Ulteriori valutazioni sull'analisi del computer Apple MACBOOKPRO sequestrato a Raffaele Sollecito

Il sottoscritto dott. Antonio d'Ambrosio, consulente tecnico informatico della difesa di Sollecito Raffaele, successivamente al deposito della sentenza di primo grado e a fronte delle argomentazioni della Corte D'Assise di Perugia in merito all'utilizzazione o meno del computer sequestrato a Raffaele Sollecito la notte tra il 1° ed il 2 novembre 2007 , ha ulteriormente analizzato l'hard Disk del detto computer al fine di verificare se le conclusioni tecniche della Polizia Postale (integralmente recepite e fatte proprie dai primi Giudici) fossero o meno rispondenti ai dati fattuali emergenti.

All'uopo il sottoscritto si è anche avvalso della autorevole, consulenza di un docente di informatica dell'Università degli studi di Perugia, il Prof. Alfredo Milani, che ha parimenti , unitamente allo scrivente, analizzato dettagliatamente tutto il materiale informatico agli atti .

Dalla detta attenta e dettagliata analisi è emerso quanto segue:

L’analisi effettuata dalla Polizia Postale risulta metodologicamente inadeguata a reperire tutti i dati relativi alle interazioni con il computer di Raffaele Sollecito, ed inoltre fornisce conclusioni incomplete e non corrette sulla base dei dati raccolti.

Tale consulenza infatti risulta inficiata da forti limitazioni metodologiche, riassumibili in:

1) ***selezione preventiva di alcuni file attraverso il solo software ENCASE*** che opera utilizzando solo 3 date (tra le 5 presenti nei sistemi Mac), escludendo quindi in partenza la rilevazione di files che hanno modifiche nelle altre due date.

Per comprendere meglio quanto detto è importante precisare che nei sistemi operativi Unix, famiglia alla quale appartiene il sistema operativo Apple Mac OS X, i dati temporali (data ed ora) che annotano le principali operazioni effettuate sui file sono 5.

4 delle 5 informazioni vengono conservate in strutture dette inode del file system HFS+ (cioe’ del sistema di gestione della memoria disco), una in altre aree di memoria.

In particolare gli inode, mantengono le seguenti informazioni:

- **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 (un file di Word che viene modificato nel suo contenuto)

- **CHANGE**, l'ultima modifica all'inode
- **CREATE**, la data di creazione del file

Altre aree di memoria mantengono invece ulteriori informazioni, quali **ULTIMA APERTURA**, cioe' l'ora in cui il file e' stato aperto con uno strumento, quale ad esempio un "player multimediale".

E' importante notare che se si apre il file in lettura in modo diverso da quella appena indicato, ovvero non si usa un "player multimediale" ma bensì si usa la riga comando unix, la data **ULTIMA APERTURA** non viene modificata; per contro noteremo una variazione nel dato relativo all' **ACCESS.**

Il dato **ULTIMA APERTURA** e' visibile solo interrogando il file utilizzando l'interfaccia grafica del sistema operativo.

In fase di indagine ed analisi, abbiamo inoltre rilevato che vengono restituiti risultati attendibili se e solo se si fa uso di computer che utilizzano la stessa versione del Sistema Operativo installato sul disco sottoposto ad Analisi

2) mancata analisi delle informazioni al di fuori del periodo 01 Nov 2007 18:00 – 02 Nov 2007 8:00 **:** non si rilevano e ***non vengono considerate eventuali cause di alterazione o cancellazione delle informazioni*** intervenute in momenti successivi al periodo di interesse

3) mancata analisi dei log delle applicazioni del sistema Apple, *tra cui, in particolare i log che identificano i* ***periodi di attivazione/disattivazione della tastiera,*** *unici elementi probanti per documentare una* ***"interazione umana"***

4) ***mancata valutazione della attivita' di apertura del file "Naruto episodio 101", iniziata Giovedi' 01 Nov 2007 alle ore 21:26*** *; tale file ha una durata di oltre 20 minuti*

5) alterazioni di file rilevanti occorse quando il computer era stato sequestrato e gia' in possesso della autorita' inquirente e prima della acquisizione dei supporti alla presenza dei consulenti di parte. Tali alterazioni non vengono menzionate ne' prese in considerazione dalla consulenza della Polizia Postale .

