Gli Strumenti Open Source dell'Investigatore Digitale.

L'informatica, è innegabile, si è insinuata ormai in ogni singolo momento della nostra vita quotidiana. Solo fino a una quindicina d'anni fa, per fare un esempio, i telefoni cellulari erano riservati a pochi "fortunati", i personal computer scarsamente diffusi e tutte le informazioni conservate dalla Pubblica Amministrazione, relative alla vita sociale, erano stipate in archivi cartacei polverosi e ingombranti. Ciò che oggi sta nella normalità del quotidiano sino a qualche decennio fa era a dir poco fantascientifico. L'informatica è entrata nella vita di tutti i giorni in modo così dirompente da rappresentarne un aspetto ormai imprescindibile. Il terrore che questo nuovo vivere tecnologico possa, all'improvviso, venire a mancare è emersa in tutta la sua ampiezza già mesi prima dell'inizio del nuovo millennio. Si parlava di millennium bug. Una situazione che ha rovesciato la sua ispirazione persino sul cinema. Penso a "Mac" (Sean Connery) che nel film Entrapment sfruttava proprio il momento di passaggio all'anno 2000 per mettere a segno il colpo più importante della sua vita.

La tecnologia accompagna quindi ogni scansione della giornata.

Ed è inevitabile che l'informatica sia approdata anche nelle aule dei tribunali. Recenti fatti di cronaca hanno dimostrato quanto possa incidere un'analisi di informatica giuridica nell'evoluzione di un procedimento penale quando, ad esempio, si debba determinare per quanto tempo il computer dell'indagato sia rimasto acceso nel giorno del delitto. Però informatica e diritto (specialmente il diritto processuale, che regola lo svolgimento dei vari tipi di procedimenti) non seguono sempre le stesse logiche. L'ingresso dell'informatica nella dimensione del diritto è subordinato al rispetto delle regole che in questo mondo disciplinano le fasi che conducono, nella normalità dei casi, alla sentenza che decide il merito della causa.

È nata così la computer forensics (o informatica forense), ossia quella scienza che si occupa di rendere fruibili in ambito processuale le varie sfaccettature dell'informatica e, in generale, di attribuire un valore probatorio alle informazioni ricavate da particolari operazioni scientifico-investigative su un flusso di dati, su un supporto di memorizzazione dei dati, o, genericamente, su un qualsiasi altro supporto capace di veicolare le informazioni in forma digitale. Il risultato dell'indagine informatica, in sostanza, deve poter assurgere a elemento in grado di incidere positivamente sulla decisione del giudice nel processo in cui si inserisce. Con il termine computer forensics, inoltre, si può indicare l'ampio genus capace di ricomprendere tutte le "specializzazioni" della computer forensics. Si parla, infatti, di network forensics (la computer forensic relativa ai dati passanti su rete privata o pubblica), di incident forensics (analisi dei dati di un sistema compromesso), ecc. In questo articolo ci occupiamo di computer forensics per una serie di buoni motivi. Innanzitutto perché tantissimi strumenti utilizzati dai forenser appartengono alla categoria del Software Libero e sono quegli stessi strumenti che potrebbero venirci in soccorso per uscire da una situazione critica nella quale sia incappato il nostro sistema operativo preferito (parliamo di GNU/Linux ovviamente).

Quella del forenser, inoltre, rappresenta una buona prospettiva lavorativa per molti che alla passione per l'informatica vogliano accostare una buona retribuzione. In ultimo perché la curiosità e l'interesse per imparare a utilizzare nuovi strumenti è la caratteristica che accomuna un po' tutti gli utenti del sistema operativo del Pinguino. Il buon forenser, però, dovrebbe essere in grado di operare sfruttando sia le conoscenze tecnico-informatiche che quelle giuridiche. Un'indagine informatica imprecisa o superficiale rischia di compromettere irrimediabilmente il risultato ultimo che si intendeva raggiungere.

