RELAZIONE PERIZIA COMPUTER DI RAFFAELE SOLLECITO

Expert Report on Raffaele Sollecito’s computer

Prof.Alfredo MILANI

RELAZIONE PERIZIA COMPUTER DI RAFFAELE SOLLECITO

OBIETTIVO

Obiettivo della presente relazione è verificare e valutare la natura delle attività svolte sul computer laptop McBook Pro di Raffaele Sollecito, nel periodo 01 Nov 2007 18:00 – 02 Nov 2007 8:00 tramite a) esame diretto ripetibile di copia conforme dell'hard disk del suddetto computer ed b) alla luce della documentazione prodotta dalla Polizia Postale e presentata in dibattimento.

Il suddetto laptop McBook Pro risultava acceso nella abitazione di Raffaele Sollecito, connesso alla rete internet tramite un router wireless, e collegato ad un altro laptop marca Asus, che svolgeva funzioni di scaricamento file dalla rete. Non e' stato possibile esaminare l'hard disk del secondo laptop (hard disk Hitachi) che e' risultato inservibile.

1 Premessa metodologica: datazione e marche temporali digitali.

E'molto importante chiarire che i computer per motivi connessi al loro normale funzionamento registrano sugli hard disk, e su altri supporti di memoria volatili (RAM) e non (memorie flash, EPROM), grandi quantità di *marche temporali* di vario tipo, solitamente esse hanno la forma di una coppia *(data, ora)*[1] che viene associata ad un insieme di dati e/o ad un evento.

Alcune di queste *date* sono gestite direttamente dalla parte del sistema operativo detta *File system* e memorizzate in apposite strutture dati (come ad esempio le *date* di modifica dei file), altre *date* sono invece gestite da applicazioni di corredo al sistema operativo (come ad esempio le date di attivazione/disattivazione del salvaschermo), oppure sono gestite indipendentemente dalle varie applicazioni presenti nel computer (ad esempio la data di ascolto di una canzone, potrà essere memorizzata in modo diverso a seconda del programma di ascolto o *player* con cui tale canzone viene ascoltata).

Poiché molte e diverse applicazioni aggiornano indipendentemente le *date* , il loro aggiornamento non e' sempre coerente specie se l'evento da registrare viene

[1] Nel seguito per brevita' chiameremo *data* una informazione costituita dalla *data (giorno, mese, anno)* e dall'*ora (ore,minuti,fuso orario di riferimento)*

effettuato da un programma diverso seppur usato in modo regolare (ad esempio, ripristinando un file compresso, o *zippato*, dopo il ripristino esso puo' addirittura presentare una data precedente a quella di acquisto del computer!).

1.1 Supporti di memorizzazione delle date e formati.

È importante anche chiarire *dove* vengono memorizzate le date in questione ed in quale *formato*. Nel caso di *date scritte dal sistema operativo* esse vengono memorizzate in speciali strutture dati del disco, dette *inode* nei sistemi derivati da Unix come MacOS, il cui *formato* varia a seconda della versione del sistema in esame (ad esempio un sistema MacOS puo' registrare le stesse informazioni in modo diverso a seconda della versione).

Nel caso di *date scritte dalle applicazioni* esse vengono solitamente memorizzate all'interno di *normali file* che l'applicazione tratta in modo speciale, ad esempio per registrarvi le attività svolte (un media player memorizza solitamente quante volte un brano e' stato ascoltato sino alla fine, oppure l'ultima data in cui e'stato saltato con la funzione *skip*, oppure l'accensione/spegnimento della applicazione).

1.2 Modalità di rilevazione e memorizzazione di attivitá

Si noti che,in generale, lo svolgimento di una attivita' puo' essere rilevato attraverso:

- la ***registrazione esplicita della sequenza di date/marche temporali***, cioé di sequenze di date di operazioni o di *eventi* connessi alla attivitá, tali sequenze sono registrate in appositi file detti ***file di log*** (es. log di tastiera, plist, XML, log di rete etc.).
- ***modifica/sovrascrittura di una singola data/marca temporale***, come ad esempio la ***data di un file*** coinvolto nella attivita' stessa
- la manifestazione di ***eventi successivi***[2] che testimoniano una precedente attivita' in corso (es. il crash di un programma testimonia che esso era precedentemente in esecuzione)
- oltre ad una delle ipotesi precedenti, per rilevare correttamente una attivitá si deve anche provare **l'assenza di successive alterazioni** delle marche temporali stesse, ed il corretto funzionamento del sistema di registrazione delle date.

[2] *Atttivita' che si manifestano con eventi successivi*. Si noti che una attivita' anche non registrata nel sistema in un certo periodo di tempo puo' produrre i suoi effetti successivamente manifestandosi con un evento che poi viene registrato in un log o produce una modifica di date. Ad esempio il crash di una applicazione testimonia che tale applicazione e' rimasta in esecuzione sino al momento del crash (vedi paragrafi successivi sul crash di VLC).

È molto importante distinguere tra le due principali **modalità di memorizzazione delle date** di eventi utilizzate nei sistemi informatici:

- ***scrittura di sequenze di date***
- ***sovrascrittura di data***

Nel **primo caso** viene registrato un elenco di date/eventi riguardanti una certa risorsa. Un esempio di questo tipo é la *sequenza di attivazione/disattivazione della tastiera* memorizzata dai sistemi MacOs, cioè la sequenza di date in cui la tastiera è stata attivata/disattivata. Un altro esempio sono i file di log relativi alle comunicazioni con il web.

Nel **secondo caso** invece vi e' a disposizione uno spazio limitato ad una sola marca temporale e viene quindi registrata solo l'ultima occorrenza dell'evento, un esempio di questo tipo è la *data di ultima modifica di un file*. Se un file viene modificato più volte soltanto l'ultima delle modifiche effettuate resterà annotata nella relativa *data*.

Vi sono anche **situazioni intermedie** in cui vi e' a disposizione per la memorizzazione soltanto una sequenza limitata (ad esempio alcuni elaboratori di testi, ed alcuni player come VLC, mantengono in un menú l'elenco degli *ultimi cinque*[3] *documenti aperti di recente*)

Le due tipologie di memorizzazione degli eventi, ***scrittura in sequenza*** o ***sovrascrittura*** hanno conseguenze cruciali quanto si cerchi di provare la presenza o la assenza di attività in un certo periodo di tempo.

1.2.1 Sequenza di date, o file di log o "tabulati"

Nel caso della tipologia di memorizzazione come ***sequenza di date***, o ***file di log*** a meno di alterazioni dolose dei supporti, *la presenza di una marca temporale è fortemente probatoria della presenza cosi' come della assenza di attività connessa alla marca temporale stessa*. Ci si trova cioè in una situazione analoga a quella dei cosidetti ***tabulati*** telefonici dove vengono registrati ora e durata delle conversazioni a cura dei gestori di telefonia. Se in un certo periodo *non risulta* nessuna telefonata , è possibile concludere con ragionevole certezza che *non* sia avvenuta alcuna, a meno di modifica dolosa dei supporti o di malfunzionamento degli apparati.

[3] Solitamente tale numero é un parametro che puó essere personalizzato.

1.2.2 Sovrascrittura di data

Nel caso invece di ***sovrascrittura di data***, come si ha per le date di modifica o di apertura dei file, si ha che da un lato *la **presenza** della marca temporale in un periodo e' ragionevolmente probatoria dell'accadimento dell'evento* ad essa associato, ma si ha anche che *la **assenza** di marche temporali riferibili ad un certo periodo in esame **non e' assolutamente conclusiva** della assenza di attività, **anzi, quasi paradossalmente, tali marche risulteranno maggiormente assenti tanto maggiori sono le attività effettuate sulla risorsa in esame***.

Ad esempio, se un utente edita uno stesso documento con un sistema di videoscrittura, per un periodo prolungato nell'arco di un mese, poniamo una ipotetica Tesi di Laurea a cui tutti i giorni, il file risulterà avere una data di *ultima modifica* corrispondente all'ultimo giorno del mese di lavoro. Le date di *ultima modifica* annotate dal sistema al termine di ogni sessione giornaliera verranno sovrascritte, perdendone irrimediabilmente ogni traccia. Appare quindi evidente l'impossibilita' di basare una prova della "assenza di attività" sul documento stesso, sul fatto che *non* vi siano *date* di ultima modifica nel periodo considerato. In altre parole una qualsiasi attività successiva può cancellare ogni traccia di interazione su un certo file. Dal punto di vista pratico, la sovrascrittura di date può avvenire sia per ***azioni esplicite dell'utente***, ad esempio la ripetuta esecuzione di un brano musicale in una *playing list*, lascera' come traccia di ultimo accesso e ultima apertura, quelle dell'ultima volta che il brano e' stato ascoltato (o un film visto) cancellando le tracce di ascolti/visioni precedente.

La sovrascrittura di date puó anche avvenire in ***modo implicito/automatico***, ad esempio lo scaricamento di un file da parte di utenti remoti tramite *peer-to-peer* puo' modificare i dati di accesso dei file dell'utente locale, in altre parole gli utenti remoti accedono al computer locale leggendo il file e quindi modificandone la data di ultimo accesso.

1.3 Alterazione delle marche temporali per sovrascrittura di date successive

Ogni attivita' su un file che viene registrata con la tecnica di sovrascrittura puo' quindi essere mascherata/cancellata da aperture o esecuzioni successive del file, le nuove marche temporali vanno cioe' a **sovrascrivere quelle precedenti che non possono essere piú rilevate (neppure da prodotti come ENCASE).**

Il fatto quindi di non rilevare attivita' come apertura di un file in un certo periodo temporale non significa necessariamente che non vi sia stata tale attivita' in quanto essa puó essere stata sovrascritta da molteplici cause successive.

