1

Tecniche di Anti-Forensics: Creazione di un Falso Alibi Digitale

Aniello Castiglione, Giuseppe Cattaneo, Alfredo De Santis

Dipartimento di Informatica ed Applicazioni “Renato M. Capocelli”

Universita` degli Studi di Salerno, I-84084, Fisciano (SA), Italy castiglione@acm.org, cattaneo@dia.unisa.it, ads@dia.unisa.it Mario Ianulardo

Lawyer in Naples, Italy

marioianulardo@codicieleggi.it

Abstract

Recenti casi giudiziari hanno mostrato come le digital evidence siano sempre piu` utilizzate dalle parti processuali (difesa, accusa, parte civile). Le tracce digitali possono essere lasciate su computer, telefoni cellulari, macchine fotografiche ed anche su server di terze parti come ISP, gestori telefonici (sia fissi che mobili), gestori dei servizi Internet coinvolti quali YouTube, Picasa, Facebook, Gmail, DropBox. E` ipotizzabile che queste tracce digitali possano essere “confezionate” ad arte al fine di precostituire un alibi con l’ausilio di un complice.

In questo lavoro si mostra come sia possibile costruirsi da soli un alibi digitale senza bisogno complici. L’idea chiave e` quella di lasciare, nell’arco temporale dell’alibi, tracce digitali in maniera automatica e senza interventi umani. Le digital evidence cos`ı costruite saranno indistinguibili ex-post da quelle normalmente lasciate da un intervento umano e senza ricorrere ad automatismi. Nessuna indagine forense dopo aver soltanto analizzato tutte le tracce digitali potra` mai accertare chi ha prodotto quelle tracce, e cioe` se un intervento umano o un automatismo predisposto ad hoc. Tutto cio` rende ancora piu` marcata la differenza tra le evidenze digitali e le evidenze fisiche. Le digital evidence assumono quindi maggiore rilevanza se accompagnate da indizi e prove acquisite mediante tecniche di indagine tradizionale.

Index Terms

Digital Evidence; Anti-Forensics; Digital Forensics; Alibi Informatico; Alibi Digitale; Counter-Forensics.

May 31, 2010 DRAFT

2

I. IN T RO D U Z I O N E

Il ricorso sempre piu`massiccio all’uso di strumenti elettronici, informatici e telematici per lo svolgimento di attivita` lavorative e ricreative, ha determinato una enorme produzione di dati digitali. La pervasivita` della tecnologia elettronico-informatica ha comportato, pertanto, un sensibile aumento dei casi in cui i computer e gli apparati di comunicazione digitali vengono utilizzati come mezzo per com- mettere reati e, nel contempo, vengono sottoposti, anche in casi di commissione di reati non prettamente informatici, ad analisi forense al fine di trovare tracce utili alle indagini. Accade quindi che elementi idonei ad individuare responsabilita` in ordine alla commissione di reati siano costituiti da file contenuti nella memoria di un PC, di una videocamera, fotocamera, telefoni cellulari e quindi in numerosi tipi di supporti di memorizzazione di dati digitali.

Le digital evidence, in quanto caratterizzate dalla immaterialita` e dalla ubiquita`, possono rinvenirsi in ogni parte del mondo. Non solo perche` reperibili su tutta una serie di apparecchi connotati del requisito della facile trasportabilita` (telefoni mobili, PDA, laptop, strumentazione GPS) ma anche perche` nella stragrande maggioranza dei casi le digital evidence sono relative a tracce di connessioni IP, account di posta elettronica, dati conservati su server allocati anche in Paesi diversi da quello in cui risulta essere stato commesso un crimine. Appare ictu oculi evidente come la diversita` di legislazione vigente in ogni singolo Paese rappresenti un serio ostacolo alla applicabilita` di norme comuni che regolino le fasi di acquisizione delle digital evidence. Si tenga presente, altres`ı, che la digital forensics e` una scienza nuova tante`che solo nel febbraio 2008 l’America Academy of Forensic Sciences (AAFS) l’ha inserita tra le scienze forensi. Tale scienza appare diversa dalle altre scienze sia perche` non puo` considerarsi una scienza comparativa sia perche´ e` soggetta ad un continuo mutamento connesso all’inarrestabile processo di innovazione tecnologica. Infatti, mentre il DNA, il sangue, le impronte digitali non subiscono mutamenti essenziali nella struttura bens`ı risultano soggetti a mutamento la scienza ed i tool utilizzati per l’analisi dei predetti reperti; nel caso della computer forensics, invece, il mutamento coinvolge radicalmente non soltanto i tool necessari per l’individuazione, repertamento ed analisi delle tracce digitali ma anche le componenti strutturali ed elettroniche degli stessi strumenti oggetto dell’analisi. In tale ultimo caso si appalesa evidente la necessita` di ricorrere non solo ad un costante ammodernamento di strumenti di forensic analisys ma anche ad un aggiornamento delle stesse tecniche di analisi. Uno dei punti deboli sembra essere rappresentato dalla necessita` di una previa verifica delle capacita` tecniche dei consulenti esperti di computer forensics chiamati a deporre dinanzi alle Corti. In USA, al fine di stabilire degli standard qualitativi per la valutazione dei consulenti tecnici si ha riguardo al curriculum vitae per saggiarne l’esperienza professionale e quindi l’attendibilita` mentre la rule n. 702 (“Federal Rules of Evidence USA“) indica i presupposti di ammissione in giudizio delle tecniche utilizzate per l’analisi delle prove digitali. Secondo il “Daubert test” deve trattarsi: di una procedura sperimentata, con una accertata bassa percentualita` di errori, pubblicata e recensita, ed infine generalmente accettata.

Una caratteristica peculiare delle tracce digitali (digital evidence) e` quella della loro immaterialita`. I dati digitali sono, per evidenti esigenze tecniche, rappresentati come una sequenza di bit che notoriamente risulta essere facilmente modificabile se si hanno gli opportuni privilegi. Ad esempio, su un normale computer con Sistema Operativo della famiglia Microsoft Windows e` sufficiente la password dell’utente Administrator per poter alterare artatamente il contenuto di un qualsiasi file presente sui supporti di massa.

In linea generale, su qualunque computer che disponga di un Sistema Operativo multitask e multiutente (e che quindi faccia distinzione tra modalita` “user” e modalita` “kernel/superuser”) e` riservata ad uno specifico utente la possibilita` di eseguire operazioni particolari che consentono di accedere a qualsiasi risorsa hardware/software per lo svolgimento delle normali attivita` di gestione, talvolta scavalcando le normali “protezioni” predisposte per preservare la natura effimera del dato digitale.

