del trasporto in altro sito) dei reperti.
- **DEFR (Digital Evidence First Responder):** individuato dal team leader il DEFR opera nel piano di intervento già prefigurato per quanto strettamente attiene ai sistemi elettronici digitali (hardware/software) decidendo la procedura di sopralluogo tecnico, prendendo decisioni sull'attività (ripetibilità/irripetibilità), tenendo i contatti e redigendo correlato verbale; egli impiega, se necessario, una squadra di tecnici da lui supervisionati e comandati sul posto di cui è ovviamente responsabile per la sicurezza.

10. Processo

Questo lavoro non pretende di essere completo sotto ogni punto di vista per il repertamento di dispositivi digitali o dati elettronici in quanto l'evoluzione della tecnologia ha raggiunto ormai livelli che rendono mesi paragonabili ad anni. Oltre a ciò è ben noto agli investigatori che "ogni scena del crimine è un mondo a parte" e quindi in molti casi solo l'abilità e l'esperienza del tecnico forense possono suggerire il da farsi.

Resta il fatto però che lo scopo essenziale non è essere esaustivi quanto consentire di avere una linea di lavoro standard e documentabile che permetta di evitare al massimo gli errori.

Sulla scena del crimine, è necessario prendere tutte le precauzioni possibili per evitare di alterare le prove elettroniche e/o i dati di interesse.

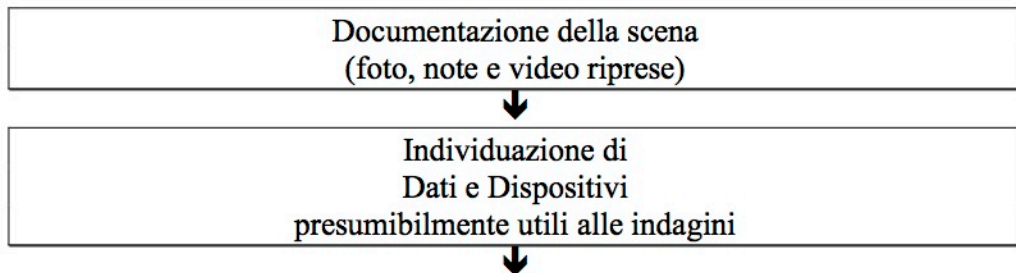
Dal punto di vista elettronico ed informatico le principali azioni da svolgere sono:

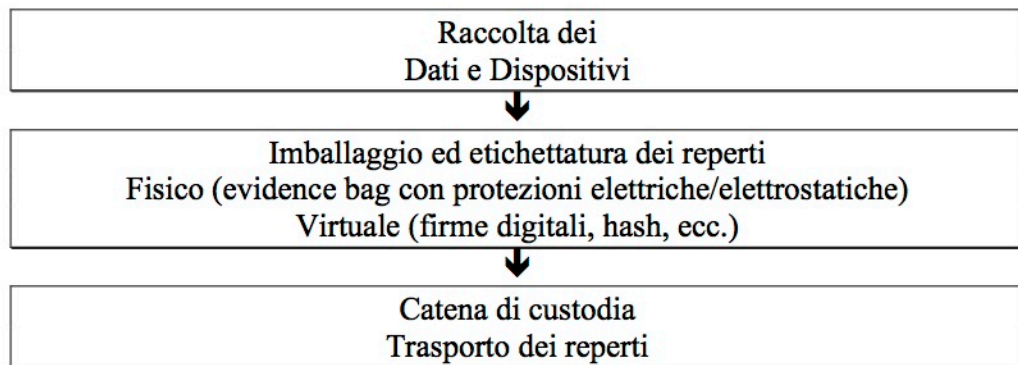
- documentazione della scena (foto, note e video riprese);
- individuazione e raccolta di dati e dispositivi utili alle indagini;
- imballaggio, etichettatura e trasporto dei dati e dispositivi individuati.

Si deve essere sicuri:

- di avere le necessarie **autorizzazioni della magistratura** per lo svolgimento delle singole azioni;
- che la scena del crimine sia stata sufficientemente documentata prima di prelevare o modificare qualcosa;
- di impiegare sempre i dispositivi di protezione personale prima di accedere a qualsiasi dispositivo.

Nota: I DEFR ed i team leader (di intervento della scientifica) devono tenere presente che l'accesso improprio ai dati sulla scena del crimine determina spesso violazioni. Inoltre devono ricordare che il sopralluogo informatico ed elettronico avviene sia in ambito fisico che virtuale. Spesso, cioè, non è possibile repertare fisicamente degli apparati ma si deve comunque procedere a repertare virtualmente (copia forense) i loro dati.





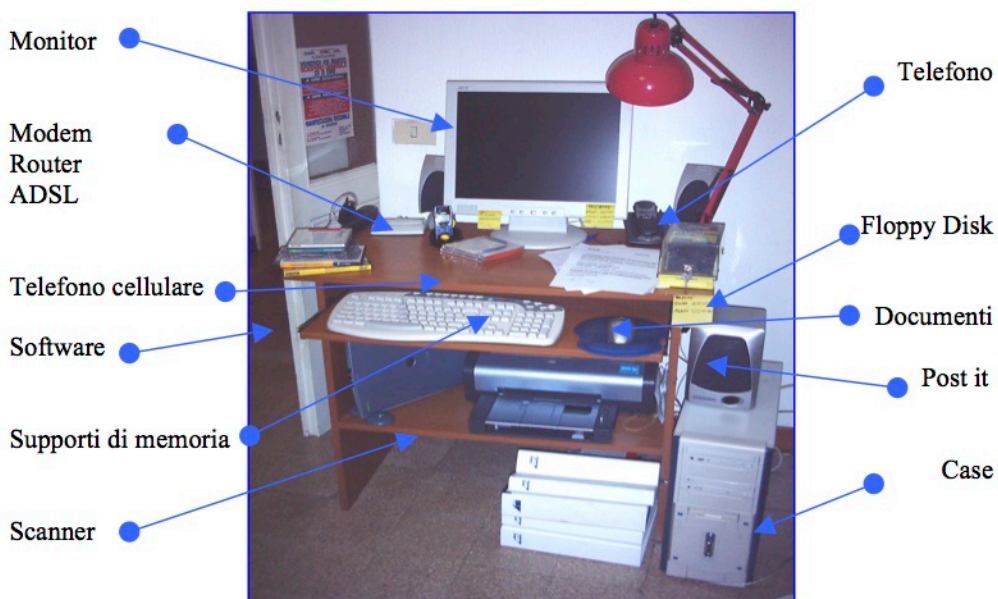
10.1. Individuazione delle fonti di prova

Le "fonti di prova elettroniche ed informatiche" sono in linea di principio ottenibili da una grande varietà di dispositivi elettronici digitali.

Di seguito si andranno a vedere i dispositivi che più comunemente si possono incontrare sulla scena del crimine con annessa una breve descrizione (uso, forma e particolarità rilevanti).

Oltre a ciò, si indicherà che tipo di "prova" potrebbe essere ottenuta da ciascun tipo di dispositivo.

Si tenga presente che molti dispositivi elettronici memorizzano i dati su memorie che hanno bisogno di batterie tampone o della corrente di rete per non perdere i dati in loro contenute. Di converso molti altri dispositivi devono essere spenti forzatamente per garantire un buon repertamento (che consenta poi un'analisi efficace).



10.1.1. Computer System



Descrizione: Un computer in linea di massima è formato da componenti fondamentali interni, quali un'unità centrale spesso chiamato central processing unit (CPU) e da unità di



memorizzazione, da componenti esterni quali un monitor, una tastiera ed un mouse, fondamentali all'utente per poter interagire con la macchina; può essere isolato o connesso in rete ad altri dispositivi elettronici. Ci sono diversi tipi di computer come: laptop, desktop, tower system, modular rack-mounted system, minicomputer e mainframe (grandi server). Componenti ulteriori di interesse sono: modem, stampanti, scanner, docking station, ed unità di memorizzazione esterne al case. Tutte queste componentistiche saranno illustrate basilamente di seguito in questo capitolo unitamente ad immagini più comuni delle stesse utili ad individuarle in sede di sopralluogo.



Uso primario: qualsiasi tipo di funzione elaborativa e di memorizzazione es. word processing, calcoli, comunicazioni, grafica, ecc..

Prove estraibili: dati in file, file cancellati, email, ecc.; esempi:

a. Normali file creati dall'utente

- Rubriche;
- File Audio/video ;
- File Database;
- Date;
- Documenti o file di testo;
- File E-mail;
- File Immagini/grafici;

- Segnalibri/favoriti Internet;
- Fogli elettronici.