Risulta inoltre evidente quindi che *maggiore tempo trascorre prima dell'acquisizione di un supporto che continui ad essere funzionante ed utilizzato, e maggiore e' la probabilità che marche temporali singole, di eventi periodici, ripetuti o automatici vadano progressivamente a sovrascrivere e quindi a cancellare le marche di periodi di tempo precedenti*.

Registrazione per Sequenza di Date **(file di log o "tabulato")**	***Registrazione per Sovrascrittura di Date*** **(date aperture, date modifica etc.)**
Data Evento	**Data Evento**
01/10/2010 h:15:00 vedi film1 01/10/2010 h:15:20 vedi film2 01/10/2010 h:15:50 scrivi testo1 01/10/2010 h:18:05 play song1 01/10/2010 h:18:10 play song2 01/10/2010 h:18:15 play song3 01/10/2010 h:18:20 play song4 01/10/2010 h:18:25 play song1 01/10/2010 h:18:30 play song2 01/10/2010 h:18:35 play song3 01/10/2010 h:18:40 play song4 02/10/2010 h:14:00 play song1 02/10/2010 h:14:10 play song2 02/10/2010 h:14:15 play song2 02/10/2010 h:16:00 vedi film2 02/10/2010 h:17:00 scrivi testo1 03/10/2010 h:15:10 scrivi testo1 03/10/2010 h:17:00 play song3 04/10/2010 h.16:30 scrivi testo1 06/10/2010 h:16:00 scrivi testo1 06/10/2010 h:17:00 play song3 ***Tutti*** *gli eventi risultano annotati*	01/10/2010 h:15:00 vedi film1 01/10/2010 h:15:20 vedi film2 01/10/2010 h:15:50 scrivi testo1 01/10/2010 h:18:05 play song1 01/10/2010 h:18:10 play song2 01/10/2010 h:18:15 play song3 01/10/2010 h:18:20 play song4 01/10/2010 h:18:25 play song1 01/10/2010 h:18:30 play song2 01/10/2010 h:18:35 play song3 01/10/2010 h:18:40 play song4 02/10/2010 h:14:00 play song1 02/10/2010 h:14:10 play song2 02/10/2010 h:14:15 play song4 02/10/2010 h:16:00 vedi film2 02/10/2010 h:17:00 scrivi testo1 03/10/2010 h:15:10 scrivi testo1 03/10/2010 h:17:00 play song3 04/10/2010 h.16:30 scrivi testo1 06/10/2010 h:16:00 scrivi testo1 06/10/2010 h:17:00 play song3 ***Solo l'ultimo evento*** *su ogni risorsa risulta annotato*
Le due tabelle raffrontano il diverso modo di registrare la stessa sequenza di eventi. Si noti che ad una analisi "ingenua" delle registrazioni per "sovrapposizione di data", mostrate a destra, le intense e ripetute attivita' sulle canzoni preferite *song1, song2, song3, song4* del 01/10/2010 vengono paradossalmente completamente perse mentre nei giorni 03/10/2010 e 04/10/2010 addirittura non risulta alcuna attivita'.	

Fig.1 Raffronto e limiti della registrazione per "sovrapposizione di data"

La fig.1 seguente illustra in un esempio molto semplice come registrazioni per "sovrascrittura di date" possano trarre in inganno un analista ingenuo, che legge solo le dae in neretto a destra, deducendo ad esempio che non vi sono state attivita' nel pomeriggio dopo le 15:00 del 01/10/2010 o che non vi e' stata alcuna attivita' nei giorni 3 e 4, o che il file *testo1* e' stato scritto soltanto il 06/10/2010. Paradossalmente le attivita' piu' ripetute e frequenti sono quelle che riusltano meno fedelmente registrate, come nell'esempio l'ascolto delle "canzoni preferite" *song1*, *song2*, *song3* e *song4*.

E' quindi necessario *integrare* l'*analisi delle date sovrascritte (es. date di creazione, ultima modifica, ultima apertura etc.)* con quella dei diversi *file di log* prodotti dal sistema (log di crash, log monitoraggio della tastiera, log di sistema, log delle applicazioni etc.) al fine di avere un quadro completo delle attivita' avvenute/non avvenute.

Inoltre e' necessario *verificare che* nell'arco temporale che va da quello di interesse sino alla acquisizione del supporto disco *non siano avvenute attivita' che abbiano potuto compromettere e/o alterare, le marche temporali o i file di log relativi al periodo di interesse dal* 01 Nov 2007 18:00 al 02 Nov 2007 8:00, si nota per inciso che il computer in questione restava in attivita' sino al successivo 6 Novembre 2007.

Le alterazioni possono essere causate, ad esempio, da riesecuzione di file musicali o video che sovrascrivono le date, oppure possono essere causate dall'azzeramento o cancellazione di file di log.

3. Principali punti critici delle consulenze della Polizia Postale.

La sentenza di primo grado ha fondato le proprie considerazioni relative alle interazioni presenti sul computer Mc Book Pro di Raffaele Sollecito, sulla consulenza prodotta dalla polizia postale.

Tale attività tecnica, tuttavia *non può ritenersi metodologicamente corretta*, poiché ha prodotto *risultati fortemente incompleti* e *conclusioni ingiustificate dai dati* disponibili, i punti di maggiore criticitá'sono i sequenti:

1. L'analisi della polizia postale si basa su **selezione preventiva di alcuni file attraverso il software ENCASE** che opera utilizzando solo 3 date di sistema (tra le 5 presenti nei sistemi Mac), e su un **successivo approfondimento delle info di alcuni dei file risultanti da tale selezione utilizzando "Spotlight" e/o il Finder**; cioè l'interfaccia grafica del sistema operativo (es. vedi perizia su "Il fantastico mondo di Amelie").
2. Non viene menzionata una **attività di apertura file multimediale "Naruto episodio 101" avvenuta Giovedì 01 Nov 2007 alle ore 21:26.**
3. Nella perizia **vengono ignorati i log delle applicazioni (ad es. VLC) ed i log di tastiera** che indicano l'inizio e la fine delle attività del computer
4. Non viene menzionata una **attività di ascolto brani musicali avvenuta tra le 5:41 e le 6:38 del mattino del 2 Novembre 2007**
5. **non vengono analizzate informazioni al di fuori del periodo 01 Nov 2007 18:00 – 02 Nov 2007 8:00** quindi l'analisi della polizia non discute e non rileva eventuali cause di alterazione/sovrascrittura delle info relative al periodo di

interesse, e parimenti non si rilevano eventi successivi causati da azioni avvenute nel periodo di interesse

6. nelle conclusioni effettuate si utilizza una **ipotesi metodologica gravemente errata**, cioe' *si assume che l'assenza di marche temporali in un certo periodo sia probatoria della assenza di attivitá sul computer* (si veda anche il paragrafo 1), omettendo di evidenziare che qualsiasi attivitá successiva su un file puó alterarne la data (il computer in questione é stato utilizzato ed é rimasto ininterrottamente acceso per ben 4 giorni dopo il periodi di interesse) oppure che vi sono attivita' che non lasciano traccia (es. lettura di CD/DVD), mentre all'interno del laptop e' stato anche rinvenuto un CD di musicale tra i numerosi in possesso di Raffaele Sollecito
7. Non viene menzionato l'utilizzo **della applicazione *SAMBA*** con cui dal MacBook si accedeva in rete (disco virtuale) all'harddisk dell'altro laptop di Raffaele Sollecito (Acer) che risulta inservibile ai fini degli accertamenti
8. Non viene menzionata una **attivita' di accesso certo al computer** di proprieta' di Raffaele Sollecito per consultazione di una pagina web **avvenuta il 5 Novembre 2007 mentre lo stesso era sottoposto ad interrogatorio**
9. Non vengono menzionate **alterazioni di date su un numero rilevante di file avvenute sul computer stesso in un periodo successivo alla sua acquisizione da parte della autorita' giudiziaria**, la alterazione ha riguardato numerosi file di filmati (tra cui lo stesso Naruto Episodio 101 di cui al punto 6).

Nei successivi paragrafi tali criticitá saranno esaminate nel dettaglio raggruppando l'esame per punti omogenei.

1. **Analisi limitata alle sole tre date di file rilevate da Encase**
2. **Apertura del file multimediale "Naruto episodio 101" avvenuta Giovedì 01 Nov 2007 alle ore 21:26**

È evidente che seguendo il metodo che limita l'analisi delle date a quelle rilevate da Encase, se un file non viene individuato nella fase di selezione iniziale (cioè se le tre date non sono nel periodo di interesse) esso viene escluso dai risultati della ricerca ristretta successiva, anche se presenta una delle altre due date (su cinque complessive[4]) localizzate nel periodo di interesse.

Tale metodologia errata ha prodotto risultati fortemente incompleti, infatti, a seguito di ulteriori approfondimenti compiuti dal consulente della difesa, successivi alla definizione del giudizio di primo grado, utilizzando per la prima volta un sistema operativo della stessa *versione* e *built*[5] di quello utilizzato da Raffaele Sollecito, cioè Mac OS X **10.4.10 (Build 8R2232),** è stato possibile ottenere la corretta visualizzazione dei dati acquisendo informazioni di fondamentale importanza per la prova di attivitá.