NOZIONI DI DIRITTO

Per comprendere meglio i vari passaggi della computer forensics, e il perché di certe operazioni che potremmo realizzare anche per altre vie e con differenti strumenti, è opportuno affrontare, seppure en passant, alcune nozioni di diritto processuale, per poi giungere al cuore del nostro discorso, ossia le distribuzioni GNU/Linux orientate alla computer forensics e a una panoramica sui principali tool Open Source e al loro utilizzo. La computer forensics può essere utilizzata sia nei processi penali che in quelli civili, ma per attenerci al titolo di questo articolo, ci riferiremo prevalentemente al processo penale. Le competenze dei forenser, in ambito penalistico, possono essere richieste sia dalla polizia giudiziaria, sia dai pubblici ministeri e dai giudici, sia

dagli avvocati. La scienza dell'acquisizione delle prove digitali si colloca, rispetto al nostro sistema giuridico di tradizioni millenarie, in un momento recentissimo. I principi che regolano queste nuove prove non hanno subito ancora importanti stratificazioni empiriche e pronunce giurisprudenziali. Per utilizzare una terminologia cara agli informatici, potremmo dire che il rapporto tra computer forensics e il nostro procedimento penale è ancora in "fase beta". In altri paesi, come gli Stati Uniti, la situazione è ben diversa: sono stati fissati standard e procedure per tutti i singoli passaggi della computer forensics.

LE PROVE NEL PROCEDIMENTO PENALE

Le nozioni minime di diritto processuale penale che è importante qui richiamare riguardano, ovviamente, le prove nel procedimento penale.

Il processo penale di primo grado si suddivide, di regola, in tre fasi principali: le indagini preliminari, l'udienza preliminare e fase processuale vera e propria (in cui si colloca la sotto-fase del dibattimento, sede naturale di formazione delle prove in contraddittorio tra le parti del processo).

La prima fase, delle indagini preliminari, è dominata dalla figura del pubblico ministero e della polizia giudiziaria che, acquisita una notizia di reato, esegue tutte quelle operazioni necessarie per giungere alla determinazione di richiedere un provvedimento di archiviazione, o di rinvio a giudizio, se si ritiene che solo un processo penale potrà stabilire la responsabilità dell'indagato. La fase dell'udienza preliminare, invece, è una fase prevista per ragioni di economia processuale: si tratta della cosiddetta udienza-filtro alla quale consegue la sentenza di non luogo a procedere o il rinvio a giudizio. Nell'ultima fase, guidata dal giudice (che è terzo rispetto alla difesa e alla pubblica accusa), abbiamo il dibattimento che si conclude con una sentenza che può essere di proscioglimento o di condanna. Ciò che determina e guida il ragionamento del giudice del dibattimento (ossia il giudice che emana la sentenza) sono, normalmente, le risultanze istruttorie (prove o indizi). Nel nostro processo penale non esistono le prove legali (ossia quelle in presenza delle quali la decisione del giudice deve adeguarsi al loro risultato) in quanto il giudice penale può, eventualmente, anche decidere in modo diametralmente opposto (dandone adeguata motivazione in sentenza) rispetto ai risultati illustrati al giudice, ad esempio, dal perito in computer forensics (si veda l'art. 192 del codice di procedura penale).

In ciascuna delle tre fasi processuali che abbiamo sommariamente descritto, pertanto, la prova assume un significato differente. Solo nell'ultima fase, quella dibattimentale, conserva il suo significato più pieno.

La nostra Costituzione, infatti, prevede (art. 111, quarto comma) che la prova si formi a dibattimento nel contraddittorio delle parti. In questo modo viene consentito all'imputato di partecipare attivamente (anche a mezzo di propri consulenti tecnici ove occorra) al momento della formazione delle prove che è determinante per la sua condanna o assoluzione. Tuttavia l'esigenza di assicurare il contraddittorio tra le parti potrebbe emergere anche in una fase antecedente a quella dibattimentale e, per la precisione, in quella che si colloca nel momento antecedente alla conclusione della fase delle indagini preliminari. In questa evenienza è previsto l'istituto dell'incidente probatorio (artt. 392 ss. c.p.p.). Con l'incidente probatorio si congela nella fase delle indagini preliminari il momento processuale in cui vengono concesse all'indagato le medesime garanzie previste all'acquisizione della prova nella fase dibattimentale. Abbiamo una porzione della fase dibattimentale all'interno della fase delle indagini preliminari.