Tali file possono essere distinti e catalogati su base dell'attributo di tipologia che possiedono.

b. File protetti

L'utente può nascondere o proteggere dati di interesse in diversi modi. Ad esempio è possibile criptare i dati e vincolare la loro visione al possesso di una parola chiave (password). E' anche possibile cambiare estensione ad un file e spostarlo in una cartella che contiene migliaia di altri file simili, ecc. Di seguito alcune tecniche:

- File compressi ;
- Misnamed file (file con estensione/tipologia alterata);
- File criptati;
- File protetti da password;
- File nascosti o steganografati.

Si rilevano tracce importanti anche su file creati in automatico dal sistema operativo durante il funzionamento della macchina a seguito delle attività svolte dall'utente (es. le attività di navigazione su Internet).

Nota: dei file spesso si usa la data di creazione/modifica o l'orario proprio come elemento di interesse ai fini delle indagini. Quindi non solo il contenuto ma anche gli attributi dei file possono essere fonti di prova.

c. File del computer analizzati dal tecnico

- File di Backup;
- File di configurazione;
- Cookies;
- File nascosti;
- File cronologici;
- File di log;
- Printer spool file;
- File di swap;
- System file;
- File temporanei.

d. Altre aree dati analizzate dal tecnico

- Bad clusters;

- Data, ora e password di sistema;
- File cancellati;
- Spazi liberi;
- Partizioni nascoste;
- Cluster persi;
- Metadata;
- Altre partizioni;
- Aree riservate;
- Slack space;
- Informazioni di registrazione software;
- System area;
- Unallocated space.

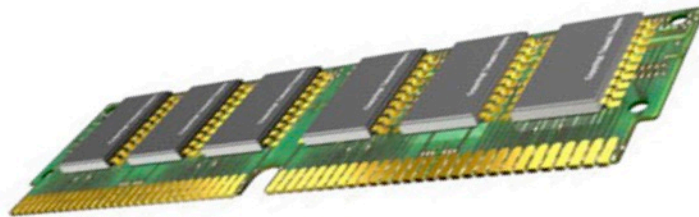
10.1.2. Cenni sulle componenti del computer

a. Memoria RAM

Descrizione: circuito removibile interno al case; mantiene le informazioni solo fino a quando alimentato elettricamente.

Uso primario: permette di memorizzare i dati temporaneamente durante le elaborazioni.

Prove estraibili: dati non ancora memorizzati su memorie permanenti o semipermanenti: ad esempio in molti casi le password, i malware attivi, ecc.

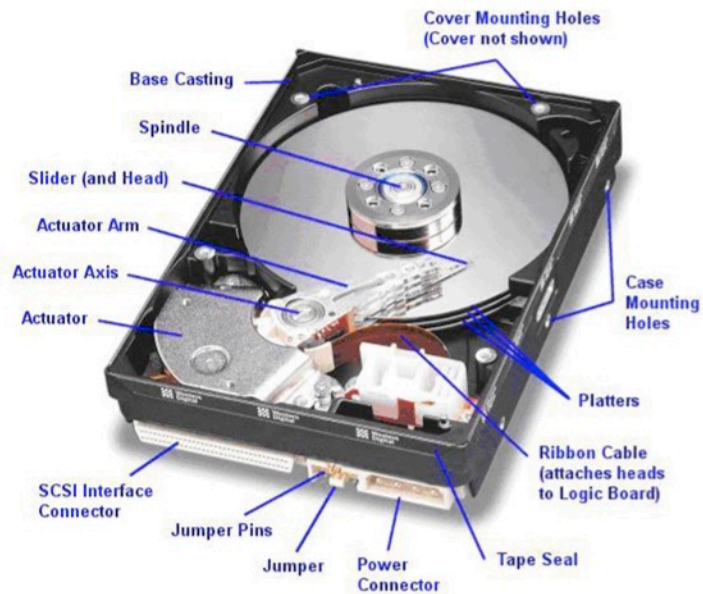


b. Hard Disk (Magnetico o SSD/elettronico)

Descrizione: scatola sigillata di metallo/plastica contenente circuiteria ed uno o più dischi magnetici su cui possono essere registrati dati digitali. Normalmente è interno al case ma può trovarsi anche esternamente se l'utente è esperto.

Uso primario: memorizzazione di dati digitali (programmi, documenti, immagini, video, multimedia files, ecc.).

Prove estraibili: le stesse indicate per il computer system.



Har Drive 3.5-inch magnetico

Figura 6



External Hard Drive Pack



Removable Hard Drive Tray



2,5-inch IDE Hard Drive



5,25-inch IDE Hard Drive



Microdrive

c. Memorie di massa di vario genere

Descrizione: dischi, nastri e pennette USB (es. vecchi floppy disk, CD, DVD, cartucce, nastri).

Uso primario: dispositivi portatili in grado di memorizzare programmi, documenti, immagini, video, ecc.. Nuovi tipi di memorie di massa sono continuamente progettate ed immesse sul mercato.

Prove estraibili: stesso che su computer system.



Cartucce Syquest



Cassette da 4 e 8 mm



Cartucce DLT



Cartuccia Jaz



Cartuccia Zip



FD LS-120



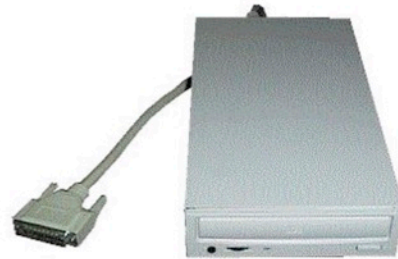
Floppy Disk 3.2'



DVD-RAM



CD-Recordable



External CD-ROM Drive



External Media Disk Drive



External Zip Drive



DAT Tape Reader



Tape Drive



Pennette USB



d. Componenti di rete

(1) Scheda di rete (LAN) Card o Network Interface Card (NIC)

Nota: questi componenti sono evidenza del collegamento in rete del computer per cui si deve richiedere l'ausilio dell'esperto forense.

Descrizione: Scheda elettronica associata a dei cavi di collegamento che finiscono generalmente a muro.

Uso primario: comunicazione tra computer in un'area limitata (edifici) e possibilità di connessione ad Internet.

Prove estraibili: il MAC address per l'intercettazione delle attività svolte in rete e la presenza del dispositivo.



PCMCIA Network Interface Card



Wireless PCMCIA Card



Wireless Network Interface Card



Internal Network Interface Card

(2) Router, Hub e Switch

Descrizione: dispositivi per gestire reti di computer generalmente posti in armadi speciali.

Uso primario: gestione di reti.

Prove estraibili: la presenza delle unità che compongono la rete.



Ethernet Hub



Router

(3) Server

Descrizione: un server è un computer generalmente di grandi dimensioni (rispetto a quelle di un PC) che fornisce servizi ad una rete di elaboratori.

Uso primario: permettere la condivisione di file, stampanti e dati su una rete di computer.

Prove estraibili: le stesse indicate per il computer system.



(4) Connettori e cavi di rete

Descrizione: connettori e cavi di diverse forme e colori che vanno a collegare tra loro computer, hub, switch, router, ecc. o computer a speciali spine su muro.

Uso primario: connessione di componenti di rete.

Prove estraibili: il dispositivo stesso.



RJ-11 Phone Cable



RJ45- LAN Cable



USB Cable



Parallel Port & Centronics - Printer Cable



Ultrawide SCSI Cable



SCSI Multiple Cable



Serial Cable & Mouse



PS2 Cable With PS2 AT Adapter



Audio/Video Cable



Network Cable Dongle
& Network Card

Figura 15

e. Modem

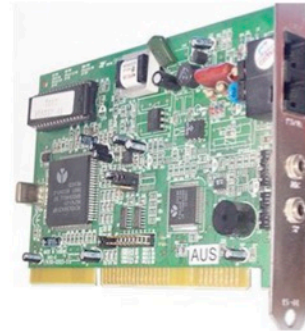
Descrizione: dispositivo interno/esterno al case (analogico, DSL, ISDN, cable), in grado di connettere quest'ultimo alla linea telefonica.

Uso primario: supportare le comunicazioni digitali, prima fra tutte il collegamento ad Internet, e quindi navigazione, email, chat, ecc..

Prove estraibili: la possibilità di comunicare...



Modem esterno



Modem interno



Modem Wireless



PCMCIA Modem

Figura 16

f. Stampanti

Descrizione: ne esistono di diverso tipo - termiche, laser, a getto d'inchiostro, impatto, sublimazione, ecc.. in genere sono connesse ad un computer o ad una rete tramite cavo seriale, parallelo o USB oppure mediante porta infrarossi. Le stampanti dipartimentali hanno dentro un PC con hard disk.

Uso primario: stampare testo ed immagini su carta.

Prove estraibili: log (date ed orari), network ID, caratteristiche di stampa (es. documenti anonimi).



Multifunzione



Stampante laser

Figura 17

g. Scanner

Descrizione: dispositivo ottico connesso ad un computer tramite porta parallela, porta seriale, USB, ecc..