[4] Nei sistemi Mac OS X i dati temporali (data ed ora) che annotano le principali operazioni effettuate sui file, vengono in parte conservati in strutture dette inode del *file system* HFS+ (cioe' del sistema di gestione della memoria disco), ed in parte in altre aree di memoria.
In particolare gli inode, mantengono:
ACCESS, l'ultimo accesso in lettura o scrittura effettuato al file, ad esempio per copiarlo
MODIFY, l'ultima modifica in scrittura effettuata al contenuto del file
CHANGE, l'ultima modifica all'inode
CREATE, la data di creazione. Altre aree di memoria mantengono invece ulteriori informazioni, sull' utilizzo del file diverse dalle precedenti quali la data di ULTIMA APERTURA, cioé l'ora in cui il file e' stato aperto con uno strumento, quale ad esempio un "player". É da notare che se si apre il file in lettura in modo diverso (ad esempio da riga comando unix), la data ULTIMA APERTURA non viene modificata. La data di ULTIMA APERTURA e' visibile utilizzando l'interfaccia grafica "spotlight" del sistema operativo mentre non é visibile da riga di comando.
Le informazioni sui file sono visibili con *appositi programmi* (es.ENCASE), con *appositi comandi* (es. stat) o anche con l'*interfaccia grafica "spotlight"* utilizzabile da un qualsiasi utente. Se le informazioni vengono lette con una versione di sistema operativo diversa da quella con cui esse sono state scritte possono apparire informazioni diverse da quelle corrette o non essere affatto leggibili. Cio' e' particolarmente vero per i dati estesi o gestiti dalle applicazioni, quali le date di ULTIMA APERTURA. In particolare si nota che la data ACCESS corrisponde alla data di chiusura di un brano musicale o film, mentre la data ULTIMA APERTURA all'inizio dell'ascolto/visualizzazione \
Va inoltre ricordato che, come giá detto, oltre a queste date, alcuni programmi mantengono date informazioni sulle attivita' svolte in appositi file in formato XML detti *plist* nei sistemi MacOS, o in appositi *file di log*.

[5] Sistema Operativo
I sistemi operativi vengono aggiornati continuamente, quello utilizzato da Raffaele Sollecito era la versione 10.4.10 (Build 8R2232) di Mac Os X nome in codice Tiger. Del sistema operativo Mac OS X "Tiger" sono state prodotte 12 versioni (da 10.4, 10.4.1, a 14.4.11) per un totale 29 "built" diverse (la "built" e' una ricompilazione della versione con piccoli dettagli di differenza). Il risultato evidenziato sul film Naruto Episodio 101 é stato ottenuto analizzando l'hard disk con la stessa esatta versione di sistema operativo presente nel Mac OS X di Raffaele Sollecito.

Si legge invece nel rapporto della Polizia di Stato del 19 Novembre 2007 prot.1975/207, avente per oggetto la attivita' di analisi del materiale sequestrato ed indirizzato alla Procura della Repubblica di Perugia che

> ANALISI DEI DATI
>
> La ricerca di interattività sul pc è stata condotta estrapolando tutti i file creati, scritti, modificati, cancellati e sul quale vi era stato un ultimo accesso, tra le ore 18:00 del 01/11/2007 e le ore 08:00 del 02 Novembre.

sono stati quindi esplicitamente esclusi dalla analisi tutti i file che avrebbero potuto modificare tali informazioni, poiche' accesso/modifica/scrittura avvengono per sovrascrittura di date.

Viene rilevato soltanto una attivita' sino alle 21:10:32 relativa al film "Il Favoloso Mondo di Amelie"

> Dall'analisi era possibile affermare che vi era stata interattività sulla macchina nel tardo pomeriggio del 01 novembre, quando tra le ore 18:27:15 e le ore 21:10:32 veniva visionato, tramite il programma "VLC", il film "Il Favoloso Mondo Di Amelie".

che si afferma di aver anche verificato tramite un "pc portatile Apple con caratteristiche tecniche **analoghe** a quelle dell'indagato"

> A conferma di quanto sopra scritto è stato rigenerato su di un idoneo supporto magnetico, l'Hard-disk dell'indagato mediante il "Restore Drive" di Encase, con detto supporto è stato poi avviato un pc portatile Apple con caratteristiche tecniche analoghe a quello dell'indagato. Una volta avviato il pc si è andati a cercare il file video denominato **"Il Favoloso Mondo Di Amelie"** identificato dal percorso **HITACHI\1 Merged_Untitled\MacOS HD\Users\macbookpro\Desktop\aMule Downloads\Film visti\[DivX - ITA] - Il Favoloso Mondo Di Amelie.avi** , da qui, controllando le proprietà del file, era possibile verificare che l'ultima apertura dello stesso risaliva appunto alle ore 18:27 del 01/11/2007 ed era stata eseguita appunto mediante il programma "VLC" (vedi allegato nr.03).

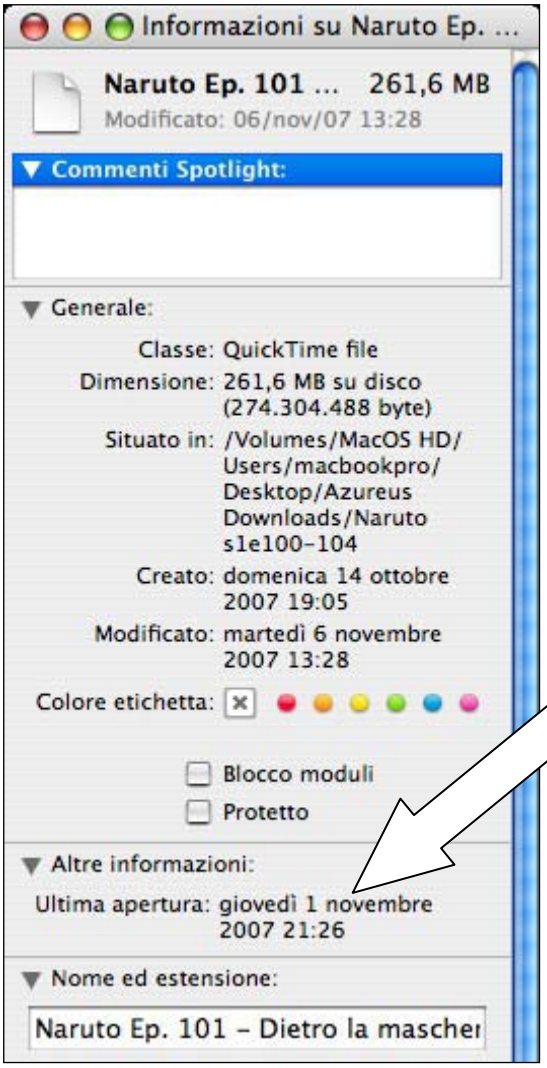
Preme rilevare, infatti, che la sentenza impugnata, basandosi su tale analisi, ha collocato alle **21:10:32** l'ultima operazione compiuta da Raffaele Sollecito nella giornata del 1° novembre 2007.

In realta nell'hard disk di Raffaele Sollecito si trova almeno un file "Naruto ep. 101.avi" che viene escluso dall'analisi poiche' le sue date di modifica esulano dall'intervallo ristretto in cui la Polizia Postale ha effettuato la ricerca, il file generato da Encase riporta infatti

1	Name	Last Accessed	File Created	Last Written
63514	Naruto Ep. 101 - Dietro la maschera - By Gadriel[ITA].avi	6-nov-07 10.18	14-ott-07 19.05	6-nov-07 13.28

Effettuando invece una ricerca con "*Spotlight*" nella versione Mac OSX 10.4.10 tale file ***"Naruto ep 101.avi"*** riporta come data di ultima apertura giovedì 1° novembre 2007 alle **ore 21:26** (cioè nel periodo preso in esame dalla polizia postale: 1° novembre 2007 ore 18:00 – 2 novembre 2007 ore 8:00).

Si vede infatti la seguente finestra di Spotlight:



Tale file non viene in alcun modo reperito dalla Polizia postale che aggiungeva altresì:

> Dall'analisi era possibile affermare che vi era stata interattività sulla macchina nel tardo pomeriggio del 01 novembre, quando tra le ore 18:27:15 e le ore 21:10:32 veniva visionato, tramite il programma "VLC", il film "Il Favoloso Mondo Di Amelie" .

ommiss

> Nelle ore successive non vi sono state operazioni effettuate dall'utilizzatore sino alle 05:32:08, quando è stato lanciato il programma VLC per riprodurre alcuni file audio.