In questo modo il risultato dell'incidente probatorio potrà essere utilizzato per la decisione dal giudice del dibattimento.

I casi per i quali è previsto che si possa ricorrere all'incidente probatorio è limitato a quelle particolari ipotesi in cui – per ragioni di irripetibilità o di pericolo per la dispersione della prova derivante dal lungo lasso di tempo che potrebbe intercorrere tra commissione del reato e fase dibattimentale – vi sia il fondato timore che l'attesa della fase dibattimentale potrebbe disperdere o pregiudicare l'acquisizione della prova.

Tra le ipotesi in cui è possibile ricorrere all'incidente probatorio vi è quella in cui vi sia la necessità di effettuare un esame tecnico irripetibile.

Un esame tecnico (come può essere, ad esempio, il prelievo di una traccia ematica che determini la distruzione della traccia) si dice irripetibile quando, per le condizioni in cui deve essere eseguito, determinerebbe la perdita di tutte o di parte delle caratteristiche dell'elemento di prova, tale da rendere impossibile la ripetizione delle analisi sullo stesso oggetto. In campo informatico, data la delicatezza dei supporti da analizzare e la possibilità di deteriorare irrimediabilmente gli stessi, ci si troverà quasi sempre di fronte ad esami che, ab origine, presentino i caratteri dell'irripetibilità. Di fronte alla necessità di disporre un accertamento tecnico irripetibile il pubblico ministero dovrà arrestarsi e consentire alla controparte processuale di partecipare, nominando un proprio consulente tecnico, oppure di richiedere che l'esame si svolga seguendo le garanzie dell'incidente probatorio (al riguardo si vedano gli artt. 360 e 391decies, comma III, c.p.p.). Qualora, ad esempio, la difesa dell'imputato faccia espressamente riserva di promuovere incidente probatorio e ciò nonostante il pubblico ministero proceda ugualmente all'accertamento tecnico non ripetibile (a parte i casi in cui le analisi, se differite, non potrebbero più essere utilmente compiute), allora i risultati di quegli accertamenti non saranno utilizzabili nel dibattimento (art. 360 u.c. c.p.p.). A prescindere dalle restanti

complicazioni processuali è evidente, riassumendo, che le difficoltà legate alle digital evidences non dipendono unicamente dalla novità del medium quanto dalla difficoltà di veder rispettate le garanzie difensive dell'indagato dal perseguimento di una prova attendibile e capace di resistere alle contestazioni (che potrebbero esserle mosse in riferimento ad ogni singola fase di formazione, sia essa in quella dell'acquisizione, conservazione, analisi o presentazione). Il discorso potrebbe apparire noioso ma il nostro ordinamento, nel corso dei secoli, ha raggiunto alti gradi di civiltà giuridica (per quanto riguarda le garanzie processuali) che sarebbe veramente un paradosso perdere in "un bicchier d'acqua". Abbiamo già accennato alle fasi della computer forensics. Queste sono fasi di un procedimento, guidato dalle conoscenze tecnico- informatiche, che va dall'identificazione del mezzo sul quale eseguire le analisi sino alla presentazione dei risultati delle analisi al giudice perché possa utilizzarli per emettere la sentenza. Il valore probatorio che si deve ricercare è, ovviamente, un valore forte e capace di resistere alle contestazioni (che possono incidere sulle modalità di acquisizione, di conservazione, di estrazione o di rappresentazione dei risultati). Ma quali sono queste fasi? Sono le fasi canoniche (universalmente riconosciute) che permettono di riconoscere ad una sequenza di bit una valenza probatoria.

LE FASI DELL'ANALISI - L'IDENTIFICAZIONE

Le fasi in cui si può suddividere l'analisi forense sono: l'identificazione, la conservazione, l'acquisizione, l'analisi e la presentazione.

L'identificazione si colloca nel momento in cui l'esperto investigatore dovrà solitamente individuare il "contenitore tecnologico" dal quale estrapolare il materiale probatorio. Benché possa sembrare una fase priva di difficoltà, in realtà presenta numerosi profili da tenere in considerazione, e se pensiamo al proverbio "chi ben comincia..." comprendiamo quale sia l'importanza di questa fase.