Uso primario: convertire documenti cartacei in formato file.

Prove estraibili: in diversi casi di frode è l'unità stessa la prova.



Sheetfed Scanner



Flatbed Scanner

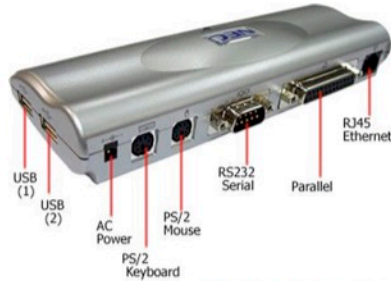
Figura 18

10.1.3. Altri sistemi elettronici...

Ci sono diversi altri sistemi elettronici che possono essere rinvenuti sulla scena del crimine e che sono di notevole interesse per le indagini. Seguono alcuni esempi.



Identificatore di chiamata



Docking Station



Port Replicator



Cellular Phone Cloning Equipment

Figura 19

a. Palmari ed agende elettroniche (Personal Digital Assistants [PDA], Electronic Organizers)

Descrizione: un personal digital assistant (PDA) è un piccolo dispositivo che può includere PC, tel/fax, cerca persone, rete, ed altre funzioni. Normalmente è trasportato in tasca dall'utente. Può contenere memorie di vario tipo anche molto capaci e performanti. Spesso vengono sincronizzate al contenuto di un PC. Se è presente un cavo con spinotto quasi sicuramente è stato connesso ad un PC che è da reperire anch'esso.

Uso primario: lo stesso di un PC, con portatilità e facoltà di comunicazione inclusi.

Nota: le batterie del dispositivo, una volta scariche, possono attivare pericolosi meccanismi di protezione e processi di alterazione dei dati.

Prove estraibili:

- Indirizzi;
- Appuntamenti;
- Voce.
- Numeri di telefono;
- Scritture a mano scannerizzate;
- E-mail;
- Documenti;
- Password;
- Messaggi;



PDA



Accessori Palmare



Palmare con Cradle



Smartphone

b. Schede di memoria

Descrizione: unità portatile di minime dimensioni simile ad un piccolo circuito elettronico. Usate nei PDA, nelle macchine fotografiche digitali, nelle video camere digitali, ecc..

Uso primario: memoria addizionale removibile di facile trasporto.

Prove estraibili: stesso che su computer system.



Memory Stick



Flash Card in PCMCIA Adaptor



Compact Flash Card



Smart Media Card



Smart Media Floppy



FD Adaptor/Memory Stick



Memory Cards

Figura 22

c. Videocamere/macchine fotografiche digitali

Descrizione: normale telecamera che registra in Hi8 o MiniDV, oppure VideoCam su PC; macchina fotografica senza pellicola.

Uso primario: acquisizione di immagini reali su formato digitale esportabile su PC e/o su memorie digitali.

Prove estraibili:

- Immagini;
- Video;
- Cartuccia rimovibile.
- Date ed orari;
- Suoni;



QuickCam



Snappy Device



Videofonia



Macchine Fotografiche

d. Smart Card e Scanner Biometrici (dispositivi per il controllo degli accessi)

Descrizione: una smartcard è un dispositivo delle dimensioni di una carta di credito che include un microprocessore. Può essere impiegata per trasportare denaro, password, autenticazioni, certificati digitali ed altro.

Uno scanner biometrico è un dispositivo che, connesso ad un computer permette di identificare le caratteristiche biometriche di un essere umano (impronte, voce, retina, ecc.).

Uso primario: accesso a risorse informatiche protette o a particolari circuiti di carte di credito.

Prove estraibili: identificazione ed autenticazione presenza dell'utente, configurazione impostata, permesso di accesso, ecc.. Idem per una chiave USB.



Smart Card



Biometric Scanner



USB Dongles



Parallel Donale

e. Telefoni

Descrizione: si può trattare di telefono fisso, cordless o cellulare.

Uso primario: comunicazione bidirezionale tra due utenti. possono impiegare linee analogiche o sistemi di collegamento digitali. Funzione non principale ma importante è la memorizzazione dati.

Note: il "first responder" deve tenere presente che a batterie scariche il telefono può perdere dati anche di rilevanza.

Prove estraibili:

- Date ed orari;
- Nomi e numeri di telefono della rubrica;
- Informazioni sull'identificazione del chiamante;
- Appuntamenti e orari;
- Suoni e voci registrate;
- Pagine web, e-mail e voice mail;
- Sms e messaggi di testo;
- Electronic serial number;
- Password;
- Cartuccia rimovibile.



Cordless



Telefono Cellulare

f. Segreteria telefonica

Descrizione: dispositivo parte del sistema di ricezione telefonico che permette di registrare le chiamate in assenza dell'utente. Alcuni modelli usano ancora i nastri magnetici analogici ma molti si sono orientati verso la registrazione digitale.



Uso primario: registrare messaggi vocali telefonici.

Nota: si noti che a batterie scariche o alimentazione scollegata la segreteria telefonica perde il contenuto.

Prove estraibili: voci e dati sul chiamante...

g. Cerca persone

Descrizione: dispositivo portatile di piccole dimensioni che può contenere numeri di telefono, email ecc.. Alcuni cellulari e PDA possono essere impiegati come cerca-persone.



Uso primario: inviare e ricevere messaggi, numeri di tel/fax, email.

Nota: a batteria scarica perdono il contenuto.

Prove estraibili:

- Numeri di telefono;
- Indirizzi e messaggi di testo;
- E-mail e Voice mail.



Rim Pager

Sigle Pager



Pagers

h. Fax

I fax possono contenere numeri di telefono, log di comunicazione e tracce di documenti trasmessi/ricevuti. alcuni fax sono costituiti da un sistema scanner, stampante, PC special purpose per cui devono essere repertati come computer system.

Prove estraibili:

- Documenti;
- Numeri di telefono;
- Film cartridge;
- Log di rice/transmissione.



i. Credit Card Skimmer

I credit card skimmers sono usati per leggere le informazioni memorizzate nelle carte magnetiche (es. bancomat, carte di credito, pass di ingresso/uscita cancelli, ecc.).

Prove estraibili: informazioni sul possessore della carta di credito o su colui a cui essa è stata copiata, quali

- Numero di carta;
- Data di scadenza;
- Nome e cognome;
- Indirizzi



Credit Card Skimmer



Credit Card Skimmer Laptop



Credit Card Skimmer

j. Orologi digitali

Ci sono diversi orologi digitali in grado di comunicare digitalmente e/o di memorizzare anche discreti quantitativi di dati. Alcuni supportano collegamenti ad esempio tramite USB ad un PC divenendo a tutti gli effetti un hard disk camuffato.

Prove estraibili:

- Indirizzi;
- Numeri di telefono;
- Appuntamenti;
- E-mail;
- Note.



k. Global Positioning Systems (GPS)

I Global Positioning Systems possono indicare rotte e/o posizioni di uomini e mezzi. Alcuni dispongono di sofisticati sistemi di memorizzazione per cui devono essere trattati come computer system.

Prove estraibili:

- Posizioni fisse;
- Coordinate di punti in percorsi
- Destinazioni già raggiunte;
- Nomi di vie;
- Log di viaggio.



Global Positioning Systems (GPS)

1. Macchine fotocopiatrici

Diversi fotocopiatori attuali sono sostanzialmente complessi scanner collegati ad una sorta di PC specializzati "special purpose" e quindi mantengono in memoria (talvolta anche in hard disk interni) dei dati.

Prove estraibili:

- Documenti;
- Log di utilizzo;

- Orari e date.



Fotocopiatrice

10.1.4. Individuazione dei reperti virtuali

a. Siti web

Qualora sulla scena del crimine sia presente un computer o sistema embedded (es. Ipad, iPhone, smartphone, ecc.) attivo e connesso ad una rete è possibile che risulti operativo su di esso un browser (software come explorer, firefox, chrome, ecc.) che stia navigando o abbia navigato da poco su un sito web. Dal punto di vista delle indagini le informazioni ricavabili da un sito web possono essere enormi e variegate. Si tratta in definitiva di un ambiente prettamente virtuale in cui indagare ha molto di simile con quanto si potrebbe fare nel mondo reale. Per l'individuazione è molto importante imparare a riconoscere i browser più comuni (come quelli citati ad esempio), le loro funzioni (es. lo storico) e le funzionalità dei più diffusi siti web come i motori di ricerca (es. google) ed i social network (es. facebook).