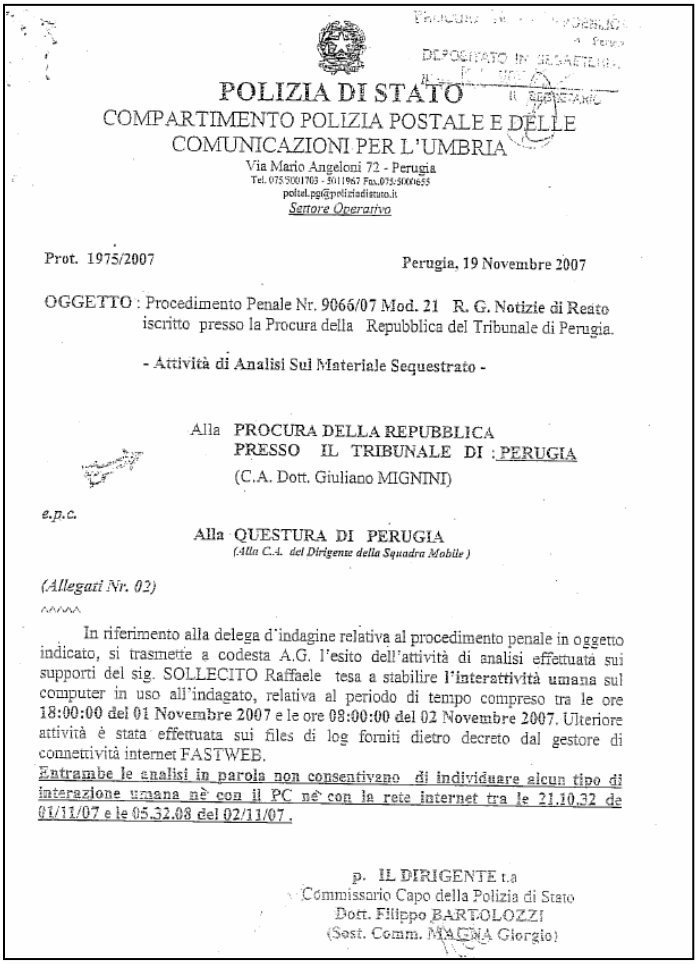
E’ evidente che tale file non e’ stato rilevato sopratutto per il grave errore metodologico di limitare il periodo delle date dei file esaminati da ENCASE alla data massima delle ore 8:00 del 2 novembre 2007, e per non aver verificato con Spotlight (nella **esatta versione** del computer dell’indagato e non con una **versione “analoga”**). Il fatto che ENCASE riporti la data di ultimo accesso al 6 Novembre 2007, non e’ in contraddizione con tale risultanza poiche’:

- la data ultima apertura visualizzata da Spotlight e’ gestita tra le *Altre Informazioni* cioe’ viene modificata dalle applicazioni (ad esempio quando si guarda il film), mentre le date mostrate ENCASE si limitano alle date del file system (che sono modificate, ad esempio copiando o leggendo il file con un programma);

Una attivita’ sconosciuta avvenuta il 6 Novembre 2007 ha quindi sicuramente modificato la data di ultimo accesso e quella di ultima modifica del file “Naruto Ep.101” senza pero’ modificare quella di “ultima apertura” che risulta invece ancora visibile.

Va inoltre evidenziato come la data di ultimo accesso (martedì 6 novembre 2007 ore 10:18:38) e di ultima modifica di tale file (martedì 6 novembre 2007 ore 13:28:09) corrispondono ad *un periodo coincidente con il prelievo del laptop dalla abitazione di Raffaele Sollecito, periodo nel quale vengono rilevate anche numerose altre attività sul suddetto portatile testimoniate dai file di log di sistema.*

Deve essere infine notato che la durata del suddetto episodio animato e’ di circa 20 minuti, se tale filmato sia stato guardato per intero o meno non e’ dato di sapere, poiche’ alterazioni successive hanno sovrascritto tale informazione, come hanno fatto ad esempio le alterazioni avvenute martedí 6 novembre 2007 al momento e successivamente al sequestro del computer.



POLIZIA DI STATO
COMPARTIMENTO POLIZIA POSTALE E DELLE COMUNICAZIONI PER L'UMBRIA
Via Mario Angeloni 72 - Perugia
Tel. 075 5001703 - 5011967 Fax.075/5006655
poltel.pg@poliziadistato.it
Settore Operativo

Prot. 1975/2007 Perugia, 19 Novembre 2007

OGGETTO : Procedimento Penale Nr. 9066/07 Mod. 21 R. G. Notizie di Reato iscritto presso la Procura della Repubblica del Tribunale di Perugia.

- Attività di Analisi Sui Materiale Sequestrato -

Alla PROCURA DELLA REPUBBLICA
PRESSO IL TRIBUNALE DI : PERUGIA
(C.A. Dott. Giuliano MIGNINI)

e.p.c.

Alla QUESTURA DI PERUGIA
(Alla C.A. del Dirigente della Squadra Mobile)

(Allegati Nr. 02)

In riferimento alla delega d'indagine relativa al procedimento penale in oggetto indicato, si trasmette a codesta A.G. l'esito dell'attività di analisi effettuata sui supporti del sig. SOLLECITO Raffaele tesa a stabilire l'interattività umana sul computer in uso all'indagato, relativa al periodo di tempo compreso tra le ore 18:00:00 del 01 Novembre 2007 e le ore 08:00:00 del 02 Novembre 2007. Ulteriore attività è stata effettuata sui files di log forniti dietro decreto dal gestore di connettività internet FASTWEB.
Entrambe le analisi in parola non consentivano di individuare alcun tipo di interazione umana nè con il PC nè con la rete internet tra le 21.10.32 de 01/11/07 e le 05.52.08 del 02/11/07 .

p. IL DIRIGENTE t.a
Commissario Capo della Polizia di Stato
Dott. Filippo BARTOLOZZI
(Sost. Comm. MACCIA Giorgio)

3. Nella consulenza vengono ignorati i log di tastiera che indicano l'inizio e la fine delle attività del computer ed i log di importanti applicazioni utilizzate nel periodo in questione, tra cui i log di VLC

Nella consulenza della polizia postale non vengono menzionati i file di log, di alcune applicazioni, in particolare i file di log di VLC ed i file di log di tastiera che consentono di chiarire importanti attivitá nel periodo di interesse.

File di log di VLC

Il file *plist* (property list) di VLC contiene tra le altre informazioni l'elenco degli ultimi file multimediali che sono stati visionati.

Solitamente tali file vengono mostrati all'utente che apre l'applicazione in un menu a scorrimento, per poterli richiamare piu' facilmente.

In particolare tale elenco presenta, in ordine inverso dal piú recente al piú remoto il seguente elenco di filmati:

	Percorso ultimo file visto in VLC
11	MacOS_HD/Users/macbookpro/Desktop/aMuleDownloads/Stardust-2007.iTALiAN.LD.TC.XviD.CD1-SiLENT.avi
10	MacOS_HD/Users/macbookpro/Desktop/aMuleDownloads/Stardust 2007 Italian Md Tc Xvid-Silent-Cd1.avi
9	MacOS_hD/Users/macbookpro/Desktop/aMuleDownloads/(Divx-Ita) Stardust Ok.avi
8	MacOS_HD/Users/macbookpro/.Trash/(Divxit) Stardust 2007 - Xvid-Italian.avi
7	MacOS_HD/Users/macbookpro/.Trash/(divx - ita) - stardust.avi
6	**MacOS_HD/Users/macbookpro/Desktop/[DivX - ITA] - Il Favoloso Mondo Di Amelie.avi_____**
5	MacOS_HD/Users/macbookpro/Desktop/aMuleDownloads/Film visti/I.Simpson.Il.Film.2007.iTALiAN.LD.DVDSCR.XviD-SiLENT.avi
4	MacOS_HD/Users/macbookpro/Desktop/[DivX-JAP] - Suicide Club (sott. ita).avi
3	MacOS_HD/Users/macbookpro/Desktop/aMuleDownloads/[DivX-JAP]-SuicideClub(sott. ita).avi
2	MacOS_HD/Users/macbookpro/Desktop/aMuleDownloads/Film visti/Spider (D Cronemberg).AVI
1	MacOS_HD/Users/macbookpro/Desktop/aMuleDownloads/SouthParkSerie11(incompleta)/[XviD - ITA-ENG] South Park - 1101 - With Apologies to Jesse Jackson.avi

Si notano alcune informazioni rilevanti, (anche queste assenti dalla analisi della Polizia):

a) il film "Il favoloso Mondo di Amelie" **risulta in un percorso diverso da quello indicato da ENCASE** e dalla relazione della Polizia Postale
b) vi sono rilevanti attivita' riguardanti 5 **versioni diverse dello stesso film "Stardust"** successive alla visione del film "Il favoloso Mondo di Amelie"

a) il film "Il favoloso Mondo di Amelie" risulta in un percorso diverso da quello indicato da ENCASE e dalla relazione della Polizia Postale

In particolare si nota che, mentre VLC (che ricordiamo e' un visore di film e multimedia) lo colloca sul percorso:

MacOS_HD/Users/macbookpro/Desktop

Nell'hard disk analizzato il file risulta sul percorso

MacOS_HD/Users/macbookpro/Desktop/aMule Downloads/Film visti

L'informazione rilevante che se ne deduce e' che al momento della visione il file in questione risultava direttamente sul "Desktop", mentre successivamente veniva posto nella cartella "Film Visti" rivelando un comportamendo consequenziale ad una visione completa del film stesso, mentre in piu' momenti si e' dubitato della visione intera del film che avrebbe potuto scorrere senza che effettivamente nessuno lo visionasse. In realta' queste due informazioni sul percorso suggeriscono che l'interazione delle 21:10:02 e' dovuta con ogni probabilità allo spostamento del film per terminata visione.

analoghe a quello dell'indagato. Una volta avviato il
video denominato **"Il Favoloso Mondo Di Amelie"** identificato dal percorso **HITACHI\1 Merged_Untitled\MacOS HD\Users\macbookpro\Desktop\aMule Downloads\Film visti\[DivX - ITA] - Il Favoloso Mondo Di Amelie.avi** , da qui, controllando le proprietà del file, era possibile verificare che l'ultima apertura dello stesso risaliva appunto alle ore 18:27 del 01/11/2007 ed era stata eseguita appunto mediante il programma "VLC" (vedi allegato nr.03).

b) vi sono rilevanti attivita' riguardanti 5 versioni diverse dello stesso film "Stardust" successive alla visione del film "Il favoloso Mondo di Amelie"

I file in questione, da quello di visione piu' recente al piu' remoto sono:

```
Stardust-2007.iTALiAN.LD.TC.XviD.CD1-SiLENT.avi
Stardust 2007 Italian Md Tc Xvid-Silent-Cd1.avi
(Divx-Ita) Stardust Ok.avi
(Divxit) Stardust 2007 - Xvid- Italian.avi
(divx - ita) - stardust.avi
```

Si noti che tale comportamento di visionare piu' copie e' tipico di chi scarica piu' copie di uno stesso film per tenere le migliori, oppure quelle che vengono scaricate per prime, evitando copie fasulle (spam).
Le varie versioni scaricate vengono visionate e si conservano le migliori.