Nel dettaglio :

A – MANCATA ANALISI DEI FILE DELLE APPLICAZIONI

A fronte della richiesta di analizzare le interazioni avvenute nell'arco temporale dalle 18.00 del 1 Novembre 2007 alle 8:00 del 2 Novembre nel computer Apple di Raffaele Sollecito, si sarebbe dovuto acquisire ed analizzare, in primis, il file **"windowsserver.log" che registra la cronistoria dei periodi in cui tastiera e mouse sono disattivati dal salvaschermo e successivamente riattivati da una interazione utente**. Questo assieme all'esame del file ***com.apple.screensaver.0016cba1b0b7.plist*** (che mostra il tempo per l'attivazione dello screen saver in 240 secondi cioe' 4 minuti di inattivita') avrebbe consentito di determinare preliminarmente periodi o "finestre" di *sicura assenza di interazioni* e *periodi in cui la tastiera e' attivata da una interazione utente*; le finestre risultano essere:

[inattiva 17:53:18-18:26:14][1 Nov]

[attivata 18:26:14-5.36:18][1-2 Nov]

[inattiva 5:36:18-5:41:34][2 Nov]

[attivata 5:41:34-5:45:52][1-2 Nov]

[inattiva 5:45:52-5:46:02][2 Nov]

[attivata 5:46:02-5:50:16][2 Nov]

[inattiva5:50:16-5:56:34][2 Nov]

[attiva 5:56:34-6:00:46][2 Nov]

[inattiva 6:00:46-6:06:38][2 Nov]

[attivata 6:06:38-6:14:37][2 Nov]

[inattiva 6:14:37-6:18:16][2 Nov]

[attivata 6:18:16-6:22:28][2 Nov]

[inattiva 6:22:28-12:18:24][2 Nov]

Si noti come nel periodo tra le 18:26 del 1 Nov e le 6:22 del 2 Nov i periodi in cui *assenza certa di interazione* sono al massimo di 6 minuti, mentre gli altri periodi sono di interazione/non interazione potenziale.

E' importante evidenziare inoltre che la data di ultima modifica (MODIFY) del file ***com.apple.screensaver.0016cba1b0b7.plist*** risale alle 22.30 del 26 aprile 2007 come illustrato dal comando Unix ***"stat –x":***

Input:
stat -x /Volumes/MacOS\ HD/Users/macbookpro/Library/Preferences/ByHost/com.apple.screensaver.0016cba1b0b7.plist

Output:
File: "/Volumes/MacOS HD/Users/macbookpro/Library/Preferences/ByHost/com.apple.screensaver.0016cba1b0b7.plist"
Size: 235
FileType: Regular File
Device: 14,6
Inode: 3065898
Links: 1
Access: Tue Nov 6 13:27:40 2007
Modify: Thu Apr 26 22:30:42 2007
Change: Tue May 22 00:53:26 2007

Questo risultato certifica che le impostazione dello screensaver non sono state più modificate dal giorno 26 aprile 2007 e per cui nell'intervallo precedentemete

considerato lo screensaver era attivo e sarebbe dovuto entrare in azione qualora non ci fosse più stata interazione col sistema.

Il file "windowserver.log" e il log del salvaschermo vengono invece completamente ignorati nella analisi della Polizia Postale .

Tale consulenza analizza infatti, attraverso il software ENCASE, i soli file creati, acceduti, modificati o cancellati nel periodo in oggetto, ignorando le informazioni provenienti dai file di log dove vengono registrate **le attivita' delle applicazioni**.