Explorer, Firefox e Chrome



Facebook

b. File di interesse

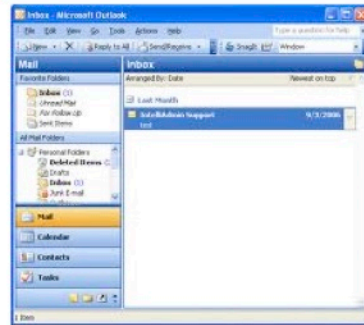
Individuare i file di interesse all'interno di un sistema attivo sulla scena del crimine è importante quando si pensa che il non copiarlo, visionarlo o prelevarlo in quel momento porti direttamente o indirettamente alla sua perdita. Ciò in quanto i file di interesse possono essere rilevati nella successiva analisi di laboratorio. Rilevare file di interesse può essere importante per memorie crittate (es. truecrypt) e/o per software che operano in remoto sulla rete (es. dropbox). Conoscere i sistemi di crittazione più comuni ed i software di sharing dei dati sulla rete costituisce una base indispensabile.



Truecrypt & Dropbox

c. Email

Bisogna fare la distinzione tra email su webmail e su software client. Nel primo caso l'email è un dato estraibile da una pagina web (es. Gmail) di un browser connesso mentre nel secondo caso un file di un particolare software installato sul computer in studio (es. Outlook). È importante appurare di quale dei due casi si tratta perché bisogna poi operare diversamente per non perdere i dati.



Gmail & Outlook

d. Software di comunicazione interattiva

si può considerare una macro-categoria che include:

- P2P e file sharing in rete o subnet;
- le svariate forme di VoIP, telefonia su rete IP;

- le diverse tipologie di IM (instant messaging) e di chat, ecc.
Risulta molto complesso effettuare una classificazione esaustiva data la varietà di strumenti software che possono essere usati in quest'area.



Emule, Kazaa, Skype & Messenger

e. Altro software...

Esistono svariate altre categorie di software che potrebbero essere interessanti dal punto di vista investigativo ma trattarle esaustivamente e con metodo unificato è praticamente impossibile. Comuni nelle indagini sono i data base, i software di cracking e clonazione, i malware ed i virus, ecc.

10.2. Raccolta di dati e dispositivi

10.2.1. Autorizzazioni legali

Sulla scena del crimine, è indispensabile innanzitutto disporre delle necessarie autorizzazioni della magistratura per lo svolgimento delle singole azioni; è necessario, inoltre, prendere tutte le precauzioni possibili per evitare di alterare le prove elettroniche e/o i dati di interesse.

Qualora siano necessarie azioni non ripetibili il DEFR ne deve immediatamente prendere atto e contattare l'A.G. inquirente in proposito.

10.2.2. Prerequisiti

Le attività devono essere autorizzate dal punto di vista legale (bisogna avere con se tutte le previste autorizzazioni) e tutti gli operatori presenti sulla scena devono avere la prevista conoscenza di base informatica/elettronica a seconda del loro livello (DEFR, DES, operatore di supporto, ecc.).

Dato che potrebbe svilupparsi attività di copia dei dati sul posto è necessario avere a disposizione almeno una **memoria portabile semipermanente** sufficientemente capiente (es. hard disk portabile alimentato tramite USB), libera da contenuti e sottoposta a precedente "ripulitura forense" (wiping) dove poter riservare i dati.

10.2.3. Procedura

Chiuso l'accesso alla scena del crimine, il Team Leader della squadra di intervento deve attivare le riprese video/fotografiche ed individuare le possibili fonti di prova tra cui quelle elettroniche.

Ciò premesso, bisogna stabilire un **"piano di repertamento"** che stabilisca l'ordine con il quale repertare i dispositivi, ciò sotto due condizioni:

- evitare di danneggiare i reperti mediante azioni dirette;
- agire prima che degli eventuali reperti (dati o sistemi fisici) spariscano o siano non più individuabili a causa della non tempestività dell'intervento e/o dell'imperizia.

La necessità di stabilire una corretta priorità del repertamento viene proprio da tali condizioni. Si può stabilire un ordine di riferimento come segue:

(1) **Il contenuto delle memorie volatili** (memorie soggette a perdere il loro contenuto se non alimentate elettricamente) ha l'assoluta priorità. La mancanza di intervento specifico, in tal senso, porta alla precoce perdita di tali informazioni.

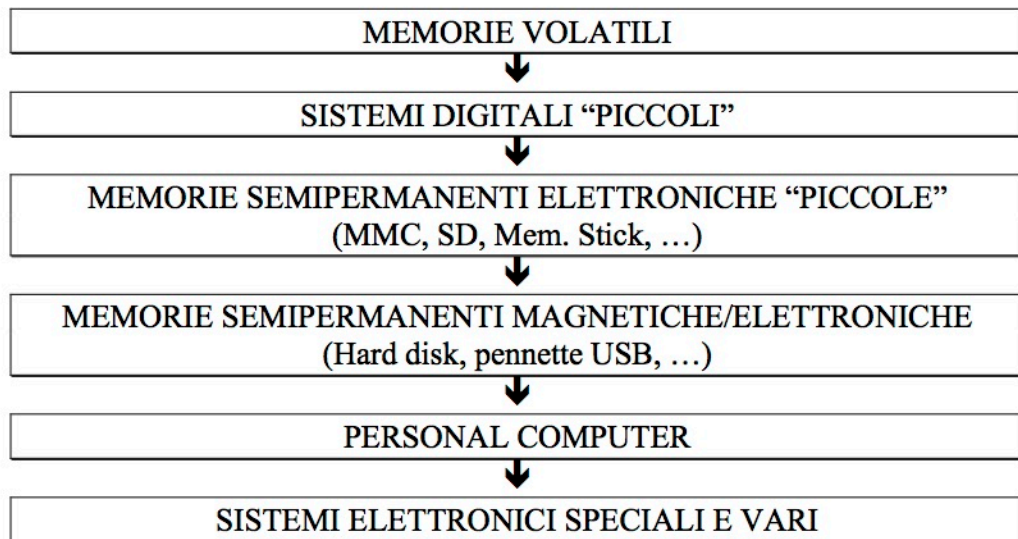
(2) Bisogna poi privilegiare i **sistemi digitali di piccole dimensioni** come cellulari, smartphone, iPod, palmari, macchine fotografiche digitali, ecc. in quanto generalmente portatori di informazioni la cui fruibilità è immediata nel prosieguo delle indagini grazie sia al continuo aggiornamento che le caratterizza che al loro legame con le comunicazioni e le necessità individuali dei soggetti.

(3) Si può passare quindi alle **memorie semipermanenti portabili** (removable media) **di natura elettronica** (Multi-media card (MMC) - memoria flash che costituisce a tutti gli effetti un hard disk allo stato solido - Secure Digital card (SD) - simile alla MMC con meccanismi di protezione dei dati - Memory stick, TransFlash, ecc.). Questo in quanto

all'immediatezza e semplicità del loro repertamento ed analisi nonché al fatto che spesso sono impiegate sui sistemi digitali di piccole dimensioni di cui al punto precedente.

(4) Il repertamento prosegue con le **memorie semipermanenti portabili di natura elettromagnetica** (hard disk portabili, usb key, ecc.) che possono risultare collegati al sistema digitale che le impiega attraverso connessioni wireless, USB, firewire, bluetooth, ecc..

(5) Si devono repertare quindi i **personal computer** ed i **sistemi elettronici speciali** (skimmer, sensori, spie ambientali, malware, ecc.) eventualmente presenti.



Isolare l'area:

a. I^a Regola:

- persone non autorizzate fuori dall'area;
- nessuno deve toccare i dispositivi;
- ciò che è SPENTO deve rimanere tale.

a. II^a Regola:

- se vi sono dispositivi che stanno inevitabilmente per perdere dati, ispezionarli manualmente nei limiti delle proprie conoscenze, riprendendo il tutto via videocamera e

riportando successivamente sia le azioni che i risultati in uno specifico verbale.

b. III^ Regola:

- individuare prese telefoniche, elettriche e di rete - hub, switch, "strani" computer o sistemi elettronici - e filmare il tutto, per poi annotare, vocalmente e per iscritto, una descrizione anche sommaria.

Nota: Tastiere, FD, CD ecc. possono riportare impronte digitali per cui devono sempre essere trattati con i previsti guanti. Si tenga presente che l'eventuale estrazione di impronte digitali può talvolta essere motivo di alterazione DEFINITIVA del dispositivo.

Raccogliere le informazioni:

- a. Identificare le persone di interesse e separarle.
- b. Richiedere ed annotare le seguenti informazioni:
 - Possessori dei dispositivi ed abituali utilizzatori;
 - Username e Password per file, hardware e connessioni Internet (es. password del BIOS, system login, network or ISP, application files, encryption pass phrase, e-mail, access token, ecc.);
 - Impiego del sistema;
 - Schemi di sicurezza dei dispositivi (se presenti);
 - Eventuali dispositivi di memorizzazione sul larga scala;
 - Documentazione relativa al sistema (se presente).