Si noti che l'ultima scrittura sul file "(Divx-Ita) Startdust Ok.avi" riportata da ENCASE e' alle 19:18 del 01/11/2007

1	Name	Last Accessed	File Created	Last Written
62409	(Divx-Ita) Stardust Ok.avi	6-nov-07 2.47	1-nov-07 17.03	1-nov-07 19.18

ora in cui presumibilmente ne viene terminato lo scaricamento da rete tramite il programma peer-to-peer *aMule,* infatti il file si trova attualmente nella cartella dei "downloads" di aMule nel percorso:

HITACHI \HITACHI\1 Merged_Untitled\MacOS HD\Users\macbookpro\Desktop\aMule Downloads\(Divx-Ita) Stardust Ok.avi

Ancora una volta non e' dato di sapere con certezza se sia stato acceduto e visionato nel periodo immediatamente successivo al termine dello scaricamento poiche' come si notera' alle ore 2:47 del 6-nov-2007, (un periodo in cui l'indagato era trattenuto sotto interrogatorio) la data precedente di "Ultimo accesso" e' stata sovrascritta.

Infine si rileva una circostanza insolita, secondo le informazioni di ENCASE tutti gli altri file "Stardust" mostrati dal menu' di VLC non risultano ne' tra i file presenti nel disco ne' tra quelli cancellati.

Tale problema veniva rilevato anche dalla Polizia Postale che forniva al riguardo della scomparsa di questi ed altri file messi a scaricare tramite aMule, la seguente spiegazione:

I file cancellati

I consulenti hanno prodotto in allegato alla loro controanalisi parte del log di Amule (versione per utenti della rete FASTWEB del noto software P2P denominato Emule), relativo al periodo compreso tra le ore 17:01:56 e le ore 21:28:25 del giorno 01/11/2007, dal quale si evince che il software Amule, in detto arco di tempo, ha eseguito il download completo di 3 dei 6 file messi a scaricare: si tratta di file riconducibili ad un filmato dal titolo "*Stardust*".

L'ipotesi avanzata dalla relazione dei c.t.p. è che due dei tre file di cui è stato terminato il download "sono stati cancellati manualmente da un operatore, direttamente dall'interfaccia di Amule dopo le ore 21.28" (orario di fine dell'ultimo download ndr).

. E' parere di quest'ufficio che sia vero che tali file siano stati rimossi dal sistema, ma non attraverso l'interfaccia di Amule, in quanto, in tal caso, nel log prodotto dall'applicativo stesso, sarebbero state trovate le indicazioni relative alla data e ora della cancellazione (il programma avrebbe generato una riga di log con i seguenti campi: *Data, Ora, Cancellazione file e* "nome file", come accaduto nel caso del download del file seguente, estrapolato dal medesimo log:
2007-11-01 17:04:02: Download di Stardust.2007.iTALiAN.MD.TC.XviD-SiLENT-CD2.avi
2007-11-05 13:05:33: Cancellazione file: Stardust.2007.iTALiAN.MD.TC.XviD-SiLENT-CD2.avi).

Inoltre la cancellazione effettuata con le normali operazioni di eliminazione del file che il sistema operativo prevede, è avvenuta *tra le ore 21.28 del giorno 01.11.2007 e l'ora del sequestro del computer, avvenuto il giorno 06.11.2007.*

La circostanza ha a nostro parere due altre possibili spiegazioni non mutuamente esclusive:

-ENCASE non riesce a rilevare completamente i file cancellati dal sistema Mac OS X nella versione del laptop di Raffaele Sollecito

-i file risiedevano in un disco virtuale esterno al laptop (vedi punto 5 su applicazione SAMBA)

E' comunque assodato dal file di VLC che tali file sono stati visionati successivamente alla visione del file "Amelie".

I log di tastiera

Nella analisi della Polizia Postale viene ignorata una finte di informazione di fondamentale importanza, che contiene informazioni registrate come *elenco di marche temporali* e non tramite *sovrascrittura di date*, si tratta dei ***log di tastiera***, contenuti nel file *windowserver.log*.

Tale file e' molto importante poiche' il sistema Mac OS X registra su di esso gli eventi principali che riguardano la attivazione/disattivazione della tastiera. Questo eccesso di informazioni e' stato anche largamente discusso dagli utenti Apple come eccessivo, questo, ad esempio e' un commento su un blog di utenti Apple vicino al periodo in questione (luglio 2007).

In sostanza in tale file vengono registrati le date delle attivita' della tastiera utente attraverso una semplice sequenza di "acceso/spento". Quando la tastiera e' disattivata ("spento")

sicuramente non c'e' stata una interazione umana con tastiera o mouse. La prima volta che tastiera o il mouse vengono utilizzati viene registrata una attivita' di "acceso", cioe' si segnala che il sistema e' attivo. Dopo un certo periodo (quattro minuti nel caso in questione) se non vi sono attivita' la tastiera va in "standby" e, se configurato puo' partire il salvaschermo.
Alcuni programmi, come ad esempio VLC o altri programmi per la visione di film o l'ascolto di musica lasciano la tastiera ed il computer nella posizione di "acceso" in modo da non interrompere o disturbare mai la visione o l'ascolto.

L'analisi del file di log *windowserver.log* e' quindi fondamentale per analizzare **i periodi in cui il computer puo' essere stato utilizzato** o **con certezza non e' stato utilizzato**.

Dall'analisi del windowserver.log di Raffaele Sollecito, per il periodo considerato dalla Polizia, risulta una sequenza di log che identifica i seguenti periodi:

1-Nov-2007	17:03:34		**risveglio tastiera**
	sistema attivo per 0:49:44		
	17:53:18		disabilita tastiera
	inattivo per 0:32:56		
	18:26:14		risveglio tastiera
	sistema attivo per 11 h circa		
2-Nov-2007	5:32:04		crash di VLC
	5:36:18		disabilita tastiera
	inattivo per 5 minuti e 16 secondi		
	5:41:34		risveglio tastiera
	sistema attivo *per* 0:04:18		
	5:45:52		disabilita tastiera
	5:46:02	inattivo per 0:00:10	risveglio tastiera
	5:50:16	**attivo per 0:04:14**	disabilita tastiera
	5:56:34	inattivo per 0:06:18	risveglio tastiera
	6:00:46	**attivo per 0:04:12**	disabilita tastiera
	6:06:38	inattivo per 0:05:52	risveglio tastiera
	6:14:37	**attivo per 0:07:59**	disabilita tastiera
	6:18:16	inattivo per 0:03:39	risveglio tastiera
	6:22:28	**attivo per 0:04:12**	disabilita tastiera
	inattivo per 5:55:56		
	12:18:24		risveglio tastiera
	12:26:33	**attivo per0:08:09**	disabilita tastiera
	inattivo per 18 h circa		
3-Nov-2007	5:42:12		risveglio tastiera

E' da notare che nel periodo tra le 18:26:14 del 1 Novembre e le 5:3:18 del 2 novembre 2007 il sistema e' attivo senza interruzione, presumibilmente un player multimediale, come ad esempio VLC, o altri player per CD e DVD che lo mantengono attivo. La disabilitazione della tastiera che avviene alle 5:36:18 causata da una crash di VLC alle 5:32:04, ed e' subito seguita da una nuova interazione dopo 5 minuti e 16 secondi. Si susseguono interazioni brevi interazioni per attivazioni di canzoni sino alle 6:22:28. Il sistema resta poi inattivo per circa 6 ore sino alle 12:18:24.

L'analisi della attivita' di tastiera non era presente nella relazione della Polizia Postale.

4. **Non viene menzionata una <u>attività di ascolto brani musicali avvenuta tra le 5:41 e le 6:38 del mattino del 2 Novembre</u>**

Dalla relazione della Polizia non viene menzionata la attivita' di ascolto di brani musicali, avvenuta nel periodo in questione. Tale attivita' e' rilevabile da varie fonti dati, sia dai report di ENCASE che contengono le date di accesso ai file, sia dal file di log contenuti nella libreria musicale di iTunes denoiminato "iTunes Music Library.xml", l'analsi di iTunes e' importante poiche' esso memorizza l'ultima volta che una canzone e' stata completamente ascoltata distinguendo se e' stata solo ascoltata in parte ("skipped') Le canzoni ascoltate risultano:

Canzone	**Orario inizio da ENCASE**	**Termine ascolto da iTunes**
10 Stealing fat.mp3	11/2/2007 5:44:45	Non risulta
Breed.MP3	11/2/2007 5:46:11	2007-11-02 05:49:15
Come as you are.mp3	11/2/2007 5:49:12	2007-11-02 05:52:54
In bloom.mp3	11/2/2007 5:52:51	2007-11-02 05:57:09
Lithium.MP3	11/2/2007 5:57:06	2007-11-02 06:01:26
32 32 POLLY.MP3	11/2/2007 6:06:24	2007-11-02 05:44:48
Smells like teen spirit.mp3	11/2/2007 6:06:24	2007-11-02 06:06:27
Its My Life.mp3	11/2/2007 6:06:39	Non risulta
32 Prelude.MP3	11/2/2007 6:06:41	Non risulta
05 Songbird.mp3	11/2/2007 6:06:42	2007-11-02 06:08:52
06 Little by little.mp3	11/2/2007 6:11:51	2007-11-02 06:13:45
Dont look back an anger.MP3	11/2/2007 6:13:42	2007-11-02 06:18:09
07 Sleeping Awake.mp3	11/2/2007 6:18:07	2007-11-02 **Skipped** 06:18:17
Jan Johnston - Flesh (DJ Tiesto remix).mp3	11/2/2007 6:18:17	Non risulta

Ancora una volta si fa notare che la tipica modalita' con cui gli utenti ascoltano canzoni e' quella dell'*ascolto ripetuto* delle canzoni preferite. Poiche' le informazioni sono registrate per sovrascrittura delle date, dell' ascolto ripetuto delle stesse canzoni nella stessa serata non risulterebbe che l'ultima data di ascolto. Dal file iTunes risulta poi che molte canzoni sono possedute sin dal 2005.