B – RISCONTRO EFFETTIVO DI ULTERIORI DATI/INFORMAZIONI UTILI NON RILEVATI DALLA POLIZIA POSTALE

Inoltre la ricerca di ulteriori date (es. "ultima apertura") con altri programmi, nella fattispecie "Spotlight" (funzione di ricerca avanza del sistema MAC OS X), viene limitata ai soli file individuati da Encase. In tal modo non e' stata reperita una attivita' di "ultima apertura" su alcuni file multimediale tra cui ***"Naruto episodio 101",*** probante con certezza una interazione umana ***iniziata Giovedi' 01 Nov 2007 alle ore 21:26 .***

Tale file ha una durata di oltre 20 minuti, ed e' stato reperito da una approfondita analisi dei supporti, successiva alla sentenza, estendendo la ricerca con "Spolight" a tutto il periodo successivo sino alla acquisizione del computer (vedi allegato XXX schermata spot light che vi invio domani).

C – ERRATA VALUTAZIONE DEI DATI AI FINI DELL'ACCERTAMENTO DI INTERAZIONE UMANA CON IL COMPUTER

Nella consulenza della Polizia Postale non viene mai evidenziata la *grave carenza probatoria* costituita dall'asserire una assenza di interazione, basandosi esclusivamente sulle date dei file.

E' infatti noto che le "data di ultima apertura" e "ultimo accesso" vengono sovrascritte dal sistema ogni qualvolta avviene una interazione con un file.

Una successiva, ed anche brevissima, interazione con un file, quale ad esempio un filmato, provoca l'automatica sovrascrittura, e dunque cancellazione, delle informazioni precedenti. Ad esempio, una breve apertura del film "Amelie" nei giorni successivi al 1 Novembre 2007 avrebbe provocato la assenza di qualsiasi riscontro di interazione nelle ore dalle 18:00 alle 21:10:32, momento dell'ultimo accesso al file "Amelie".

La conseguenza e' che la mancata presenza di file modificati nell'orario successivo alle 21:10,32 non puo' assolutamente essere ritenuta conclusiva dell'assenza di interazioni con il sistema. Infatti, svariate e numerose interazioni con il sistema, senza presenza di file e con date modificate nel periodo analizzato da Encase, sono possibili ed ipotizzabili per vari e diversi motivi:

- *visione di un film cancellato in data successiva* (e non reperito data la limitata sfera di indagine temporale utilizzata nella consulenza della Polizia Postale con Encase di cui sopra);

- *visione di un film riaperto in data successiva o file che ha subito una interazione successiva da parte di altro software (P2P)*. Si noti come un numero elevato di

filmati, tra cui “Naruto Episodio 101”, risultino avere le date modificate intorno alle 13:30 del 6 Novembre 2007, momento del sequestro.

Si può affermare con certezza che in fase di sequestro c’è stata una errata gestione del computer; i log del sistema infatti certificano un anomalo spegnimento della macchina sicuramente legato alla mancata fornitura di corrente che ha causato l’alterazione di molti files nei dati temporali;

- *ascolto di musica reiterato successivamente*: è pratica comune ascoltare la musica attraverso “playing list” cioe’ liste di canzoni preferite che si ripetono.

In questo caso l’ascolto successivo di una “lista” cancellera’ le tracce della precedente. Si noti che nelle interazioni documentate tra le 5:44 e 6:20 del mattino del 2 Nov, attraverso i log di iTunes (non esaminati nella perizia) risultano ascoltate proprio due sequenze di “playing list”, di cui una interrotta dopo un ciclo, che hanno cancellato i dati di ascolti precedenti delle stesse; inoltre i contatori di ascolto di alcune di tali canzoni risultano elevati (da 2 sino a 26 volte);

- *ascolto diretto di musica da CD-ROM :* questo tipo di ascolto non lascia tracce di modifiche ai file poiche’ le canzoni risiedono su un CD di sola lettura non modificabile. A questo proposito si noti che, come risulta dai verbali, dal computer di Raffaele Sollecito e’ stato estratto dalla Polizia Postale , un CD di un gruppo musicale.

Nella consulenza della Polizia Postale non viene invece evidenziata questa *incapacita’ di provare con certezza l’assenza di interazioni nei periodi in cui la*

tastiera e' attiva, incapacita' dovuta a possibili successive alterazioni delle informazioni.