Repertamento:

Come già visto a un punto di vista concettuale esistono due livelli di repertamento di un sistema informatico o telematico:

- il **repertamento dell'oggetto fisico** (in genere il supporto magnetico e/o ottico che mantiene memorizzati i dati);
- il **repertamento dei dati (virtuale)**, che in ambito forense internazionale viene identificato con il termine "*data copying*" o clonazione dei dati o "*forensic copy*" (copia forense).

Nel repertamento fisico si deve identificare il dispositivo e tutte le periferiche hardware: tastiera, monitor, stampanti e altro ancora. La regola

generale è prendere possesso di tutto l'hardware, incluse le periferiche. Generalmente il repertamento fisico anticipa quello dei dati ma si noti che questa ormai non è più una regola fissa: sono infatti diffusi dei sistemi di repertamento dei dati che consentono di registrare il contenuto dati di un PC senza necessariamente prelevare dalla scena del delitto e trasportarlo in un laboratorio specializzato.

Il repertamento dei dati è attività dello specialista informatico, o di chi abbia una specifica preparazione.

RICORDARE: la ricerca delle prove elettroniche richiede talvolta specifiche autorizzazioni da parte della magistratura (es. indagine su server).

Principio: i reperti elettronici devono essere trattati con molta cura ed impacchettati con diverse protezioni (es. cartone arrotolato). Devono inoltre essere tenuti accuratamente LONTANI DA CAMPI ELETTRICITÀ (altoparlanti, cellulari, luce solare, ecc.) E DA FONTI DI CALORE O RADIAZIONI.

Elementi correlati alle prove elettroniche sono:

- fogli, appunti e post-it ritrovati in prossimità dei dispositivi elettronici con scritte frasi o testi anche di piccole dimensioni (per le parole chiavi);
- calendari con appunti, annotazioni e scritte varie;
- fotografie appesi sopra il computer;
- appunti/libri di vario genere tenuti vicini al computer.

Nota: prima di repertare, si suppone che la documentazione descrittiva della scena del crimine sia completa (foto, video, ecc.) ricordando di fare riprese video e/o fotografiche anche agli eventuali collegamenti dei dispositivi.

ATTENZIONE: L'IMPIEGO DEI GUANTI DI PROTEZIONE E' SEMPRE RILEVANTE SULLA SCENA DEL CRIMINE! ANCHE QUANDO SI TRATTANO SISTEMI INFORMATICI, ELETTRONICI E/O TELEMATICI!

Repertamento di Computer (Desktop/Laptop)

Si individuano desktop (da tavolo) e laptop (portatili).

I "laptop" integrano tutto in una singola unità di medie dimensioni. Presentano il problema dell'alimentazione elettrica sia tramite rete (220V) che tramite batteria interna.

Documentare e isolare la scena:

- prendere nota di tutto quello che si nota sul sistema, compresi ovviamente i dati sul monitor i quali per sicurezza possono essere ripresi tramite videocamera;
- evitare di interagire con il sistema. Laddove sia indispensabile produrne documentazione a verbale e/o su video.

ATTENZIONE: se sono presenti più computer è plausibile l'esistenza di una rete; allo stesso modo, una rete locale è in genere sempre presente all'interno di aziende. In tali casi il repertamento è difficile e possono essere facilmente commesse violazioni legali.

Nel caso di reti locali bisogna contattare l'esperto forense e richiedere un intervento specifico; nel frattempo bisogna individuare l'AMMINISTRATORE DEL SISTEMA: quest'ultimo dovrà garantire di "congelare la situazione".

- a. Se il computer è **SPENTO**, deve rimanere tale, fine attività.
- b. Se il computer è **ACCESO**, prendere nota della situazione e seguire la procedura seguente:
 - (2) **Situazione 1:** sul monitor è resa disponibile la normale attività della macchina
 - (a) prendere nota di ciò che si vede e riprendere il monitor via video camera;
 - (b) Se non si ha la preparazione tecnica minima prevista passare al punto c.
 - (c) Se si ha la preparazione tecnica minima indispensabile si procede alla **ispezione virtuale** dei dati disponibili. Ciò soprattutto nei casi che seguono:
 - (b.1) presenza di programmi di crittazione;
 - (b.2) presenza di programmi di anti-forensics;
 - (b.3) presenza di dati online in procinto di perdersi (es. webmail, siti web, dati non salvati su hard disk, ecc.)

- (b.4) possibilità di ispezionare la RAM con tool speciali alla ricerca di password o dati specifici (attività specialistica).
- (d) passare al punto c.
- (3) **Situazione 2:** screen saver attivo o monitor in "sleep"
 - (a) muovere il mouse e verificare il risultato;
 - (b) se il movimento del mouse non causa cambiamenti, **NON ESEGUIRE ALTRE AZIONI SUL COMPUTER;**
 - (c) prendere nota e riprendere il monitor via videocamera;
 - (d) passare al punto c..
- (4) **Situazione 3:** Monitor spento
 - (a) prendere nota e, mentre si riprende il monitor tramite videocamera, attivare SOLO il MONITOR e rivedere le due situazioni precedenti.
- c. Se si è proceduto all'ispezione virtuale e risultano dati da prelevare sulla scena a causa di urgenza per la loro possibile perdita:
 - (1) riprendere l'attività tramite videocamera;
 - (2) connettere con l'eventuale presa USB l'hard disk destinatario;
 - (3) prendere nota a verbale di data, orario e seriale della memoria collegata;
 - (4) se si hanno dei tool software forensi per la copia sulla scena del crimine procedere con essi dandone atto a verbale;
 - (5) se non si hanno i tool forensi di copia si deve procedere con cautela attraverso la classica funzione di copia prevista dal sistema operativo della macchina (**SI DEVE FARE ATTENZIONE A NON APRIRE NESSUN FILE MA LIMITARSI AL PROCESSO DI COPIA**).
- d. **SPEGNERE FORZATAMENTE IL COMPUTER** mediante rimozione dei cavi di alimentazione; nel caso di laptop, **RIMUOVERE ANCHE LA BATTERIA** (alcuni laptop hanno anche una seconda batteria di riserva!).
 Alcuni sistemi sono collegati a gruppi di continuità per cui è necessario staccare i cavi da dietro il computer e non solo le connessioni a muro.
- e. Prendere nota di eventuali connessioni (es. tel, modem, cavi, ISDN, DSL). Qualora sia presente un telefono in prossimità del computer, rilevarne il numero.
- f. Per evitare danneggiamenti, prelevare gli eventuali FD e chiavette USB inseriti ed etichettarli a parte.
NON RIMUOVERE CD dal drive relativo.
- g. Riprendere tutte le attività tramite videocamera.

- h.** Prendere nota di modello, numero seriale ed altri eventuali ID.
- i.** Fare foto alle connessioni etichettate.

SCHEMA RIASSUNTIVO REPERTAMENTO COMPUTER

SISTEMA SPENTO → REPERTAMENTO FISICO → STOP.

SISTEMA ATTIVO
↓
SISTEMA IN RETE LOCALE
↓
CONTATTA CONSULENTE/AMMINISTRATORE

SISTEMA ATTIVO
↓
SISTEMA ISOLATO O CONNESSO AD INTERNET
(chiavetta UMTS o linea ADSL)
↓
NESSUN DATO RILEVANTE SULLO SCHERMO
↓
SPEGNIMENTO E REPERTAMENTO FISICO
↓
STOP.

SISTEMA ATTIVO
↓
SISTEMA ISOLATO O CONNESSO AD INTERNET
(chiavetta UMTS o linea ADSL)
↓
DATI RILEVANTI SUL MONITOR
↓
ISPEZIONE VIRTUALE
↓
REPERTAMENTO VIRTUALE
↓
SPEGNIMENTO E REPERTAMENTO FISICO
↓
STOP

Repertamento di altri tipi di dispositivi elettronici

I dispositivi che sono menzionati di seguito possono facilmente perdere dati se trattati impropriamente: per questo motivo sarebbe sempre buona norma impiegare un esperto per il loro trattamento.

Ragioni di urgenza, però, possono giustificare un intervento immediato anche non specialistico, motivo per il quale vengono menzionati alcuni suggerimenti.