Sui dispositivi digitali meno complessi di un computer (GPS, macchine fotografiche ed in parte anche telefoni cellulari) in genere non c’e` distinzione sulle modalita` di accesso ai dati ivi contenuti e quindi e` relativamente agevole poter accedere a tali dati ed eventualmente modificarli a proprio piacimento senza dover ricorrere a particolari artifici per scavalcare i vincoli predisposti dai Sistemi Operativi propriamente detti. Qualunque dato digitale presente sui computer/dispositivi appena citati e` quindi di conseguenza facilmente (ed anche volontariamente) alterabile. Se tali dati fossero considerati alla stregua di prove e`, evidente che potrebbero non essere del tutto affidabili in quanto facilmente alterabili.

Risulta chiaro che per poter modificare dei dati digitali bisogna disporre delle necessarie autorizzazioni e delle dovute competenze tecniche per utilizzare gli strumenti adeguati. L’utilizzo di tali strumenti, e la predisposizione della giusta sequenza di operazioni, e` normalmente demandata ad un umano che interagisce con i dispositivi elettronici, quali che essi siano. A seguito dell’utilizzo di tali strumenti e` possibile quindi alterare un dato digitale. Tale alterazione puo` anche avvenire per opera di un programma che esegue una sequenza di azioni. L’esigenza di automatizzare una serie di azioni/procedure e` presente in diversi campi di applicazione sui dispositivi elettronici, e spesso l’automazione viene utilizzata per far eseguire ad un sistema delle operazioni ripetitive e che non necessitano della presenza umana nel mentre tali azioni vengono effettuate.

A. Alibi digitali in recenti procedimenti giudiziari

In numerosissimi casi giudiziari le digital evidence sono servite ad identificare i responsabili di gravi reati. Tuttavia, non mancano casi in cui esse, costituendo un alibi, hanno scagionato l’indiziato dalle accuse.

Si pensi al caso di Rodney Bradford( [1], [2], [3]), un ragazzo di 19 anni che era stato arrestato per rapina a mano armata commessa il 17 ottobre 2009 a Brooklyn, citta` di New York, zona in cui egli viveva. Il suo avvocato difensore Robert Reuland ebbe a dichiarare che l’imputato, al momento della rapina, si trovava nella casa del padre nel quartiere di Harlem. La difesa sostenne che la pagina di Facebook dell’imputato era stata aggiornata alle 11:49 di mattina, esattamente un minuto prima della rapina, con un messaggio alla fidanzata “On the phone with this fat chick... where my IHOP”. E` noto che Facebook pubblica sempre la data e l’orario esatto di ogni contenuto inserito e dall’analisi forense e` emerso effettivamente che l’aggiornamento del messaggio era stato fatto attraverso una connessione da un appartamento al

71 West, 118th Street di Manhattan (New York), ovvero la casa del padre, che distava oltre 13 miglia dal luogo del reato. Dopo 12 giorni scontati nella prigione di Rikers Island, Rodney venne rilasciato dal giudice e la sua posizione archiviata. Si e` anche obiettato, nel caso di specie, che l’aggiornamento del messaggio poteva essere stato fatto da chiunque al fine di costituire l’alibi, magari un parente o un amico in possesso dei dati (username e password) necessari per autenticarsi e modificare un profilo di Facebook. Ma l’avvocato difensore ebbe fermamente ad escludere cio` in quanto il precostituirsi l’alibi avrebbe implicato un livello di genio criminale inusuale in un ragazzo cos`ı giovane. Altro caso giudiziario, noto come il caso Garlasco( [4], [5]), estremamente interessante sotto il profilo della valutazione dellalibi digitale, si e` concluso con l’assoluzione di Alberto Stasi, principale indiziato di omicidio della propria fidanzata Chiara Poggi. “Non ho ucciso Chiara. Io era a casa a scrivere la tesi al computer, mentre lei moriva”. Questa la frase ripetuta in piu` occasioni dallimputato il quale sin dall’inizio ha proclamato la propria innocenza adducendo un alibi informatico. Tale caso giudiziario e` caratterizzato da un serrato confronto tra risultati di analisi effettuati su ogni tipo di reperto: dal DNA su tracce ematiche alle digital evidence sui PC in uso alla vittima ed all’indiziato. A tali accertamenti si sono affiancate anche tecniche tradizionali di ricerca di mezzi di prova consistiti nella raccolta di informazioni e testimonianze rese da soggetti informati sui fatti. Quattro i tipi di accertamenti peritali — una perizia tecnico/informatica, una medico/legale, una chimico/sperimentale e la quarta definita come “semi-virtuale”

— ai quali si aggiungono le consulenze tecniche disposte dalle altre parti processuali. Lattenzione comunque si e` focalizzata sullaccertamento dell’alibi digitale fornito da Stasi il quale ha dichiarato, offrendo agli inquirenti il proprio computer portatile affinche´ venisse analizzato, di essere stato a casa sua, distante circa 2 km dal luogo del delitto, a scrivere sul computer la tesi di laurea proprio nell’orario in cui Chiara sarebbe stata uccisa nonche´ di aver effettuato alcune telefonate sull’utenza telefonica mobile della fidanzata. Peculiare appare la circostanza che il giudice, pur constatando la presenza di errori commessi dagli esperti nella fase di repertamento ed analisi delle digital evidence, giunge comunque ad emettere sentenza di assoluzione cos`ı motivando: “Partendo da questo dubbio di fondo e tenuto conto della grave anomalia rappresentata dalle alterazioni del contenuto informativo dovute agli accessi dei Carabinieri che ben potevano avere determinato la cancellazione delle normali evidenze presenti all’interno del sistema operativo, il collegio peritale (con la collaborazione dei consulenti tecnici delle parti) ricercava delle particolari informazioni che si trovano fuori del sistema operativo (i c.d. metadati). Questa ricerca dava esito positivo: questi metadati ed il loro contenuto attestano con certezza (e questo e` un’evidenza probatoria non contestata dalle parti) l’interazione diretta e sostanzialmente continuativa dell’utente con il computer dalle ore 10.17 fino alle ore 12.20 del giorno 13 agosto”.

Cio` significa che l’alibi digitale, sebbene minato da errori e sebbene si fosse reso necessario il ricorso all’analisi dei metadati per ricostruirne le parti compromesse, sembra aver fornito al giudice la chiave per “collocare” lindiziato al lavoro davanti al suo computer portatile in quel lasso di tempo critico correlato all’omicidio della sua fidanzata.

Questi casi giudiziari fanno riflettere circa le origini della produzione delle digital evidence in quanto non sempre e` possibile risalire all’identita` dellautore o scoprire come le stesse siano state prodotte automaticamente.

Rodney Bradford, un ragazzo di 19 anni era stato arrestato per una rapina con una pistola commessa nella zona dove viveva a Brooklyn, nella citta` di New York, il 17 ottobre 2009 [1], [2], [3]. Il suo avvocato difensore Robert Reuland dichiaro` che l’imputato si trovava nella casa del padre nel quartiere Harlem.