Tanto è vero che si conclude (così consulenza Polizia Postale prot.1975/07 del 19 Novembre 2007): "*Nelle ore successive* ***non vi sono state operazioni*** *effettuate dall'utilizzatore sino alle 05:32:08*" ; e, ancora, si affermava nelle trasparenze proiettate in dibattimento, che nello stesso periodo "*non viene registrata interazione umana*", conferendo valore di certezza probatoria alla assenza di date di modifica nel periodo indicato, pur in presenza di una nutrita' attivita' nei momenti e nei giorni successivi (sic!).

D) SPECIFICO ERRORE D VALUTAZIONE IN MERITO ALL'ASSERITA INCERTEZZA DI INTERAZIONE UMANA CON IL COMPUTER ALMENO SINO ALLE 21:10,32.

Altresì , nella relazione del Prot.1975/07 del27 Nov 2007 a firma del Dirigente dott.Bartolozzi si sottolinea come l'ultima interazione con il file Amelie delle 21:10:32 del 1 Nov, fosse ***"non necessariamente di un utilizzatore" ,*** cioe' che la visione si potesse essere conclusa senza un utilizzatore presente.

Tra le ore 18.27 e le 21.10.32, quando il sistema ha interagito per l'ultima volta sul file in questione, è possibile ipotizzare un numero indefinito di ulteriori azioni: il film può essere stato visionato senza interruzioni dalla sigla di inizio ai titoli di coda, terminando cosi la visione del film alle ore 20:23 circa oppure possono essere intervenute sospensioni nella riproduzione dell'opera (ad esempio azionando il tasto di pausa di cui l'applicativo VLC è dotato), ma, con certezza è possibile asserire **che l'utilizzatore ha lanciato la visione del film in questione alle ore 18:27 e che c'e' stata un' ultima interazione del sistema, e non necessariamente di un utilizzatore, sullo stesso file AVI alle ore 21:10:32 dello stesso giorno.**

Di contro.

Dalla analisi del file di log **org.videolan.vc.plist** del visore multimediale VLC si rileva invece che al momento del termine della visione il file "Amelie" era collocato sul "Desktop", mentre al momento della data "ultimo accesso" esso risultava nella cartella **"MacOS HD/Utenti/macbookpro/Scrivania/aMule Downloads/Film visti":** ***e' quindi ricavabile con certezza che ad operare tale spostamento e' intervenuta sicuramente una azione dell'utente successiva alla visione del film***.

Poiche' l'analisi di tale file (riprodotto in allegato XXX) e' stata ignorata dalla Polizia Postale, la conclusione a cui è giunta quest'ultima, non puo' che essere parziale/errata .

E) ERRATA VALUTAZIONE DELLE INFORMAZIONI RELATIVE AL FILE "STARDUST"

La mancata analisi dei file di log di VLC, da parte della Polizia Postale, ha impedito ai giudici di disporre di informazioni corrette anche in ordine alla visione del film "Stardust"; infatti in sentenza si afferma :

"(omissis)Per es., e' stato spiegato, é in positivo riscontrato che nel pomeriggio del 1.11.07 si completava il download di file multimediali "Stardust" che l'utente aveva chiesto alla Rete con il sistema P2P. I file richiesti erano stati in numero di sei (quelli della serie Stardust), ***dove l'utente aveva visionato i tre*** per prima scaricati risultati evidentemente di buona fattura" (…)

"In astratto si può ipotizzare che la visione del file Stardust (e di altri ancora) scaricati dalla Rete e in condivisione con il mondo Internet sia stata lanciata anche dopo le ore 22.00 del 1.11.07. ***Di fatto non si saprà mai se ciò sia effettivamente avvenuto, in quanto il sistema Encase fornisce l'informazione limitata all'ultimo accesso,*** ove ***l'accesso in parola neppure è riferibile all'utilizzatore del computer*** quanto invece ad un quisque de populo dell'intero globo terrestre che con il sistema P2P richieda la condivisione dei file della apposita cartella del computer di Sollecito. ***Che una visione vi sia stata, oppure no, resta un dato dunque relegato nel mondo delle ipotesi***"

Al contrario, una semplice lettura del file **org.videolan.vc.plist** ha consentito di rilevare l'elenco degli ultimi 10 film visualizzati con VLC (vedi allegato XXXX che ti ho inviato in PDF ma cerco di frnirti in formato più facile e comprensibile). In tale elenco compare, ad ulteriore conferma, il gia' citato "Amelie", e risultano visualizzati successivamente ad esso, non gia' 3, ma ben 5 file del film Stardust; tali visualizzazioni inoltre sono riferibili *con certezza* ad azioni dell'utilizzatore

del computer e potenzialmente successive non gia' alle 22, ma alla visione di Amelie che era gia' terminata alle 21:10 (e verosimilmente al file "Naruto ep. 101") .