Esempi di dispositivi:

- Audio recorder
- Answering machine
- Cable
- Caller ID device
- Cellular telephone
- Chip
- Copy machine
- Databank/Organizer digital
- Digital camera
- Dongle o alter chiavi hardware
- Drive duplicator
- External drive
- Fax machine
- Flash memory card
- Floppy, diskette
- CD-ROM
- GPS device
- Pager
- Palm Pilots/electronic organizer
- PCMCIA card
- Printer
- Removable media
- Scanner (film, flatbed, watches, etc.)
- Smart card/secure ID token
- Telephone
- VCR
- Wireless access point

Nota: se si sequestrano dispositivi removibili, come Zip®, Jaz®, ORB, Klik!™, Syquest, LS-120, sarebbe buona norma repertare anche i relativi dispositivi di lettura (se presenti).

a. TELEFONI CELLULARI

Se si sospetta che un cellulare possa contenere informazioni pertinenti al caso bisogna procedere come segue:

- (1) Per mantenere i dati presenti nell'apparecchio:
 - agire con guanti monouso se è prevista una successiva analisi dattiloscopica;
 - nel caso il cellulare sia spento, lo si DEVE lasciare spento;
 - nel caso il cellulare sia attivo si può procedere all'**ispezione virtuale** facendo attenzione a non effettuare chiamate o operazioni di alcun tipo in ambito comunicativo (al massimo la visione dei numeri in memoria e degli SMS, ma senza spostare fisicamente il cellulare da dove si trova);
 - nel caso il cellulare sia attivo, spegnerlo rimuovendo la batteria;
- (2) Raccogliere gli accessori connessi o in dotazione al cellulare:
 - ricercare e raccogliere tutti i possibili cavi e/o accessori in dotazione al cellulare (ad es. cavi di collegamento, carica batterie);
 - annotare o evidenziare in qualsiasi modo, lo stato nel quale si è rinvenuto l'apparecchio, in modo da stabilirne l'uso per il quale esso veniva impiegato (ad es. possibile connessione al portatile);
- (3) Eventualmente, nel caso in cui il cellulare sia acceso, fotografare se possibile il display e/o riprenderlo su video, ciò anche durante l'ispezione virtuale così da acquisire velocemente i dati
- (4) Procedere alla classificazione e all'imballaggio dei dispositivi:
 - annotare tutte le caratteristiche dei cellulari repertati (modello e stato al momento del sopralluogo, accessori dell'apparecchio);
 - conservare e annotare tutti gli appunti rinvenuti in prossimità o ricollegabili ai cellulari che possano contenere numeri o codici (PIN, PUK, ecc);
 - conservare singolarmente ogni reperto.

Nell'attesa che il tecnico forense disponga dei dispositivi sequestrati, custodirli in luogo chiuso, avendo cura di preservare l'imballo.

SCHEMA RIASSUNTIVO REPERTAMENTO TELEFONO CELLULARE



b. TELEFONI CORDLESS

Se si sospetta che un telefono cordless possa contenere informazioni pertinenti al caso, al fine di mantenere i dati presenti nell'apparecchio:

- agire con guanti monouso se è prevista una successiva analisi dattiloscopica;
- nel caso il dispositivo sia spento, lo si DEVE lasciare spento ed imballarlo;

- nel caso il dispositivo sia attivo, non effettuare chiamate od operazioni di alcun tipo e non allontanarlo dalla base-station;
- nel caso il dispositivo sia attivo, curarsi di tenere sempre alimentata la base station e di agganciarvi sopra la cornetta, per poi richiedere l'intervento del tecnico forense;
- riprendere con videocamera o macchina fotografica il dispositivo.

c. SEGRETERIE TELEFONICHE

Se si sospetta che una segreteria telefonica possa contenere informazioni pertinenti al caso, per mantenere i dati presenti nell'apparecchio:

- agire con guanti monouso se è prevista una successiva analisi dattiloscopica;
- nel caso il dispositivo sia spento, lo si DEVE lasciare spento ed imballarlo;
- nel caso il dispositivo sia attivo, premunirsi di mantenerlo attivo staccandolo dalla linea telefonica in quanto nuove chiamate potrebbero andare a cancellare quelle già registrate;
- riprendere con videocamera o macchina fotografica il dispositivo.

d. CERCA PERSONE

Se si sospetta che un cerca-persone possa contenere informazioni pertinenti al caso, per mantenere i dati presenti nell'apparecchio:

- agire con guanti monouso se è prevista una successiva analisi dattiloscopica;
- nel caso il dispositivo sia spento, lo si DEVE lasciare spento ed imballarlo;
- nel caso il dispositivo sia attivo, premunirsi di mantenerlo attivo e navigare tra i messaggi presenti riprendendo l'azione con videocamera e descrivendo poi tutto con apposito verbale di operazioni tecniche.

e. FAX

Se si sospetta che un fax possa contenere informazioni pertinenti al caso, per mantenere i dati presenti nell'apparecchio:

- agire con guanti monouso se è prevista una successiva analisi dattiloscopica;

- nel caso il dispositivo sia spento, lo si DEVE lasciare spento ed imballarlo;
- nel caso il dispositivo sia attivo, chiamare il tecnico forense.

f. CARTE DI CREDITO E SISTEMI CORRELATI

Per mantenere inalterati i dati presenti in un sistema di clonazione di carte di credito, al momento del repertamento dovreste seguire, nel luogo di intervento, i seguenti principi:

- (1) Raccogliere e conservare le carte di credito in modo da:
 - mantenerle debitamente distanti da qualsiasi tipo di fonte di calore od elettromagnetica;
 - annotare gli elementi significativi delle carte repertate (intestatario, numeri sovra impressi, ecc), anche facendo una fotocopia delle stesse;
 - repertare le schede raccolte riponendole singolarmente in una bustina antistatica.
- (2) Repertare anche gli eventuali sistemi di lettura/scrittura:
 - nel caso si tratti di uno skimmer di carte (un sistema stand alone alimentato a batteria e non collegato ad un terminale), non tentare operazioni di alcun tipo facendo scorrere supporti magnetici nel lettore.
 - non staccare la batteria che alimenta il supporto per evitare che vadano persi eventuali dati contenuti nella memoria volatile;
 - nel caso si tratti di un sistema collegato ad un PC, sarà necessario repertare anche quest'ultimo oltre che il sistema di lettura (secondo le modalità riferite al repertamento di PC);
 - è sempre utile effettuare alcune foto o riprese video degli apparati hardware.
- (3) Raccogliere la documentazione connessa al sistema di clonazione:
 - è utile conservare accuratamente qualsiasi tipo di documentazione che possa trattare le intenzioni, i progetti dell'organizzazione che usava il sistema rinvenuto;
 - controllare che non vi siano componenti elettroniche di possibile interesse nei cestini limitrofi.

g. ALTRI DISPOSITIVI ELETTRONICI

Contattare il tecnico forense per consigli...

Repertare ed analizzare elementi virtuali (Internet e file)

a. SITI WEB

Repertare un sito web (es. www.carabinieri.it) o una email diviene sostanzialmente differente dal repertare un oggetto fisico in quanto i due citati elementi sono esclusivamente formati da dati e non hanno un necessario corrispettivo fisico.

A livello legale molti ancora ritengono che non esista un modo univoco e preciso per repertare un sito web: in molti casi si assiste alla presentazione della stampa del sito in dibattimento, annettendo tale informazione cartacea quale possibile fonte di prova di un fatto criminoso, ma sfortunatamente un sito web è qualcosa di molto più dinamico e complesso di un foglio di carta e né la sua immagine né il suo contenuto momentaneo lo qualificano del tutto.

A livello investigativo ci si limita a registrare l'URL¹⁶ ossia l'indirizzo (es. www.carabinieri.it) per poi lasciare al tecnico forense le varie operazioni di analisi ed eventuale tracciamento del creatore del sito stesso.

Oltre alla non fisicità "dell'oggetto" da repertare, sopravvengono altri problemi che gli investigatori si troveranno ad affrontare, a volte vanamente.

Di fondamentale interesse per le indagini è il fatto che ogni server crea dei file di "log" sui quali vengono archiviate le informazioni relative all'indirizzo IP dell'utente, al tipo di servizio del quale ha usufruito, nonché ai riferimenti di tempo relativi quando questo è avvenuto.

Il metodo classico, con il quale avvengono i repertamenti sulle reti è mediante l'acquisizione dei file di log.