A sostegno della sua tesi sostenne che la pagina di Facebook dell’imputato era stata aggiornata con un messaggio alla fidanzata “On the phone with this fat chick... where my IHOP.” alle 11:49 di mattina, esattamente un minuto prima della rapina. E` noto che Facebook pubblica sempre la data e l’orario esatto di ogni contenuto inserito. L’aggiornamento era avvenuto dal computer del padre. La successiva verifica con gli esperti di Facebook confermo` che la modifica era stato fatta da una connessione da un appartamento al 71 West, 118th Street di Manhattan (New York), ovvero la casa del padre, che distava piu` di 13 miglia dal luogo del reato. Dopo 12 giorni nella prigione di Rikers Island, Rodney e` stato rilasciato dal giudice. Probabilmente questo e` il primo caso in cui un aggiornamento su Facebook e` stato usato come alibi. E` evidente che chiunque conoscesse le opportune username e password avrebbe potuto modificare un profilo di Facebook. Ad esempio tali modifiche potrebbero essere state fatte da un parente o da un amico proprio per creare un alibi. Secondo l’avvocato difensore Reuland, questa eventualita` sarebbe remota perche´ avrebbe implicato un livello di genio criminale inusuale in un ragazzo cos`ı giovane.

II. AL I B I DI G I TA L E

Innanzi tutto verra` mostrato cosa adduce l’imputato come alibi. In seguito verranno mostrate quali sono le evidenze digitali che vengono trovate dai consulenti tecnici su disposizione dell’Autorita` Giudiziaria. Verra` mostrato che tali tracce risultano compatibili con tutte le dichiarazioni dell’imputato e quindi confermano il suo alibi. Infine verra` mostrato come, in maniera automatica, e` possibile predisporre una serie di azioni tali da lasciare le stesse tracce digitali che risulterebbero del tutto indistinguibili dal risultato delle stesse azioni se fossero state fatte proprio da lui in prima persona nei tempi e nei luoghi riscontrati.

A. Alibi dell’Indagato

L’indagato conclama la propria estraneita` ai fatti affermando che nel mentre veniva perpetrato il crimine era a casa sua a lavorare al computer. In particolare, a sostegno del suo alibi afferma di aver effettuato una serie di operazioni, fornendo anche una indicazione temporale di massima (a volte precisa e a volte un po` meno).

In particolare, l’indagato afferma di:

1. aver lavorato al suo computer e di averlo acceso circa alle ore 9:35;
2. essersi connesso ad Internet mediante una linea ADSL da casa sua;
3. aver lavorato alla stesura della sua tesi di laurea e di conseguenza di aver creato/modificato, salvato ripetutamente, convertito in PDF, e stampato tale documento elettronico consistente in un file in formato Microsoft Word;
4. aver visualizzato foto e filmati sia dal suo computer e sia da Internet (da YouTube e da Picasa);
5. di aver inviato alcune e-mail tramite Gmail e di aver chattato/postato su Facebook;
6. di aver effettuato alcune telefonate da casa sua tramite il telefono fisso e tramite il suo cellulare verso alcune numerazioni (sia fisse che mobili) compresa l’utenza fissa e quella mobile della persona che ha subito il reato[[1]](#footnote-1);
7. di aver scattato alcune foto e girato piccoli spezzoni di filmati con la sua macchina fotografica;
8. di aver effettuato una copia di backup di alcuni dei suoi file (tra cui la tesi) sul servizio di backup online DropBox [18];
9. di aver infine spento (o messo in stand-by) il suo computer circa alle 12:30.

Le attivita` dell’imputato sono compatibili temporalmente e sono distribuite nell’arco della mattinata in modo tale da non lasciare intervalli temporali (senza tracce) che gli avrebbero potuto consentire di andare sul luogo del reato e tornare indietro.[[2]](#footnote-2)

B. Digital evidence ed Analisi Forense

A seguito delle dichiarazioni dell’indagato (ma anche perche´ le norme lo consentono) l’Autorita` Guidiziaria dispone consulenza tecnica[[3]](#footnote-3) per verificare se quanto da lui affermato corrisponda o meno a verita` ed incarica dei periti di accertare tutto cio` ritenuto utile alle indagini.

Il sequestro e` stato effettuato il giorno successivo all’evento criminoso e per tale motivo si riescono a recuperare tutte le tracce. In alternativa, se ne sarebbero trovate di meno. A valle dell’acquisizione forense dei dispositivi coinvolti (computer, telefono cellulare, macchina fotografica) ed anche delle informazioni ricevute dalle terze parti (ISP, gestori telefonici delle utenze fisse/mobili, gestori dei servizi Internet coinvolti quali YouTube, Picasa, Facebook, Gmail, DropBox) i consulenti dell’A.G. accertano quanto segue:

1. dall’analisi dei file di log del computer e` emerso che effettivamente tale dispositivo e` stato acceso alle ore 9:35 e che l’indagato ha lavorato al computer dalle 9:36 alle 12:20 (con una interruzione tra le ore 11:37 e le 11:49, verosimilmente per scattare le foto come indicato al punto G));
2. grazie all’acquisizione dei tabulati di connessione forniti dal ISP utilizzato dall’indagato per collegarsi alla rete Internet, e` emerso che effettivamente la sua utenza era connessa alla rete Internet e che su tale connessione e` transitata una quantita` di byte compatibile con una connessione di tale durata. Ulteriori prove dell’avvenuta connessione risultano da quanto mostrato ai punti D) ed E);
3. grazie all’acquisizione della copia forense del materiale informatico ritenuto interessante, e in par- ticolare, grazie all’esame del hard disk del computer dell’indagato, si e` potuto verificare che effettivamente il file contenente la sua tesi e` stato “lavorato” dalle 9:36 alle ore 12:20. In particolare, si e` potuto constatare che tale file in formato Microsoft Word e` stato piu` volte salvato, e` stato convertito in formato PDF ed infine anche stampato. Risulta una inattivita`
4. su tale file tra le ore 11:37 e le11:49;
5. a seguito dell’analisi del hard disk e` stato possibile stabilire che nell’orario fornito dall’indagato sono state visualizzate diverse foto e video presenti sull’hard disk. Inoltre, dall’analisi della cache del browser e a seguito dei tabulati di accesso dei fornitori di servizi Internet (YouTube e Picasa) si e` potuto verificare che effettivamente ci sono stati da tale computer diversi accessi a foto e video presenti sui due siti appena citati;
6. a seguito dell’analisi del software di gestione della posta elettronica ed anche dei tabulati di connes- sione forniti dal gestore del servizio (Gmail) e` stato possibile verificare che dal computer dell’indagato risultano spedite 3 e-mail (rispettivamente alle ore XX:XX, YY:YY, ZZ:ZZ). Inoltre, dall’analisi dei file relativi all’utilizzo del browser nonche´ dell’esame dei dati ricevuti da Facebook e` stato possibile verificare che l’IP attribuito all’utenza in uso all’indagato risultava essere collegato al portale di Facebook per tutto l’arco temporale interessato (dalle ore 9:37 a circa le ore 12:15) ed inoltre risultano due post in bacheca rispettivamente alle ore XX e YY;
7. a seguito dell’analisi dei tabulati telefonici del gestore dell’utenza fissa di casa dell’indagato, e` stato possibile verificare che tale utenza ha telefonato al Customer Care del suo gestore di telefonia mobile alle ore 09:56 (per una durata di 5 minuti) e sull’utenza fissa dell’abitazione dove si e` consumato il reato alle ore 10:47 (ma senza ricevere alcuna risposta). Inoltre a seguito dei tabulati del gestore di telefonia mobile dell’indagato e` stato possibile stabilire che dalla sua utenza mobile e` partita una telefonata verso l’utenza mobile della persona che ha subito il crimine alle ore 10:51 (anche questa volta senza ricevere alcuna risposta). I tecnici hanno anche verificato dove si trovasse l’indagato quando ha effettuato la chiamata dal suo telefono cellulare: per stabilire cio` il gestore mobile ha comunicato a quali BTS (e relative Cell-ID) fosse agganciata tale utenza per l’intera mattinata. Considerando che il segnale GSM non va oltre il limite tecnologico di 63 x 550m (circa 35Km) [23] e che la casa dell’indagato dista da quella della vittima circa 40 km, insieme alla analisi delle localizzazioni tramite Cell-ID, si e` potuto accertare che il telefono cellulare dell’indagato si trovava in prossimita` della sua abitazione; a seguito dell’analisi delle foto (e di un filmato) presenti sulla macchina fotografica dell’indagato, si e` potuto stabilire che tutto cio` e` stato effettivamente prodotto (dalle ore 11:37 alle ore 11:49) da tale dispositivo e che non sono state introdotte deliberatamente dal suo possessore in un secondo momento. Inoltre, una attenta analisi di tali foto ha permesso di verificare che gli orari erano perfettamente compatibili con quanto affermato dall’indagato ed anche con le pause introdotte nello svolgimento delle attivita` come descritto ai punti A) e C). Per stabilire se le foto (ed il filmato) siano state scattate da quella macchina fotografica si e` fatto ricorso a recentissime tecniche di Image Forensics che tengono conto di alcuni fattori altamente discriminanti quali, ad esempio il rumore del sensore ottico del dispositivo;
8. a seguito dell’analisi dei file di log relativi al programma DropBox e delle informazioni fornite dal gestore del servizio di backup online, e` stato possibile verificare che effettivamente dall’IP collegato all’utenza dell’indagato e` stato utilizzato il servizio di backup online4 pochi istanti prima di aver spento il computer e cioe` circa alle 12:12;
9. a seguito dell’analisi di log del computer dell’indagato e` stato possibile stabilire che tale dispositivo e` stato spento in un orario compatibile con quanto affermato dall’indagato (alle ore 12:19). Inoltre, a partire da tale orario, non risulta ulteriore traffico Internet sulla connessione ADSL di casa sua.

I periti trovano solo tracce digitali che confermano quanto affermato dall’indagato. Inoltre non esistono altre tracce digitali che sono in contraddizione con le affermazioni del indagato e non vi sono tracce di altre attivita` svolte in quella mattinata.

III. CR E A Z I O N E AU TO M AT I C A D E L L A DI G I TA L EV I D E N C E

In questa sezione viene mostrato come sia possibile costruire in maniera automatica e senza complici una serie di “evidenze digitali” che risultano essere del tutto indistinguibili da eventuali tracce che verrebbero lasciate normalmente se un utente eseguisse di persona tali operazioni. Per dare un senso di concretezza, viene proposto un caso di studio. Chiaramente, l’esempio proposto e` solo scopo di illustrare un insieme di possibili attivita`: se le attivita` fossero troppo numerose o troppo dense nell’arco temporale, sarebbe possibile per l’imputato selezionarne un sottoinsieme che sia adeguato al suo comportamento tipico. In questo caso di studio, vi e` un indiziato che viene indagato per aver commesso un reato. Tale reato e` stato perpetrato a circa 35 km di distanza dalla abitazione dell’indagato. Verra` mostrato come e` possibile che l’indagato si sia potuto creare un alibi in maniera deliberata. In linea, generale verra` spiegato come effettuare in maniera del tutto automatico quanto l’indagato adduce come alibi (operazioni elencate dal punto a) al punto i)), senza complici ed in modo tale che a seguito delle perizie elaborate dai 4 tramite accesso con username e password dell’indagato consulenti (come dai punti A) fino ad I)) risulti effettivamente che tali operazioni siano state effettuate dall’indagato.

Di seguito verranno indicate alcune delle possibili azioni che l’indagato ha potuto effettuare per far risultare che tutto quanto indicato dai punti a) fino ad i) sia stato fatto effettivamente da lui medesimo, e nei luoghi e nei tempi da lui indicati [28]. Tali spunti non vogliono essere una guida esaustiva su tutte le possibili modalita` in cui tali operazioni possano essere state effettuate, e neanche intendono essere dei consigli per chi volesse utilizzarle per crearsi un alibi, ma stanno solo ad indicare quanto sia semplice per la maggior parte delle persone, dotate di medie capacita` tecniche, poterle effettuare o magari farsele preparare da una terza persona. Siccome l’ordine temporale e la collocazione spaziale sono fondamentali in un’analisi forense, si potrebbe pensare che l’indagato potesse aver modificato semplicemente l’orologio del suo computer in modo tale da farlo risultare compatibile con quanto da lui affermato. Tale modifica dell’orologio del computer pero` non sarebbe stata efficace perche´ essendo il computer collegato ad Internet ed avendo l’indagato effettuato una serie di operazioni su diversi servizi Internet (connessione ADSL, Gmail, Facebook, Picasa, YouTube) tali servizi remoti avrebbero in ogni caso “memorizzato” gli orari reali rendendo vano il tentativo di “spostare le lancette” del computer. Inoltre, i tabulati telefonici (sia per il fisso che per il mobile) non potrebbero in ogni caso essere falsificati (o almeno non sarebbe facile per l’indagato farlo da solo senza complici). Pertanto, l’indagato e` dovuto ricorrere a strumenti piu` elaborati rispetto al semplice “spostare le lancette” dell’orologio del proprio computer (ad esempio operando nel BIOS del computer).