Il computer forenser potrebbe essere chiamato a intervenire su uno strumento che può essere un personal computer o uno smartphone, una macchina fotografica digitale o una scheda di memoria, e così via. Inizialmente il suo compito sarà quello di congelare la situazione che si trova di fronte al fine di ottenere, in modo "pulito" (ossia senza inquinamento delle prove), quante più informazioni possibile. Deve muoversi immaginando di essere un elefante in un negozio di cristalli. Egli dovrà adottare la massima prudenza per conservare intatta la prova che si accinge a ricercare o prelevare. Immaginiamo che il nostro esperto si trovi di fronte a un computer: dovrà verificare se nelle vicinanze ci siano altri computer; se esso sia o meno alimentato elettricamente e acceso; se sia collegato a una rete; se vi siano processi attivi con utenti connessi da remoto; se siano presenti utenti o amministratori dovrà intervistarli (in particolare sull'esistenza o meno di password... ma senza far intervenire tali soggetti sulla macchina); dovrà descrivere le condizioni generali del luogo in cui si trova la macchina (anche per valutare la presenza di eventuali fonti di disturbi elettromagnetici); dovrà prestare attenzione a non toccarne la tastiera; se acceso non dovrà spegnerlo in modo convenzionale (si preferisce, nella maggior parte dei casi, togliere l'alimentazione elettrica in modo brutale, piuttosto che spegnere la macchina in modo convenzionale e rischiare, così, che il sistema operativo vada a intaccare quelle che potrebbero essere possibili prove); dovrà annotare l'ora precisa riportata dal computer (se già acceso); verificherà la presenza di tool anti-forensics (di cui si parlerà in seguito); dovrà annotare tutte le operazioni effettuate.

LE ALTRE FASI DELL'INDAGINE

La conservazione rappresenta, più che una fase, il collante tra tutte le fasi. Significa "mettere in freezer" e preservare la prova digitale in modo che nemmeno fattori esterni, come una forte influenza elettromagnetica, possano intaccarne la genuinità. Ciò comporta che si debba mettere in opera e tenere quella che viene definita chain of custody, ossia l'indicazione e la documentazione di ogni operazione che venga compiuta durante tutta la fase dell'esame forense. La chain of custody riguarderà, anche le copie bitstream (di cui parleremo in seguito) create a partire dall'originale adoperando (nella maggior parte dei casi) dei blocchi hardware in scrittura sui supporti magnetici contenenti le delicatissime digital evidences.

L'acquisizione rappresenta la fase di estrazione del contenuto dal contenitore. Perché i contenitori originali non vadano dispersi, deteriorati o, comunque, alterati a seguito delle investigazioni digitali, si eseguono delle copie speculari (comprensiva degli spazi vuoti in cui potrebbero "annidarsi" delle informazioni essenziali ai fini processuali) dei supporti da analizzare. Dall'analisi dei supporti-copia si ottengono risultati (ad esempio tracce di immagini pedopornografiche cancellate dal sistema o copie di e-mail o informazioni sulla modifica di file o sull'utilizzo del sistema informatico) che però devono essere resi in un linguaggio comprensibile all'autorità giudicante.

È questa la fase della presentazione, che deve allo stesso tempo semplificare il risultato probatorio ed evitare di interferire con la libertà di valutazione e di qualificazione giuridica riservata al giudice (jura novit curia).

PERCHÉ UTILIZZARE SOFTWARE LIBERO?

Tutte queste fasi possono essere gestite dall'investigatore digitale per mezzo del Software Libero, con una serie di profili positivi che, enunciati, possono

sicuramente rendere l'esposizione della prova digitale più convincente agli occhi del giudice. Ma quali sono i punti forti del Free Software in relazione a un processo penale? Innanzitutto occorre apprezzarne la disponibilità del codice sorgente. Questo aspetto permette di prevenire le eventuali contestazioni attinenti al corretto funzionamento del software in una qualsiasi delle fasi della computer forensics.