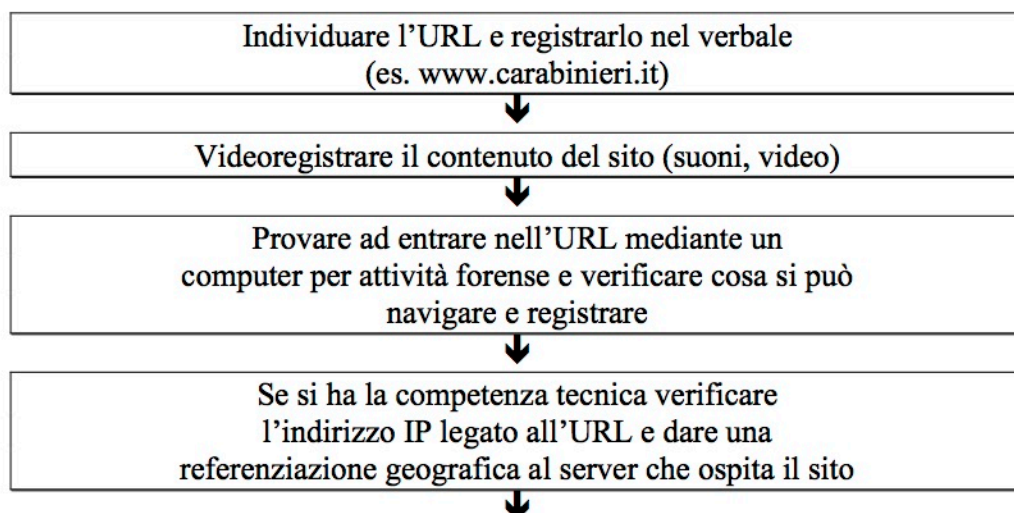
¹⁶ URL: Uniform Resource Locator, una sequenza di caratteri che identifica univocamente l'indirizzo mnemonico di una risorsa in Internet. Ogni nodo collegato su Internet deve avere un IP address ossia un indirizzo univoco in quell'istante (se IPv4 è costituito da 32 bit (4 byte) suddiviso in 4 gruppi da 8 bit (1 byte), separati ciascuno da un punto (notazione dotted), se IPv6 è costituito da 128 bit (16 byte), viene descritto da 8 gruppi di 4 numeri esadecimali che rappresentano 2 byte ciascuno (quindi ogni numero varia tra 0 e 65535) separati dal simbolo "due punti" – fonte wikipedia.org). L'URL viene associato proprio all'IP address per ragioni mnemoniche e commerciali.

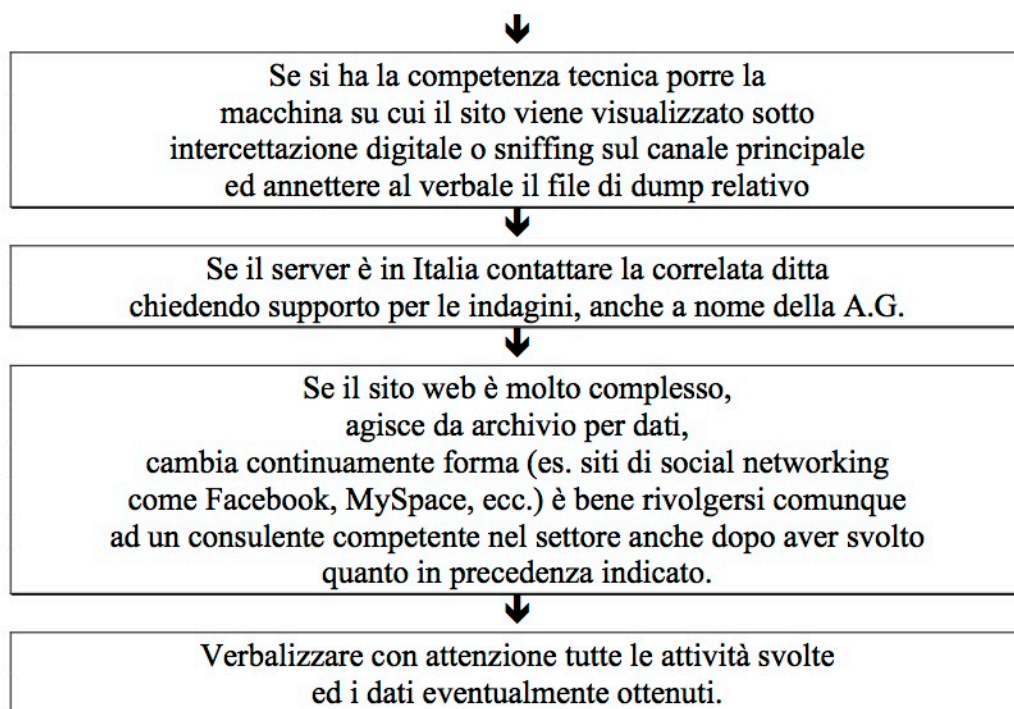
Al fine di individuare quale utente è associato all'indirizzo IP scaturito dall'analisi dei file di log, sarà necessario ripercorrere a ritroso l'instradamento dei dati seguendo nodo per nodo sino ad arrivare al server che ha erogato il servizio. Tale procedura investigativa è denominata tracciamento dell'indirizzo IP

Quando tale attività conduce presso server esteri si incontrano legislazioni e sistemi giudiziari differenti, in deroga ai quali esistono particolari convenzioni che permettono all'indagine di avere ulteriore corso, parimenti a quanto avviene nel territorio nazionale. Nel caso che gli stati interessati dall'indagine non aderissero a tali convenzioni, l'indagine si bloccherà non potendo in tal caso acquisire i file di log.

Ulteriori problematiche sono date da tecniche di mascheramento dell'IP mediante proxy o di occultamento dell'informazione trasmessa mediante i servizi di Tunneling, tutti offerti da un numero di siti sempre maggiore, che rendono quasi impossibili le indagini.

SCHEMA DI REPERTAMENTO DI UN SITO WEB GENERICO TROVATO APERTO SU UNA MACCHINA DELLA SCENA DEL CRIMINE





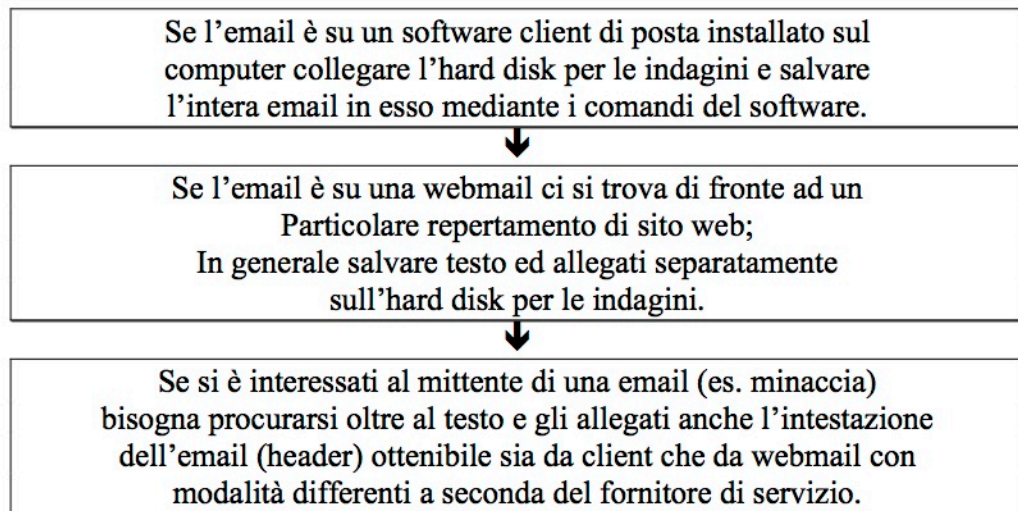
b. EMAIL

Per l'email (Electronic Mail = Posta elettronica), data la vicinanza del concetto a quello di "cartolina postale" (molta attenzione – cartolina e non lettera!) si può dire qualcosa in più sul repertamento. Per mantenere inalterati i messaggi di posta elettronica al momento del repertamento si devono seguire, nel luogo di intervento, i seguenti principi:

- (1) Mantenimento degli elementi significativi del file e corretta spedizione:
 - nel caso si abbia a che fare con il **programma di posta elettronica** come Microsoft Outlook (o comunque un client simile) occorre selezionare il messaggio da estrarre, scegliere l'opzione "salva con nome" dal menu "file" (verrà prodotto un file ad esempio con estensione ".eml" oppure ".msg") ed esportare il tutto verso l'hard disk per le indagini preventivamente preparato; operando in questo modo, saranno conservate tutte le informazioni sensibili del documento;

- conservare il file trattandolo con un software di crittazione (ad esempio Pgp) o, in alternativa, utilizzando un programma di compressione come Winzip che assicuri la protezione tramite l'impostazione di una password di almeno 20 caratteri alfanumerici;
 - fare più copie dello stesso file su supporti diversi (ad esempio FD, CD-R, ecc.);
 - in caso si debba spedire il messaggio via e-mail, avere cura di spedire il file, ottenuto con la procedura suddetta, come allegato;
- (2) Trattenere un quadro dei contatti dell'utente:
- può essere utile inviare anche una lista contatti dell'utente, salvando la rubrica presente nel programma, ed inviandola insieme al documento in questione, estraendola in più formati diversi (per Outlook Express si procede selezionando dal menù l'opzione "esporta" e poi selezionando il formato ".csv" oppure ".wab");
 - non accedere agli eventuali allegati.
- (3) Nel caso si tratti di una **webmail**, ossia non ci sia il software di client installato sulla macchina in analisi ma si acceda alla posta da web (es. www.tiscali.it o www.gmail.com) :
- Caso URGENTE: bisogna provvedere sul posto a prelevare tutti i dati altrimenti si corre il rischio di perderli irreparabilmente in quanto alla indisponibilità delle password di accesso all'area.
 - Non si propone ovviamente il problema del testo delle email che può essere copiato ed incollato su un file dell'hard disk per le indagini opportunamente collegato (USB o altro).
 - Gli allegati devono essere scaricati sempre sul citato hard disk per le indagini, lo stesso dicasi per indirizzi, rubriche, eventuali discussioni di chat rinvenibili ecc.
- (4) Qualora si sia interessati ad **individuare il reale mittente** di una email falsificata (es. minaccia):
- Il testo dell'email, pur essendo essenziale al reato, NON lo è generalmente ai fini di tracciamento.
 - Fondamentale invece è l'intestazione (**header**) dell'email (normalmente non visibile all'utente) che ogni webmail e client di posta provvede a fornire secondo una sequenza personalizzata di comandi.