Vediamo punto per punto alcuni modi in cui l’indagato avrebbe potuto simulare le azioni descritte dal punto a) al punto i) pur non essendo lui fisicamente presente. Per l’esposizione si fara` riferimento ai principali tipi di computer al giorno d’oggi in commercio: Apple iMac con sistema operativo Mac OS X (10.6.2) e un PC DELL Optiplex 755 con sistema operativo Windows XP. Tali tipologie di hard- ware/software sono puramente indicative considerato che le stesse operazioni possono essere effettuate senza notevoli variazioni anche su altre varianti di hardware/sofware.

A. Accensione computer [VERIFICARE COME CANCELLARE EVENTUALI TRACCE]

Con il sistema operativo Mac OS X e` possibile accendere il computer automaticamente impostando semplicemente i parametri corretti nel menu` “Risparmio Energia” ➙ “Programma” delle “Preferenze di Sistema”. Nei comuni PC/portatili con sistema operativo Microsoft Windows e` possibile effettuare le stesse operazioni da BIOS o mediante la tecnica del Wake-On-Lan (tecnica che puo` essere usato anche dai sistemi Apple).

B. Schedulazione automatica operazioni Mediante l’utilizzo di appositi script e` possibile simulare tutta una serie di attivita` che sono indistinguibili dalla normale attivita` al computer di una persona fisica. In particolare, e` possibile visitare siti e creare traffico su Internet allo stesso modo come se ci si trovasse effettivamente al computer. Per la creazione di tali script e` possibile agire in diversi modi ma se ne utilizzera` solo uno per Sistema Operativo (Automator per Mac OS X e AutoIt per Windows). Tali programmi (Automator e AutoIt) sono stati scelti tra diversi altri programmi che possono essere utilizzati per raggiungere lo stesso scopo. Tra i principali programmi ci sono:

• AutoHotKey (per Windows) [12];

• AutoIt (per Windows) [13];

• Windows Host Script (per Windows) [14];

• DoThisNow (per Windows e Linux) [15];

• GNU Xnee (per Linux) [16];

• Automator (per Mac Os X) [17].

Automator e` un tool gia` presente nei sistemi Mac OS X a partire dalla versione 10.4 (Tiger). AutoIt e` un software freeware che gira sulla maggior parte delle versioni di Windows attualmente in commercio. Con entrambi i tool e` possibile sia creare uno script da dare in input al programma stesso e sia generare un file eseguibile stand-alone senza necessita` di dover installare il software stesso. In realta`, come gia` detto, in ambito Mac OS X, Automator e` gia` presente nel sistema e quindi la caratteristica di potersi svincolare dall’installazione del software mediante la generazione di un eseguibile stand-alone e` maggiormente importante per AutoIt perche´ in tal caso non risulterebbe installato alcun programma che potrebbe far suscitare sospetti. Nell’Appendice 1 viene illustrato come e` possibile riprodurre (con Automator e con AutoIt) una tipica sessione Internet in cui vengono visitati un certo numero di siti web e in cui vengono utilizzati una serie di programmi installati sul computer. In particolare, in seguito, verra` mostrato l’utilizzo di alcuni servizi/programmi specifici (cfr. i punti seguenti 3), 4) e 5).

C. Elaborazione di un documento digitale

In questa sezione ci si deve mettere tutta la parte dove si mostra come ha potuto far risultare di aver lavorato alla stesura della sua tesi di laurea e di conseguenza di aver creato/modificato, salvato ripetutamente, convertito in PDF, e stampato tale documento elettronico che consiste in un file in formato Microsoft Word (riferimento all’ultimo paper sui PDF accettato [21].

D. Foto e Video (locali e remoti)

In questa sezione ci si deve mettere tutta la parte dove si mostra come ha potuto far risultare di aver visualizzato foto e filmati sia dal suo computer e sia da Internet (YouTube e Picasa).

E. E-mail e Facebook

In questa sezione ci si deve mettere tutta la parte dove si mostra come ha potuto far risultare di aver inviato alcune e-mail (Gmail) e di aver chattato/postato su Facebook.

F. Telefonate

Per automatizzare delle telefonate ho bisogno di un modem e un cavo telefonico deve essere connesso dal modem al PC. Tale connessione e` puo` coesistere senza problemi con la connessione ADSL. Il modem rappresenta a tutti gli effettivi un apparato telefonico. E` possibile far risultare che una chiamata sia stata fatta da una utenza fissa (verso qualsiasi numerazione, sia essa fissa o mobile) semplicemente predisponendo una attivita` automatica (schedulata e controllata). In particolare, e` necessario disporre di un modem collegato ad un computer e creare una connessione ad Internet tramite tale modem, allo stesso di come si effettuano le connessioni analogiche verso gli ISP. Per attivare la connessione, il computer comporra` il numero di telefono impostato come server dial-up e quindi una telefonata partira` verso la numerazione presente come numero di destinazione. Dal punto di vista fisico, e` necessario collegare con un cavetto telefonico classico (RJ11) il modem alla spina telefonica di un’utenza fissa. Cos`ı facendo, la chiamata e` effettivamente fatta da tale utenza e viene effettuata nell’orario in cui si desidera farla.

Per far in modo che una chiamata sia realmente avvenuta, cioe` che non sia soltanto una serie di squilli ma effettivamente qualcuno abbia risposto al telefono, si puo` procedere in diversi modi. Ad esempio, si potrebbe predisporre adeguatamente il numero di telefono chiamato in modo tale che risponda in automatico, magari dopo qualche squillo (ad esempio, con i comandi modem standard Hayes, con i comandi ATS0=6 e poi ATA si imposta il dispositivo in modo da farlo rispondere automaticamente dopo 6 squilli). In alternativa, si potrebbe telefonare ad una numerazione che risponda in automatico e che fornisca informazioni utili a chi chiama, come ad esempio alcuni servizi di Customer Care di gestori telefonici o di pubblica utilita`. A seguito della risposta automatica da parte del Customer Care, si potrebbe “istruire” il computer a digitare alcuni tasti per far scegliere determinati menu` in modo tale da simulare una tipica sessione telefonica di questo genere.

Per fare le stesse operazioni da un telefono cellulare, bisogna semplicemente collegare un telefono cellulare al computer (tramite il cavetto apposito fornito dal produttore del telefono, in genere USB, oppure tramite IrDA o Bluetooth) in modo tale che il telefono cellulare funzioni da modem. Infatti, a seguito del collegamento di un telefono cellulare ad un computer (sia esso fisso o portatile) viene creata un’istanza di un soft-modem. Il termine “soft” viene utilizzato in quanto non si tratta propriamente di un modem fisico ma solo di un modem software. Cos`ı facendo, la telefonata risultera` partita da quel telefono cellulare e tale telefono risultera` localizzato proprio dove si desidera farlo risultare in quanto effettivamente

si trova in tale posto (in caso di analisi della localizzazione del cellulare tramite rete mobile). Risulta evidente che se il modem e` stato connesso solo per fare queste operazioni e` assolutamente il caso di staccarlo e riporlo a suo posto.