******

Sulla base di tutto quanto precede , il sottoscritto ritiene che gravi siano state le lacune riscontrabili nella consulenza della Polizia Postale,consulenza che ha conseguenzialmente informato il giudizio di primo grado e che è stata ritenuta prevalente su quella di parte.

In particolare risultano viziate le asserzioni dei primi Giudici in ordine alla :

-asserita impossibilita' di stabilire con certezza "se vi sia stata o no" la visione di Stardust, che risulta invece provata;

-asserita certezza di assenza di interazioni (secondo la consulenza della Polizia Postale che afferma con certezza che "non vi sono state interazioni") laddove invece nel medesimo periodo:

* la tastiera e' risultata attiva,

* le alterazioni successive intervenute per la normale attivita' possono aver modificato i dati;

- mancata analisi dei file di log, nonché incompleta ricerca dei file che sposterebbero l'interazione utente certa all'inizio della riproduzione del film "Naruto 101" alle 21:26.

In buona sostanza, periodi di *possibile interazione/non interazione*, sono stati presentati come periodi con *certezza di assenza di interazione*, mentre

interazioni avvenute con certezza documentata (es. fine filmato Amelie e suo spostamento in cartella “film visti” etc.) sono state presentate come *possibili ma non certe*, ed ancora piu’ rilevante e’ che l’insufficiente analisi ha mancato di rilevare interazioni certe oltre l’orario delle 21:10 (visione di Naruto 101 alle ore 21:26),vista l’importanza di valutare l’orario di presenza di Raffaele Sollecito nella propria abitazione .

****

Da ultimo non si puo’ non evidenziare un importante aspetto: quello relativo all’**alterazione dei dati,** alla luce di un grave fatto che puo’ aver compromesso la disponibilita’ di informazioni complete sul periodo.

Segnatamente, attraverso l’analisi del file **System.log** si sono ***rilevate attivita’ ed alterazioni che i dati sull’hard disk hanno subito il 6 Novembre 2007 dalle 13:27:36 alle 13:35:45, quindi tra il momento del sequestro del computer e il momento della acquisizione dell’hard disk alla presenza dei consulenti*** . E’, infatti, inconfutabilmente provata la alterazione delle date di numerosi file multimediali tra cui lo stesso “Naruto 101” (ultimo accesso 6 Nov 2007 ore 10:18:38 - ultima modifica 6 Nov 2007 ore 13:28:09 , vedi elenco allegato date di modifica dei file ***** e verbale sequestro che fissa l’orario dello stesso*****). Ancora una volta una analisi estesa a tutto il periodo successivo ai fatti, ed ai log di sistema avrebbe consentito di rilevare tali alterazioni ai consulenti della Polizia Postale .

E’ dunque di primaria importanza chiarire quali attivita’ siano intervenute successivamente al momento del sequestro del computer, quando esso era in consegna agli inquirenti, ma non ancora acquisito alla presenza dei consulenti di parte .

Per tutto quanto sopra espresso si ritiene assolutamente necessaria una rivalutazione di tutti i risultati espressi dalla Polizia Postale, e recepiti integralmente dai Giudici di primo grado, anche mediante la nomina di un perito da parte della Ecc.ma Corte D’Assise D’Appello che attraverso l’analisi dell’Hard Disk nonche’, e segnatamente, mediante la materiale apertura del computer sequestrato a Sollecito Raffaele analizzi nel dettaglio tutti gli aspetti e gli evidenti errori sopra indicati e documentalmente dimostrati con i sottoelecanti allegati .

Brescia , 30 ottobre 2010

Dott. Antonio d’Ambrosio