A tal proposito si consiglia la lettura della sentenza del 21 luglio 2005 del Tribunale di Bologna sul caso Vierika (www.penale.it/stampa. asp?idpag=182) nella parte in cui si afferma: "In termini generali, quando anche il metodo utilizzato dalla polizia giudiziaria non dovesse ritenersi conforme alla migliore pratica scientifica, in difetto di prova di una alterazione concreta, conduce a risultati che sono, per il principio di cui all'art. 192 c.p.p., liberamente valutabili dal giudice alla luce del contesto probatorio complessivo (fermo restando che maggiore è la scientificità del metodo scelto, minori saranno i riscontri che il giudice è chiamato a considerare per ritenere attendibili gli esiti delle operazioni tecniche)". Tra gli altri punti forti del Software Libero vi è la certezza che anche nell'ipotesi in cui la software house o il singolo programmatore venga a mancare, sarà sempre possibile: aggiornare o, comunque, risolvere i bug; adattare il software alle necessità investigative contingenti; apprezzare la maggiore compatibilità con filesystem differenti e con formati standard; la possibilità di effettuare il mount dei device da analizzare in modo da poter anche prescindere da un blocco hardware in scrittura sul supporto originale. L'investigatore digitale ha la fortuna di trovare all'interno di distribuzioni GNU/Linux confezionate ad hoc tutti i suoi strumenti da lavoro.

LE DISTRIBUZIONI GNU/LINUX

HELIX-KNOPPIX (www.e-fense. com/helix/).

Helix è una distribuzione derivata da Knoppix (probabilmente la più famosa distro-live basata su Debian) e supportata da E-fense, un'azienda che si occupa di investigazioni digitali e di computer security con il supporto di numerosi professionisti, tra cui esperti in computer forensics e reti, avvocati penalisti e programmatori. Helix, pensata inizialmente come strumento da utilizzare a uso interno dell'azienda E-fense, viene rilasciata alla fine del 2003.

DEFT (Digital Evidence & Forensics Toolkit) http://deft.yourside.it/

Progetto italiano basato su Kubuntu, guidato da Stefano Fratepietro, computer forenser e collaboratore del prof. Cesare Maioli del corso di Informatica Forense presso la facoltà di giurisprudenza di Bologna. L'ultimo aggiornamento di DEFT risale a maggio 2007.

IRITALY - www.iritaly-livecd.org/

IRItaly (Incident Response Italy) è un progetto nato presso il Dipartimento di Tecnologie dell'Informazione dell'Università Statale di Milano, Polo Didattico e di Ricerca di Crema. La distribuzione è basata su Gentoo Linux e disponibile nelle versioni base, network forensic, media forensic e win32.

FIRE - http://fire.dmzs.com/

Il progetto pare in stato di quiescenza, benché nell'ultima news sul sito si legge: "F.I.R.E isn't dead, just went silent for a little too long".

Altri progetti interessanti

PENGUIN SLEUTH KIT (http://penguinsleuth. org/index.php?option=com_ wrapper&Itemid=39); KNOPPIX-STD (http://s- t-d.org/); PLAN-B (www.projectplanb.org); FCCU (http://d-fence.be/); The Packet Master (www.thepacketmaster.com); Portable Linux Auditing CD – PLAC (http://sourceforge.net/projects/plac/ - Distribuzione GNU/Linux da CD-Card).

LINKOGRAFIA/BIBLIOGRAFIA

www.ncjrs.gov - Sito dal quale è possibile scaricare tanti documenti in tema di computer forensics, compreso Forensic Examination of Digital Evidence: A Guide for Law Enforcement del 2004 del Dipartimento di giustizia degli Stati Uniti;

www.cybercrimes.it - Interessante sito ricco di informazioni

www.utica.edu/academic/institutes/ecii/ijde/ - Rivista/forum di discussione in materia di computer forensics

http://penguinsleuth.org/index.php Piattaforma per la computer forensics

www.forensicfocus.com - Forum di discussione

www.ddj.com/184404242 – articolo del 2000 di Dan Farmer e Wietse Venema

L.Luparia – G. Ziccardi, Investigazione penale e tecnologia informatica, Milano, Giuffrè, 2007;

A.Ghirardini – G. Faggioli, Computer Forensics, Milano, Apogeo, 2007