G. Foto scattate dalla macchina fotografica

La tecnologia attuale consente (mediante recenti tecniche di Image Forensics) di stabilire con ragionev- ole certezza se una foto e` stata o meno scattata da una determinata foto/videocamera. Quindi non avrebbe molto senso provare a falsificare alcune caratteristiche di una foto digitale (quali ad esempio i campi EXIF [6]). Infatti in tal caso, sarebbe abbastanza facile risalire al dispositivo che ha generato la foto in questione. Purtroppo pero` , anche per questa operazione vale la regola che tutto cio` che e` digitale e` alterabile e di conseguenza anche i parametri che determinano l’impronta di una foto sono falsificabili. In particolare, e` possibile inserire in una foto l’impronta digitale di un’altra macchina fotografica (senza che questo sia percepibile) in modo tale da far identificare erroneamente il dispositivo che ha generato tale foto. Per poter rendere compatibili gli orari delle foto presenti sul dispositivo con gli orari in cui il reato si e` consumato, e` necessario che tali foto vengano scattate in un istante effettivamente diverso da quello del reato (o prima o dopo). Per realizzare tutto cio` , quindi, e` necessario cambiare la data e l’ora del dispositivo in maniera adeguata, scattare le foto, e poi rimettere data ed ora ai valori corretti.

In tal modo le foto avranno dei timestamp (sia sul filesystem del dispositivo e sia nella struttura EXIF) che sono assolutamente compatibili con quanto si desidera dimostrare. Sarebbe importante scattare tali foto nella stessa fascia oraria (magari un giorno prima) dell’orario che si intende far credere in modo da avere un’illuminazione realistica per quell’orario. Ad esempio bisognerebbe evitare di scattare una foto la mattina presto e mettere l’ora del dispositivo alle 12:00 perche´ in tal caso si verrebbe scoperti del falso). Inoltre, per avvalorare ulteriormente l’alibi, sarebbe auspicabile che le foto scattate includessero sia elementi caratteristici della casa dell’indagato e sia elementi riconducibili alla sua persona fisica, come il volto.

H. Copia backup su DropBox

Il software DropBox (completamente gratuito) permette di effettuare dei backup online in maniera del tutto trasparente e semplice sui principali sistemi operativi disponibili. In particolare, con Mac OS X, dopo aver installato l’apposito software ed aver linkato il proprio computer ad un determinato account, e` possibile effettuare il backup dei propri file semplicemente copiando in una cartella specifica i file che si intende preservare. In tale modo si ottiene una copia di backup dei file voluti senza dover ricorrere a software complicati da utilizzare. Per poter automatizzare tale attivita` in modo da poterla fare quando si vuole (anche senza essere fisicamente di fronte al computer) basta programmare un’azione che copi i file voluti all’interno della cartella designata come quella che DropBox utilizza. Da quel momento in poi il software si colleghera` al server del servizio DropBox (mediante una connessione TLS/SSL) ed effettuera` la copia di backup. Nell’Appendice 1 viene mostrato come e` possibile fare in modo che in automatico vengano copiati dei file in una determinata cartella (con Automator e con AutoIt) in modo da ottenere il risultato voluto;

I. Spegnimento (o stand-by) computer

Con il sistema operativo Mac OS X e` possibile spegnere (o mettere in stand-by) il computer automati- camente impostando semplicemente i parametri corretti nel menu` “Risparmio Energia” ➙ “Programma” delle “Preferenze di Sistema”. Nei comuni PC/portatili con sistema operativo Microsoft Windows e` possibile effettuare le stesse operazioni o da BIOS o mediante “Pannello di Controllo” ➙ “Prestazioni e manutenzione” ➙ “Operazioni pianificate” facendo eseguire il comando %SystemRoot%\System32\shutdown.exe -s -t 00 per fare spegnere il computer o

%SystemRoot%\System32\shutdown.exe -r -t 00

per farlo riavviare.

J. Cancellazione delle tracce

Il concetto generale e` di fare in modo che si lascino il minor numero possibile di tracce, sapendo quali sono e dove si trovano. Non vi e` necessita` di cancellare o alterare i log (di sistema e delle applicazioni). Per poter rendere maggiormente credibile l’alibi, e` fondamentale cancellare tutte le tracce lasciate dalle varie azioni “programmate” volontariamente. Tali tracce sono presenti in particolare nella parte relativa al software che automatizza tutti i processi ed anche in alcune componenti dei dispositivi coinvolti. Ad esempio, nel BIOS del computer che viene utilizzato potrebbero esserci tracce dell’accensione schedulata (come indicato al punto 1) di questa sezione). Si rende necessario quindi eliminare tale schedulazione in modo che un’eventuale analisi del BIOS non riveli l’intenzionalita` dell’operazione. Risulta importante, al fine di cosa cancellare, la tipologia di utilizzo del software per automatizzare i compiti. Infatti, nel caso in cui il software permetta di creare un file eseguibile stand-alone ed indipendente rispetto al programma stesso, sara` sufficiente cancellare un singolo file e cioe` quello che contiene la versione “compilata” dello script utilizzato per l’automazione. Tutto cio` perche` la semplice cancellazione di dati sul disco con le funzioni incluse nel proprio sistema operativo potrebbe non essere sufficiente. Infatti il dato rimane sul disco ma i settori che erano occupati sono solo resi disponibili per una nuova scrittura. Diversamente, per la cancellazione sicura (detta wiping) i dati vengono riscritti un certo numero di volte facendo uso di pattern casuali oppure predeterminati. Ci sono standard per il wiping come quello statunitense DoD 5220.22-M [7] con 7 riscritture oppure il metodo di Gutmann con 35 riscritture [8], [9]. La difficolta` non e` quella di come cancellare i dati, bens`ı di individuare quali dati cancellare. Bisogna quindi determinare esattamente quali tracce cancellare, come ad esempio quelle eventualmente lasciate dai tool usati nella preparazione degli automatismi. Eventuali tracce che potrebbero destare sospetti dovranno essere eliminati selettivamente (cioe` solo quelli relativi all’attivita` da occultare), in modo da non destare sospetti in una successiva analisi forense. Se si facesse uso di un tool di wiping installato sul PC, sarebbe non facile rimuoverlo perche´ non potrebbe essere cancellato da se stesso. Se il tool di wiping non fosse cancellato, potrebbe destare sospetti l’esistenza di una simile applicazione. Sarebbe meglio che il tool fosse installato da un drive esterno rimovibile. Ma il suo uso lascerebbe comunque tracce. Per cancellare e’ possibile procedere in modo differente a seconda che ci si trovi su Mac OS X oppure Windows XP. In ambito Mac OS X, ad esempio, e` possibile utilizzare diversi metodi. Uno potrebbe essere quello di aggiungere come ultima istruzione dello script per Automator (che in questo caso supponiamo si chiami script\_file) un comando che esegua le seguenti istruzioni sulla SHELL:

$ eval $(/usr/bin/stat -s script\_file)

$ /bin/dd if=/dev/random of=./script\_file bs=1, count=$st\_size

$ /bin/dd if=/dev/zero of=./script\_file bs=1, count=$st\_size

$ /bin/dd if=/dev/random of=./script\_file bs=1, count=$st\_size

Questo codice sovrascrive per 3 volte (con valori casuali, con zeri, e con valori casuali) il file script\_file per l’intera sua grandezza (e cioe` $st\_size). Tale operazione puo` anche essere iterata piu` volte in modo da raggiungere elevatissimi gradi di sanitizzazione paragonabili a quelli presenti in letteratura quale il DoD 5220.22-MM, il metodo di Peter Gutmann o i recenti metodi proposti dal NIST con lo standard SP800-88 [10].

K. Ulteriori accortenze per avvalorare l’alibi

Un recente articolo [11] ha mostrato come sia possibile riconoscere la persona che ha utilizzato la tastiera di un computer analizzando i batteri lasciati dai polpastrelli delle dita sui singoli tasti e sul mouse. L’impronta lasciata dai batteri sui tasti e sul mouse persiste per oltre due settimane. Questo e` potenzialmente un nuovo strumento di indagine forense. Chiaramente gli investigatori dovranno usare dei guanti prima di analizzare i computer. Questa analisi puo` essere utilizzata per avvalorare l’alibi. L’indagato si e` assicurato di essere l’unico ad utilizzare il computer e l’analisi forense richiesta dall’avvocato difensore, compiuta entro 2 settimane, confermera` sono quelle dell’indagato. che sulla tastiera e sul mouse le tracce batteriche Le persone hanno le loro abitudini e quindi seguono pattern di predicibilita`. Potrebbe essere consue- tudine per l’indagato connettersi ad Internet durante la mattina, usare l’e-mail, il browser, e lavorare alla tesi. Il comportamento dell’indagato che si evince dall’alibi digitale, ovvero le tracce lasciate, devono essere non difformi dal solito. Cioe` non devono essere rilevate da una ipotetica analisi di Anomaly Detection [19]. Il tempo di connessione, la quantita` di byte transitata, la numerosita` di accessi ai social network, e le altre azioni devono essere simili a quelle dei giorni precedenti ed alle abitudini dell’imputato. Lo stesso comportamento che si evince dalla digital evidence dell’alibi potrebbe essere ripetuto in altri giorni con una qualche randomizzazione.

Una ulteriore accortezza che sarebbe utile da osservare al fine di avvalorare l’alibi rappresenta la necessita` di fare una fase di testing di tutti gli automatismi che sono stati predisposti al fine di verificarne il funzionamento. Inoltre, tale testing, andrebbe a dare regolarita` al pattern comportamentale e quindi sarebbe utile al fine di tutelarsi da eventuali analisi di Anomaly Detection.

L. Ulteriori considerazioni necessarie per la riuscita del tutto

IV. DI G I TA L EV I D E N C E C O M E AL I B I

I due casi giudiziari, Redford e Garlasco, citati fanno riflettere circa la reale attendibilita` di un alibi costituito da digital evidence in quanto non sempre e` possibile sapere da chi o come fossero state

prodotte. Il lavoro, lungi dal volere esprimere giudizi tecnici sulle conclusioni alle quali sono pervenuti i giudici, tende a dimostrare come tale forma di alibi possa ingenerare dubbi circa il suo reale valore probatorio. Infatti, oltre al rischio concreto che l’attivita` registrata sul PC sia frutto della complicita` di un altro soggetto che provvede a svolgere tutta una serie di attivita` in vece e per conto dell’indiziato, si e` ampiamente dimostrato come possa presentarsi il rischio, non infondato, che le attivit possano essere svolte dalla stessa macchina (PC) in assenza totale di un uomo alla tastiera.

Laspetto peculiare del caso giudiziario in cui l’indiziato non e` ricorso all’ausilio di complici, ipotizzato ai fini della presentazione del lavoro, e` rappresentato dall’emergenza della “indistinguibilit” delle digital evidence prodotte per la creazione dell’alibi. In tal caso, infatti, non si riesce ad individuare con certezza se le attivit svolte dal PC siano attribuibili all’intervento umano oppure alla mera esecuzione di script impartiti al PC. Correttamente puo` parlarsi, appunto, di “indistinguibilit” delle tracce lasciate volutamente sul computer a guisa di alibi per la incontrovertibile ragione che nessun tecnico esperto sarebbe capace di attribuire all’uomo o agli automatismi generati, le attivita` svolte sul PC.

Seppure si volesse svolgere un’analisi atta a dimostrare se il PC sia stato realmente usato dall’indiziato, le tracce di materiale biologico lasciate inevitabilmente sulla tastiera, confermerebbero la circostanza del suo reale utilizzo. Addirittura, come nel caso Garlasco, e` possibile imbattersi in situazioni complesse in cui si intersecano i risultati di diverse tipologie di analisi. Ebbene, in casi come questo, in cui tra la vittima e l’indiziato vi sono stati pregressi rapporti di frequentazione tali da giustificare sulla scena del crimine la presenza di tracce biologiche appartenenti allindiziato, troverebbe piena applicazione anche il noto principio di Locard. Tuttavia, mentre tali elementi di prova “giustificherebbero” la presenza dellindiziato sulla scena criminis, al contrario quelle rinvenute sulla tastiera del PC (sudore, batteri) avvalorerebbero al contrario la tesi della reale presenza dell’uomo intento ad usare il PC in luogo diverso e negli stessi orari del crimine.

Il paradosso e` che in tale situazione il giudice si troverebbe a decidere sulla valutazione di prove che portano alla presenza dell’indiziato vuoi sulla scena del crimine vuoi in altro luogo in cui era intento a lavorare al PC. Inopinatamente, egli sara` portato a dare credito ad un report del consulente tecnico il quale, in presenza di tale tipologia di digital evidence non potra` che confermarne l’autenticita`, l’integrita`, veridicita` e quindi l’attendibilit delle stesse a dispetto di quelle relative alle tracce biologiche lasciate sul locus commissi delicti in quanto queste ultime troverebbero giustificazione con pregressi contatti avuti con la vittima. Un delitto perfetto, si potrebbe definirlo. Ma ancora una volta sovviene la necessita` di integrare la valutazione delle digital evidence, di per se stesse evanescenti e fragili, con indagini eseguite con tecniche per cos`ı dire tradizionali, fatte di pedinamenti, testimonianze, intercettazioni ambientali.