SCHEMA DI REPERTAMENTO DI UNA EMAIL SULLA SCENA DEL CRIMINE



c. ALTRO...

Esistono diverse altre forme di comunicazione su Internet per le quali ancora non sono state rilasciate neanche bozze di protocolli riguardo al processo di repertamento, per cui il contatto con l'esperto forense è essenziale in questo caso.

Si riportano ad ogni modo delle indicazioni nei casi piuttosto comuni che seguono:

- IM: diversi dati di comunicazioni sono contenuti in maniera sufficientemente permanente nell'hard disk della macchina che opera per cui spegnendo i rischi di perdita dei dati sono medio-bassi. Conviene ovviamente prendere nota degli account evidenziati ed anche delle discussioni eventualmente poste in risalto (tramite note scritte e video);
- Emule: lascia la maggioranza delle informazioni sulla memoria di massa e quindi si può procedere allo spegnimento del sistema dopo aver preso nota dello stato generale del software;
- Kazaa: simile ad Emule;

- Skype: le ultime versioni crittano il contenuto dei dati anche in locale per cui si devono acquisire quante più informazioni possibili mentre il programma è in funzione. Può accadere infatti che dopo lo spegnimento niente sia più reperibile.

Repertamento in rete

La maggior parte delle attività che vengono svolte per eseguire il repertamento su Internet, sono valide anche per qualsiasi altra Rete, essendo proprio Internet definita la rete delle reti o meglio l'insieme di tutte le reti disomogenee interconnesse tra loro in modo tale da poter comunicare mediante un unico protocollo, il TCP/IP.

Quando si parla di repertamento in rete si intende un'attività da eseguire online o comunque su i server oggetto dell'indagine in funzione.

Questo avviene ogni qualvolta si incontrano grandi reti aziendali alle quali sono annesse macchine molto performanti adibite a gestire un grande numero di utenti e/o informazioni, pertanto qualsiasi loro interruzione comporterebbe enormi danni economici sia per la società che per tutti gli utenti che accedono al servizio.

In questi casi non sarà possibile procedere al sequestro dei computer o delle memorie di massa da essi utilizzate, secondo la normale procedura prevista dagli articoli 253 e 321 del CPP, ma bensì si dovrà procedere in loco all'acquisizione dei dati di interesse per le indagini.

Si eseguirà quindi un accertamento di tipo irripetibile, ai sensi dell'art. 360 del CODICE DI PROCEDURA PENALE che potrà essere effettuato unicamente da personale specializzato.

10.3 Imballare, trasportare ed immagazzinare

Problemi in questa fase possono provenire da:

- Degradazione magnetica degli apparati;
- Degradazione elettrica degli apparati;
- Calore;
- Umidità troppo alta o troppo bassa;
- Luce del sole;
- Vibrazioni e shock meccanici.

L'imballo ha lo scopo:

- 1) proteggere il reperto dagli agenti evidenziati;
- 2) costituire un item facilmente individuabile nei verbali della catena di custodia;
- 3) garantire l'autenticità di quanto repertato.

Il luogo di preservazione dei reperti deve garantire l'assenza di polveri, sbalzi di umidità e temperatura nonché l'assenza di campi elettromagnetici. Spesso può includere gabbie di Faraday e/o contenitori antistatici. Nel migliore dei casi dovrebbe essere spazialmente organizzato e gestito attraverso procedure automatiche che possono associare al reperto ed alla rispettiva catena di custodia la sua precisa posizione.

Il DEFR durante imballo e trasporto deve:

- 1) completare l'imballo con un sigillo secondo quanto previsto dal CODICE DI PROCEDURA PENALE
- 2) trattare i reperti sempre con i previsti guanti;
- 3) evitare di toccare le memorie magnetiche nelle loro zone di magnetizzazione se accessibili (ma sarebbe consigliabile che toccassero le citate memorie il meno possibile in generale);
- 4) associare ad ogni reperto una precisa etichetta a lettura ottica o elettronica così da realizzare un'associazione univoca nei documenti della catena di custodia.
- 5) evitare di lasciare parti dei reperti in possibile movimento (es. sportellini non bloccati, drive aperti, ecc.).
- 6) non consentire alle batterie eventualmente presenti di scaricarsi.
- 7) evitare di trattare reperti che possano avere sopra tracce di natura biologica.

a. Procedura di trasporto:

- tenere lontani i reperti dalle radio-trasmittenti, dagli altoparlanti, dall'aria condizionata e dalle fonti di calore;
- non far permanere i reperti in auto per lunghi tempi (es. giorni);
- preservare i reperti da shock meccanici e vibrazioni;
- tenere lontani i reperti da monitor e cellulari;
- curare i verbali di trasferimento dei reperti.

b. Procedura di immagazzinamento:

- etichettare i reperti imballati con una copia del verbale di sequestro o trasporto;

- l'area magazzino dovrebbe avere temperatura stabile e minima umidità, essere protetta da fonti magnetiche ed al riparo dalla luce del sole.

Nota: si deve essere consapevoli del fatto che qualora un computer venga tenuto in magazzino per lungo tempo (es. più di un anno), potrebbe scaricarsi la batteria interna e quindi potrebbero perdersi i valori temporali del BIOS e con essi qualsiasi validità di tutte le date e orari rinvenibili sull'hard disk.

c. Reperti virtuali

- I reperti virtuali sono sostanzialmente file generalmente di grandi dimensioni ottenuti da copie totali o parziali di dati di sistemi attivi.
- Sono contenuti necessariamente in una memoria semipermanente (es. hard disk) o permanente (es. CD-R) che costituisce a tutti gli effetti l'involucro / imballo.
- Il sigillo di tali reperti (il file e non il loro contenitore) è una funzione matematica one-way¹⁷ che associa al file uno ed un solo valore di stringa alfanumerica la quale deve essere annessa al verbale inerente la catena di custodia.
- Il trasporto dei reperti virtuali è in realtà una trasmissione di dati. Qualora si tratti di trasporto fisico della memoria-involucro si torna alla questione precedente (reperti fisici). Se invece si tratta di invio tramite mezzo di trasmissione (es. email) allora bisogna "rinchiudere" il file (reperto virtuale) dentro un altro file che faccia da contenitore (es. un file compresso) e proteggere quest'ultimo con una password. Successivamente si invia il file protetto ed il valore calcolato dalla funzione one-way per la verifica di integrità.

¹⁷ Le funzioni di hash sono descritte nel documento ISO/IEC 10118-1: 2000 – a scopo forense è tipico l'impiego degli standard MD5 e SHA1.

Testi ed Articoli Scientifici:

1. Simson L. Garfinkel, *"Digital forensics research: The next 10 years"* digital investigation 7 (2010) S64-S73 – Elsevier (www.sciencedirect.com)
2. G. Peterson , S. Sheno, *"Advances in Digital Forensics V"* (IFIP International Federation for Information Processing) – Springer edition (January 26-28, 2009)
3. E. Casey, *"Digital Evidence and Computer Crime"* – Third edition – Academic Press (2011)

Siti web:

4. Shelton Donald E. *"The 'CSI Effect': does it really exist?"* NIJ J March 2008;259, <http://www.ojp.usdoj.gov/nij/journals/259/csieffect.htm>
5. M. Mattiucci *"Digital Forensics"* <http://www.marcomattiucci.it>
6. IISFA – Italian Chapter – <http://www.iisfa.it>

Standard guidelines:

7. ISO/IEC 27037 *"Guidelines for identification, collection, acquisition, and preservation of digital evidence"* (in tutte le sue release)
8. ENFSI-FIT-WG *"Guidelines for Best Practice in the Forensic Examination of Digital Technology"* (v.6 2009)
9. ACPO (2011) *"Good Practice Guide for Computer-Based Electronic Evidence"*
10. U.S. Secret Service (2011) *"Best Practices for Seizing Computer evidence"* del;
11. SWGDE (2011) *"Model Standard Operating Procedures for computer forensics"*