Infine si fa notare che tra le ultime operazioni effettuate sul computer prima delle 8:00 del 2 novembre 2007, termine del periodo in oggetto risulta una interazione per

attivazione/disattivazione di Front Row, che e' in grado di suonare brani e filmati scaricandoli direttamente dal web su file temporanei che poi vengono cancellati

Front Row	02/11/2007 6:18:33 (Last Accessed Date *da ENCASE*)

Alcuni minuti dopo la disattivazione della tastiera delle 6:22:28 del 2 novembre, cioe' alle 6:38 viene poi rilevata una interazione con il file "DVDPlayback" che fa presumere la presenza nel laptop di un DVD per filmati o per musiche che chiaramente non puo' essere rilevato da alcun programma come ENCASE.

DVDPlayback	02/11/2007 6:38:40 33 (Last Accessed Date *da ENCASE*

in quanto i relativi file e le relative date non vengono modificate.

5. **<u>non vengono analizzate informazioni al di fuori del periodo 01 Nov 2007 18:00 – 02 Nov 2007 8:00</u> quindi l'analisi della polizia non discute e non rileva eventuali cause di alterazione/sovrascrittura delle info relative al periodo di interesse, e parimenti non si rilevano eventi successivi causati da azioni avvenute nel periodo di interesse.**
6. **nelle conclusioni effettuate si utilizza una <u>ipotesi metodologica gravemente errata</u>, cioe' *si assume che l'assenza di marche temporali in un certo periodo sia probatoria della assenza di attivitá sul computer* (si veda anche il paragrafo 1), omettendo di evidenziare che qualsiasi attivitá successiva su un file puó alterarne la data (il computer in questione é stato utilizzato ed é rimasto ininterrottamente acceso per ben 4 giorni dopo il periodi di interesse) e che alcune a**

L’esame delle diapositive power point presentate in dibattimento conferma l’impostazione metodologica di cui al primo punto , gravemente minata dalla limitazione all’analisi dei file con date nel periodo in questione,

ad esempio le date di scrittura e modifica del file “iTunes Music Library.xml” cosi’ come rilevata da ENCASE risultano

1	Name	Last Accessed	File Created	Last Written
7147	iTunes Music Library.xml	5-nov-07 13.35		6-nov-07 0.58

rispettivamente il 5 Novembre ed il 6 Novembre 2007, e verrebbero quindi escluse dall’analisi della Polizia Postale.

Mentre e’ noto che “iTunes Music Library” contiene le date di importanti interazioni nel periodo in esame, come ad esempio le date di ascolto dei brani musicali prima menzionati.

L’affermazione quindi che “*non sono stati rinvenuti file modificati e/o cancellati nell’arco temporale della ricerca*” per quanto corretta nel senso letterale che *e’ vero che i consulenti non hanno rinvenuto tali file,* testimonia una grave imperizia metodologica, visto che e’ evidente che il file “iTunes Music Library .xml” e’ stato modificato proprio nel periodo temporale della ricerca, poiche’ contiene registrazioni di eventi avvenuti in quel periodo (le date di ascolto delle canzoni). Esso e’ stato pero’ modificato anche successivamente, e per questo riporta una data di modifica posteriore. Il criterio di limitarsi ad analizzare i file dello stretto periodo richiesto e’ fuorviante, specie considerando che il computer e’ stato accesso per oltre quatro giorni ulteriori.

Nella presentazione delle conclusioni viene affermato che “non viene registrata interazione umana”

,
mentre non viene menzionata affatto:

- la **tastiera che resta attiva** per tutto il periodo in questione (21:00-5:44 circa) ,
- la visione del file **"Naruto Ep.101.avi"** iniziata alle (il filmato ha durata di circa 20 minuti)
- il fatto che la tastiera venga ***riattivata subito dopo il crash di VLC***, mentre si parla erroneamente di "attivazione VLC", (esso non viene attivato dall'utente, ma e' l'utente che si attiva dopo il suo crash!);
- non vengono indicate le interazioni umane relative al playing di canzoni registrate dalle 5:44 circa in poi;
- **non viene analizzato il plist di VLC** che riporta visione di altri brani successivi ad "Amelie";
- **non viene menzionato lo spostamento del file "Amelie" dal "Desktop" alla cartella "film visti";**
- non viene preso in considerazione il fatto che le **"registrazioni di interazione umana"** nel periodo in questione possano essere state successivamente **sovrascritte**, come e' avvenuto per il file delle canzoni "iTunes Music Library.xml", o per l'ultimo accesso a "Naruto Ep.101";
- non viene presa in considerazione la possibilita' di **ascolto/visione di CD/DVD** pur risultando un CD musical del gruppo "Blind Guardian" presente all'interno del portatile sequestrato, e che non lascerebbe tracce su disco se ascoltato.

Peraltro dal verbale di acquisizione del materiale informatico sequestrato a Raffaele Sollecito del 15 novembre 2007, a firma degli ufficiali e agenti di Polizia Postale Bartolozzi, Trotta, Trifici ed alla presenza del consulente tecnico Formenti risulta che

esecuzione della verifica.- ==========
Dal controllo del lettore ottico tipo slot-in era possibile rinvenire all'interno del lettore ottico un CD musicale del gruppo BLIND Guardian.- ==========
Alle ore 16:30 è stato dato inizio alle

L'ipotesi che il PC nel periodo in esame abbia potuto suonare un CD, non viene presa in considerazione ed il rinvenimento all'interno del PC non viene menzionato.

Si nota come il grafico presentato in dibattimento, che mostra un "gap" annotato con la frase "non viene registrata alcuna interazione umana", sia semanticamente fuoriviante suggerendo che l'assenza di tracce di interazione sia una prova della assenza di interazione. A parte che, come si e' visto, non tutte le tracce presenti sono state individuate, inoltre, come si e' visto nell'esempio in fig.1, la sovrascrittura di date puo' dare effetti paradossali, "cancellando" tracce esplicite proprio durante periodi di intense attivita' ripetute. Si e' inoltre fatto un uso semanticamente ambiguo del termine "tabulati ENCASE" accostandoli ai piu' comuni "tabulati telefonici", e non evidenziando che, mentre questi ultimi registrano *sequenze di eventi*, dove un "gap" corrisponde effettivamente e con certezza ad assenza di attivita', i tabulati ENCASE sono invece elenchi di date per sovrascrittura ed i numerosi "buchi" temporali non sono affatto prova di assenza di attivita' in tali periodi.

Riassumendo:

Nel periodo temporale intercorrente le 21:26 del 1 novembre (inizio visione Naruto Ep. 101) e le 5:41:34 (risveglio tastiera successivo al crash di VLC), sono numerose e diverse attivita' che possono essere *ragionevolmente avvenute* la cui data puo' essere stata sovrascritta, tra quel momento ed il momento sequestro del laptop (6 novembre 2007) o che per loro natura non possono aver lasciato traccia su disco:

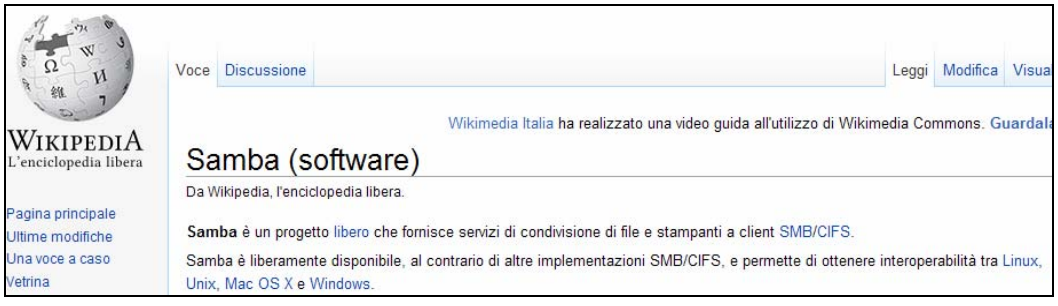
- **ascolto di brani musicali tramite iTunes o FrontRow o altro player**, ripetuto in seguito (in effetti al termine della nottata e nei giorni successivi vengono ascoltati numerosi brani in possesso da lungo tempo, vedi date di iTunes);
- **visione di filmati come Naruto Ep.101** la cui data e' stata sovrascritta successivamente al momento del sequestro del computer (in effetti le date di accesso di numerosi file filmati .avi sono state sovrascritte il 6 Novembre intorno alle 10:18 o dopo le 13:00);
- **visione di filmati come Startdust, successivamente cancellati** (i filmati Startdust sono stati sicuramente visionati in un periodo imprecisato successivo alla visione di "Amelie" e prima del sequestro del computer come testimoniato dai log di VLC plist);

- **visione di filmati/musiche su disco virtuale** del computer Asus tramite Samba, l'hard disk reale non e' piu' disponibile;
- **visione di filmati/musiche su supporto DVD** o CDROM che per loro natura non lasciano traccia (in effetti alle 6:38 del 2 novembre risulta attivato FrontRow e DVDPlayback ed al momento del sequestro un **CD del gruppo Blind Guardian viene rinvenuto nel computer** di Raffaele Sollecito, che pure ne possiede in quantita').