V. CO N C L U S I O N I

Al giudice, peritus peritorum, spetta l’arduo compito di emettere una sentenza giusta e che raggiunga un grado di certezza oltre ogni ragionevole dubbio. Le argomentazioni svolte appaiono idonee quantomeno a spingere i giudici a tenere in giusta considerazione, sotto il profilo della reale portata probatoria, le digital evidence. Si appalesa auspicabile, nonche´ necessario, il ricorso all’acquisizione ed alla valutazione anche e soprattutto degli altri elementi di prova tradizionali. Questi ultimi, solo confrontati con le digital evidence, potranno fornire al giudice un quadro piu` completo ed esaustivo, vicino alla verita` dei fatti. S`ı alla valutazione della prova digitale, ma cum grano salis !

RI N G R A Z I A M E N T I

Qui vanno gli eventuali ringraziamenti . . .

AP P E N D I C E 1: CO D I C E SO R G E N T E

Qui va eventuale codice sorgente . . .

RE F E R E N C E S

[1] Msnbc News, Facebook message frees NYC robbery suspect, November 12, 2009. http://www.msnbc.msn.com/id/33883605/ns/technology and science-tech and gadgets/

[2] The New York Times, I’m Innocent. Just Check My Status on Facebook, November 12, 2009.

http://www.nytimes.com/2009/11/12/nyregion/12facebook.html? r=1

[3] CNN, Facebook status update provides alibi, November 12, 2009.

http://www.cnn.com/2009/CRIME/11/12/facebook.alibi/index.html

[4] Stefano Vitelli, GUP presso il Tribunale di Vigevano, Sentenza del processo Stasi,

http://static.repubblica.it/laprovinciapavese/pdf/SENTENZA STASI.pdf, 17 Dicembre 2009

[5] Fabio Bravo, La computer forensics nelle motivazioni della sentenza sull’omicidio di Garlasco http://internetsociety.wordpress.com/2010/03/16/la-computer-forensics-nelle-motivazioni-della-sentenza-sullomicidio-di- garlasco/, 16 Marzo 2010

[6] Japan Electronic Industries Development Association (JEIDA), Exchangeable Image File Format, http://en.wikipedia.org/wiki/Exchangeable image file format

[7] U.S. Department of Defense, DoD Directive 5220.22, National Industrial Security Program (NISP), http://www.dtic.mil/whs/directives/corres/html/522022m.htm, 28 February, 2010

[8] Peter Gutmann, Secure Deletion of Data from Magnetic and Solid-State Memory, Sixth USENIX Security Symposium Proceedings, San Jose, California, http://www.cs.auckland.ac.nz/ pgut001/pubs/secure del.html , July 22-25, 1996.

[9] Peter Gutmann, Data Remanence in Semiconductor Devices, 2001 Usenix Security Symposium, Washington DC, http://www.cypherpunks.to/ peter/usenix01.pdf , August 13-17, 2001.

[10] US NIST, Guidelines for Media Sanitization, NIST Special Publication 800-88, September 2006. http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88 rev1.pdf ,

[11] Noah Fierer, Christian L. Lauber, Nick Zhou, Daniel McDonald, Elizabeth K. Costello, and Rob Knight, Foren- sic identification using skin bacterial communities, Proceedings of the National Academy of Sciences, Abstract, http://www.pnas.org/content/early/2010/03/01/1000162107.abstract , March, 2010.

[12] AutoHotKey website, AutoHotKey, http://www.autohotkey.com/ , March 2010.

[13] Jonathan Bennett, AutoIt v3.3.6.0, http://www.autoitscript.com/autoit3/ , March 7, 2010.

[14] Microsoft Corporation MSDN, Windows Script Host, http://msdn.microsoft.com/en-us/library/9bbdkx3k(VS.85).aspx , 2010.

[15] Radical Breeze, DoThisNow, http://radicalbreeze.com/?page id=50 , 2010. [16] Henrik Sandklef, GNU Xnee, http://www.sandklef.com/xnee/ , 2010.

[17] Apple Inc., Apple Automator, http://www.macosxautomation.com/automator/ , 2010. [18] DropBox Developer Team, DropBox, http://www.dropbox.com/ , 2010.

[19] F. Maggi, S. Zanero, and V. Iozzo, Seeing the Invisible - Forensic Uses of Anomaly Detection and Machine Learning, ACM Operating Systems Review, vol. 42, no. 3, pp. 52-59, April 2008.

[20] A. Castiglione, A. De Santis and C. Soriente, Taking advantage of a disadvantage: digital forensics and steganography using document metadata, Journal of Systems and Software, Elsevier 80 (5), pp. 750-764, May 2007.

[21] A. Castiglione, A. De Santis and C. Soriente, Security and Privacy Issues in the Portable Document Format, Journal of Systems and Software, Elsevier, Accepted Paper, April 2010.

[22] R. A. Joyce, J. Powers, F. Adelstein, MEGA: A tool for Mac OS X operating system and application forensics, Journal of Digital Investigation, Elsevier, 5, pp. 83-90, 2008

[23] 3GPP, Timing Advance, http://en.wikipedia.org/wiki/Timing advance

[24] M. Geiger, Evaluating Commercial Counter-Forensic Tools, http://www.dfrws.org/2005/proceedings/geiger couterforensics.pdf

[25] T. Bosschert, Battling Anti-Forensics: Beating the U3 Stick, Journal of Digital Forensic Practice, 1556-7346, Volume 1, Issue 4, pp. 265-273, 2006

[26] A. Smith, Describing and Categorizing Disk-Avoiding Anti-Forensics Tools, Journal of Digital Forensic Practice, 1556-7346, Volume 1, Issue 4, pp. 309-313, 2006

[27] G. Fellows, WinRAR Temporary Folder Artefacts, Journal of Digital Investigation, Elsevier, article in press, March 2010 [28] D.-Y. Kao, S.-J. Wang and F. Fu-Yuan Huang, SoTE: Strategy of Triple-E on solving Trojan defense in Cyber-crime cases,

Journal of Computer Law and Security Review, Elsevier, Volume 26, Issue 1, pp. 52-60, January 2010

May 31, 2010 DRAFT

1. Si ipotizza che la tipologia di reato commesso e` tale da richiedere la prossimita` fisica tra cui lo commette e chi lo subisce. [↑](#footnote-ref-1)
2. E` evidente che se veramente l’imputato fosse stato interessato a lavorare alla tesi non avrebbe perso cos`ı tanto tempo a fare tutte le altre cose... [↑](#footnote-ref-2)
3. E` importante ricordare che il sequestro dei dispositivi da analizzare deve essere fatto in tempi brevi al fine di preservare le tracce. Tale vincolo temporale e` ugualmente importante anche per le analisi presso le terze parti. [↑](#footnote-ref-3)