A favore della visione continuativa di filmati o di musica depone il fatto che la tastiera non va mai in *standby*, quindi una applicazione o una interazione umana la mantengono attiva (FrontRow? iTunes? VLC?). Inoltre l'applicativo VLC va in crash alle 5:32:04 e pochi minuti dopo il successivo standby il computer viene nuovamente risvegliato alle 5:41:34 tramite una interazione, che testimonia una presenza umana continuativa nei pressi del computer e della applicazione musicale o di filmato che viene in quel modo interrotta e di cui presumibilmente ci si accorge riattivandola. Inoltre non vi sono interazioni con FrontRow o con il lettore DVD successive alla notte del 2 novembre.

7. Non viene menzionato l'utilizzo <u>della applicazione *SAMBA*</u> con cui dal MacBook si accedeva in rete (disco virtuale) all'harddisk dell'altro laptop di Raffaele Sollecito (Acer) che risulta inservibile ai fini degli accertamenti

E' appurato che Raffaele Sollecito utilizzava il vecchio computer Acer soltanto come "muletto" per scaricare film/canzoni dalla rete, il problema di trasferire i file da suddetto Acer al Mac per la visione/ascolto veniva risolto utilizzando la applicazione SAMBA che consente di montare un disco remoto, facendolo apparire "virtualmente" come un disco locale del proprio computer.



In altre parole, con SAMBA era possibile aprire un file sul computer Apple senza che questo lasciasse traccia su tale computer, in quanto esso si trovava in un disco/cartella virtuale dell'Apple essendo effettivamente, in realta', nell'Acer.

Viceversa se un file dal disco virtuale veniva gettato nel cestino dell'Apple, esso veniva cancellato, ma non poteva essere ritrovato certamente tra i file cancellati di Appple tramite un'analisi ENCASE sul solo hard disk del computer Apple.

L'utilizzo di SAMBA rintracciabile nel computer di Raffaele Sollecito spiegherebbe la "scomparsa" senza tracce dei file di "startdust", si noti che almeno due di essi risultavano in VLC gettati nel cestino (.Trash):

```
MacOS_HD/Users/macbookpro/.Trash/(Divxit) Stardust 2007 -
Xvid- Italian.avi
MacOS_HD/Users/macbookpro/.Trash/(divx - ita) -
stardust.avi
```

Samba veniva regolarmente utilizzato e del suo aggiornamento automatico periodico vi e' traccia nei anche nei file ENCASE

1	Name	Last Accessed	File Created	Last Written
6068	samba	3-nov-07 3.16.44	20-ago-06 9.44.19	20-ago-06 9.44.19

8. Non viene menzionata una **attivita' di accesso certo al computer** di Raffaele Sollecito per consultazione di una pagina web **avvenuta il 5 Novembre 2007 mentre lo stesso era sottoposto ad interrogatorio**

Mentre Raffaele Sollecito veniva sottoposto ad interrogatorio, veniva effettuata con certezza una attivita' di accesso al computer in esame. Tale attivita' e' testimoniata sia dai file ENCASE prodotti dalla consulenza della Polizia Postale, sia dal file windowserver.log che registra le attivita' di tastiera, sia dai file di log dell'internet provider.
Infatti la tastiera disattivatasi alle 16:34 del 5 novembre 2007, si riattivava improvvisamente alle 22:04 andando nuovamente in standby alle 22:14.

```
Nov 05 16:34:46  [57] Hot key operating mode is now all disabled
Nov 05 22:04:28  [57] "loginwindow" (0x57cf) set hot key operating mode to normal
Nov 05 22:04:28  [57] Hot key operating mode is now normal
Nov 05 22:14:38  [57] "loginwindow" (0x57cf) set hot key operating mode to all
disabled
Nov 05 22:14:38  [57] Hot key operating mode is now all disabled
Nov 06 10:17:04  [57] "loginwindow" (0x57cf) set hot key operating mode to normal
```

per poi non riattivarsi sino al mattino successivo alle 10:17:04 del 6 novembre 2007 durante il sequestro del laptop.

Non vengono menzionate <u>alterazioni di date su un numero rilevante di file che sono avvenute sul computer in un periodo successivo alla sua acquisizione da parte delle forze di Polizia</u>, la alterazione ha riguardato numerosi file di filmati (tra cui lo stesso Naruto Episodio 101 di cui al punto 2.

******prego controllare le tempistiche del sequestro del pc poiche' non sono riuscito a disporre del verbale di sequestro del computer con indicazioni di data ed ora del sequestro che ricavo da indicazioni verbali di Raffaele Sollecito*******

Dalla relazione della Polizia Postale e dalla relativa presentazione in dibattimento, sorprendentemente non emergono indicazioni in merito al fatto che sia stata garantita l'inalterabilita' del laptop e dell'hard disk dal momento del sequestro (6 novembre ore 10:20 circa) sino alla acquisizione dei dati alla presenza dei periti (15 novembre 2007), concentrandosi sopratutto sulla garanzia della acquisizione dell'hash o impronta dell'hard disk, dai verbali non e' chiaro se l'hard disk sia stato estratto dal portatile in presenza dei periti o fosse gia' stato estratto in precedenza.

In realta' vi sono a disposizione dati che mostrano come il sequestro sia avvenuto con modalita' tecniche discutibili, e dimostrano con certezza e ripetibilita' come vi sia successivamente stata alterazione delle date di numerosi file, mentre il computer era gia' in possesso dell' autorita', in almeno un caso tali alterazioni hanno riguardato un file (Naruto Ep.101) che prova una importante interazione umana nel periodo di interesse.
Le fonti principali di riferimento per tali affermazioni sono tre:

- il file **windowserver.log** delle attivita' di tastiera;
- il file **system.log** che indica le attivita' di accensione spegnimento del sistema;
- i file **generati da ENCASE** (in possesso anche della Polizia Postale che pero' non menziona tali alterazioni poiche' esamina solo file nel periodo 1 novembre – 2 novembre).

Modalita' del sequestro:
dal file windowserver.log si ricava che il computer, si riattiva dallo standby alle 10:17:04, mentre era rimasto inattivo dalle 22:14:38 della sera precedente (interazione avvenuta mentre Raffaele Sollecito era trattenuto dalla Polizia).

```
Nov 05 22:14:38  [57] Hot key operating mode is now all disabled
Nov 06 10:17:04 57] "loginwindow" (0x57cf) set hot key operating mode to
normal
Nov 06 10:17:04 [57] Hot key operating mode is now normal
Nov 06 10:20:56  [57] "loginwindow" (0x57cf) set hot key operating mode to
all disabled
Nov 06 10:20:56  [57] Hot key operating mode is now all disabled
Nov 06 10:21:00  [57] "loginwindow" (0x57cf) set hot key operating mode to
normal
```

dalle tempistiche si ricava che non viene svolta alcuna attivita', visto che esattamente dopo 4 minuti (il tempo di attesa programmato) esso va in standby alle 10:20:56,; il portatile poi torna in modalita' attiva 4 secondi dopo, dal file system.log si ricava invece che esso inizia ad attivare la modalita' "hibernate" alle 10:20:57.

La modalita' "hibernate" consente di salvare la memoria e lo stato corrente del computer su disco, che poi effettua uno "spegnimento virtuale" risparmiando energia, tra gli specialistici di forensic e' dibattuta quale sia la modalita' migliore di acquisire un supporto. In molti casi si opta per lo "spegnimento brusco", quando non sia possibile o interessante fare analisi forense "live" sul supporto accesso. Lo "spegnimento brusco" puo' consistere, ad esempio per un portatile, nell'estrazione di alimentazione e batterie, esso consente di evitare che uno spegnimento regolare alteri date del computer. Nel caso in esame con ogni probabilita' lo schermo del laptop e' stato abbassato credendo cosi' di spegnere il computer che e' andato invece in modalita' "hibernate".

Dall'analisi di ENCASE risulta che vi sono modifiche di file sino alle 10:20:57.

Alterazioni dei dati successive al sequestro:

Alle 13:27:36 secondo il file *windowserver.log*, cioe' circa tre ore dopo il sequestro, la tastiera del sistema si riattiva,

Nov 06 13:27:36 [57] Hot key operating mode is now normal

tale registrazione e' l'ultima presente sul file windowserver.log, mentre il sistema resta ancora attivo per oltre 8 minuti sino alla 13:35:45 senza che la tastiera si disattivi, quindi con presumibili interazioni o programmi che mantengono la tastiera attiva.

Anche l'analisi del file *system.log* conferma che il sistema si e' risvegliato in quel momento.

Nov 6 13:27:36 MacBook-Pro kernel[0]: System Wake

Dopo 13 secondi il computer tenta poi di collegarsi alla rete wireless della abitazione di Raffaele Sollecito non trovando la rete, poiche' esso si trova presumibilmente in luogo diverso

```
Nov  6 13:27:49 MacBook-Pro
/System/Library/PrivateFrameworks/Apple80211.framework/Resource
s/airport: Could not find "BaseAirRaffa" on channel(s) 5 1 9
```

il computer inizia quindi a scandire, anch'esse non trovandole, le reti cui si collega abitualmente, tra cui quelle dell'Universita' "informatica" e "dip-open".

Non vi sono altre informazioni sul file *system.log* a testimonianza del fatto che successivamente il computer viene spento/si spegne improvvisamente, e' pero possibile ricavare dai file ENCASE che, nei successivi 8 minuti, mentre la tastiera e' ancora attiva, avvengono modifiche ai file che si protraggono sino alle 13:35:45. Tra gli altri risultano modificate le date dei seguenti file di tipo filmato:

	Last Accessed	File Created	Last Written
Naruto Ep. 100 - Un maestro per la vita .avi	6-nov-07 10.17.55	14-ott-07 19.05.47	6-nov-07 13.28.09
Naruto Ep. 103 - Attacco in mare aperto.avi	6-nov-07 10.18.22	14-ott-07 19.05.47	6-nov-07 13.28.09
Naruto Ep 102 - In Missione Nel Paese Del Tè.avi	6-nov-07 10.18.37	14-ott-07 19.05.47	6-nov-07 13.28.09
Naruto Ep. 101 - Dietro la maschera.avi	6-nov-07 10.18.38	14-ott-07 19.05.47	6-nov-07 13.28.09

in particolare si noti che tra essi e' presente il gia' nominato "Naruto Ep.101" ed episodi sia precedenti che successivi ad esso.

Purtroppo le date che tali file portavano al momento del sequestro sono state irrimediabilmente sovrascritte a causa della metodica utilizzata successivamente al sequestro, la cosa sorprendente e' che tali modifiche sono avvenute prima dell'intervento dei periti di parte.

E' possibile formulare varie ipotesi che spieghino tali modifiche in modo non doloso:

- imperizia ed ignoranza del funzionamento dello *hibernate* e di *aMule* che potrebbero avrebbero salvato i file automaticamente subito prima dell'hibernate e subito dopo una riaperturadel laptop modificandone le date;
- imperizia ed incauto esame dei file che qualcuno potrebbe aver tentato di aprire, o di aMule che potrebbe aver tentato di chiudere;
- chiusura fortuita del laptop appena riacceso per mancanza di carica alle batterie (teoria supportata dalle stringhe in tabella estratte da Encase che evidenziano il richiamo della funzione del sistema che indica l'imminente spegnimento del computer a seguito della batteria priva di carica), in tali casi il sistema, nel tentativo di effettuare uno "shutdown " o "chiusura regolare",

cerca di chiudere automaticamente tutte le applicazioni, che a loro volta chiudono i file aperti modificandone quindi le date, tali file potevano essere aperti in quanto scaricabili daltri utenti del peer-to-peer aMule.

Name	Last Accessed	Full Path
Resources	07-11-11 10:18	MacOS HD\System\Library\SystemConfiguration\PowerManagement.bundle\Contents\Resources
PowerManagement.bundle	07-11-11 10:18	MacOS HD\System\Library\SystemConfiguration\PowerManagement.bundle
com.apple.PowerManagement.plist	07-11-11 10:18	MacOS HD\Library\Preferences\SystemConfiguration\com.apple.PowerManagement.plist
com.apple.SystemPowerProfileDefaults.plist	07-11-11 10:18	MacOS HD\System\Library\SystemConfiguration\PowerManagement.bundle\Contents\Resources\com.apple.SystemPowerProfileDefaults.plist
Contents	07-11-11 10:18	MacOS HD\System\Library\SystemConfiguration\PowerManagement.bundle\Contents

E’ evidente come le modifiche delle date dei precedenti e di oltre 520 altri file (come testimoniato dal report ENCASE) impediscano di effettuare una analisi completa delle date originali, nel caso di “Naruto Ep.101” esse sono state fortunosamente recuperate tramite Spotlight, ma interazioni diverse potrebbero aver sovrascritto le date degli altri episodi del personaggio giapponese.

E’ inoltre quanto meno sorprendente l’utilizzo di metodiche che modificano le prove durante il sequestro, e della riaccensione del computer in assenza dei periti di parte.

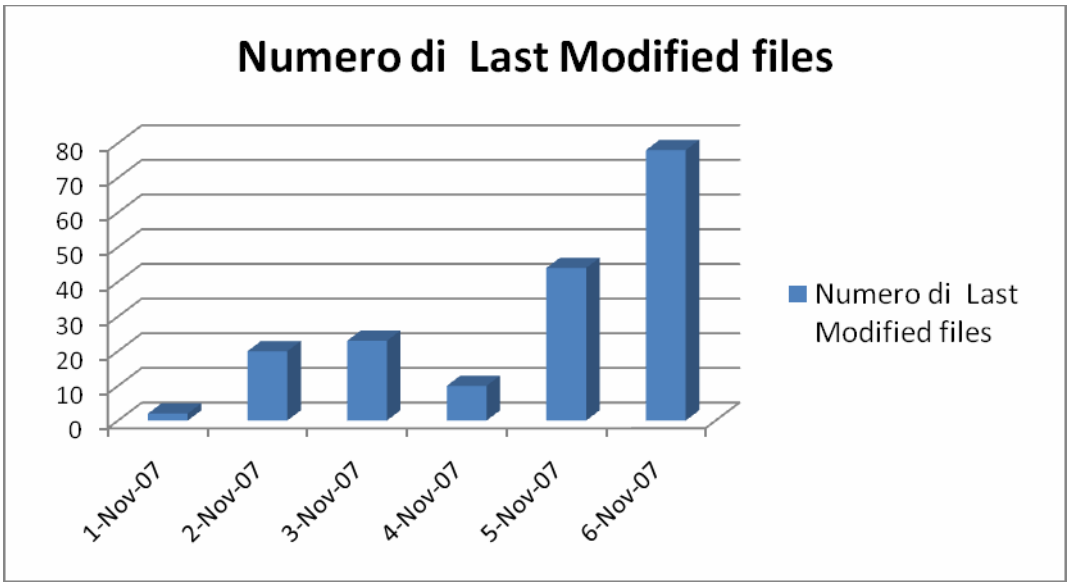
4 Conclusioni

Concludendo e' possibile evidenziare una serie di novità che hanno un impatto sulla formazione del giudizio del caso:

- la visione certa del file Naruto Episodio 101 in un orario mai rilevato prima 21:26, supporta l'ipotesi di una presenza almeno pari alla durata del film (20 minuti circa) quindi sino alle 21:46.
- lo spostamento certo del file "Amelie" dal Desktop alla cartella "Film visti", *supporta l'ipotesi di una continuita' della presenza durante la visione di Amelie.*
- la tastiera che resta attiva dalle 18:26:14 del 1 Novembre sino al crash di VLC, per disattivarsi alle Nov 02 05:36:18 e riattivarsi 5 minuti dopo circa con una interazione utente, *supporta l'ipotesi della continuita' di presenza/attivita'* (a meno di non immaginare che l'indagato rientri in casa esattamente cinque minuti dopo che il computer e' andato in crash).
- c'e' ragionevole dubbio che altre attivita' sul computer si siano svolte nel periodo dalle 21:26 le cui tracce sono state sovrascritte da attivita' ripetute (es. canzoni), o cancellate completamente poiche' virtuali (SAMBA).
- il ragionevole dubbio che tali attivita' coinvolgessero file musicali o film stante l'attivazione di FrontRow, del lettore di DVD, e stante la presenza in VLC di file non altrimenti reperibili del film "stardust", e stante la certezza che all'interno del PC e' stato rinvenuto un CD musicale del gruppo Blind Guardian.
- la certezza che c'e' stato un accesso al computer in assenza del proprietario la notte del 5 novembre 2007.
- la certezza che vi sono state alterazioni su oltre 520 file successivamente al sequestro del laptop che hanno cambiato le date di file significativi.

Ci preme ancora una volta sottolineare l'utilizzo semantico fuorviante del termine "tabulato" per informazioni come quelle di ENCASE che sono in forma tabellare, ma che riportano solo l'ultima modifica di un file e non la "sequenza" delle modifiche. Il fatto che attivita' ripetute provochino sovrapposizione delle date produce, come detto, il risultato paradossale, che utenti molto attivi, ma ripetitivi risultano avere pochi file modificati.

A tal proposito riportiamo a titolo di esemplificazione il seguente grafico a barre che riporta il numero di file "avi" o "mp3" modificati sul computer di Raffaele Sollecito, per ciascun giorno tra il 1 ed il 6 novembre 2007 il grafico e' basato sui dati reali riportati in ENCASE.



Il grafico potrebbe far dedurre ad un analista ingenuo che, avvicinandosi al 6 novembre 2007, si abbia un crescendo delle accessi ai file avi/mp3 e che non ve ne siano mai stati in passato.

In realta se si pensa al fatto che la data *Last Accesssed* viene sovrascritta, e si suppone ragionevolmente che l'utente abbia un certo grado di "riuso dei file multimediali" e' evidente che la maggior parte dei file sovrascritti debba essere recente. Mentre nel passato vi saranno pochi file modificati, in quanto essi avranno date quasi tutte completamente sovrascritte dagli usi successivi.

Per trovare tracce univoche e complete, una sorta di "tabulato telefonico", in un sistema a *sovrascrittura di date*, l'utente dovrebbe fare azioni sempre diverse e non ripetitive, come, ad esempio: non ascoltare due volte la stessa canzone, non rileggere

piu' volte lo stesso file di tesi, non controllare piu' volte il film che sta scaricando, non usare piu' volte lo stesso word processor etc., dovrebbe cioe' assumere in sostanza un comportamento opposto a quello della maggioranza parte degli utenti di computer.

Prof.Alfredo MILANI

La presente relazione si avvale dei fondamentali risultati di indagine e della preziosa collaborazione del dott. Antonio d'Ambrosio.

Utilizza inoltre suggerimenti e risultati del lavoro del dott.ing.Andrea Chiancone, dott.Paolo Bernardi, dott.Emanuele Florindi, dott.ssa Marina Latini e dott.ing.Valentino Santucci.