# POLIZIA DI STATO
COMPARTIMENTO POLIZIA POSTALE E DELLE COMUNICAZIONI PER L'UMBRIA
Via Mario Angeloni 72 - Perugia
Tel. 075/5001703 - 5011967 Fax.075/5000655
poltel.pg@poliziadistato.it
*Settore Operativo*


## PROC. PEN. 9066/07 mod. 21
## APPUNTO PER IL SOSTITUTO PROCURATORE DELLA REPUBBLICA DOTT. MIGNINI

In ordine al contro esame redatto dai tecnici della difesa di SOLLECITO Raffaele, si enunciano le osservazioni che il personale che ha condotto l'attività di indagine sul computer e sui relativi file di log ritiene utili per una corretta valutazione dei fatti da parte dell'A.G. procedente.

### Visione del film "Il meraviglioso mondo di Amelie"

Il file dei *last accessed* identificato dal progressivo di cui al nr.95 dell'allegato nr. 3 dell'analisi prodotta da questo Compartimento, è relativo al file avente estensione *.avi* denominato "***[DivX - ITA] - Il Favoloso Mondo Di Amelie.avi***", identificato dal percorso *HITACHI \HITACHI\1 Merged_Untitled\MacOS HD\Users\ macbookpro\ Desktop\aMule Downloads\Film visti\[DivX - ITA] - Il Favoloso Mondo Di Amelie.avi*, attinente un'opera cinematografica; in ordine a tale file il software ENCASE rileva che l'ultimo accesso allo stesso è avvenuto alle ore 21:10:32 del 01/11/2007.

A tal proposito è bene sottolineare che il software Encase, nella colonna delle proprietà di un file rinvenuto all'interno dell'hard disk, indica il *last accessed* collocando temporalmente il momento in cui su quel file è avvenuta una qualsivoglia attività per l'ultima volta; detta attività può consistere in una quantità indefinita di azioni quali, per citare le parole del manuale del software in questione, il trascinamento in punti diversi del desktop o in cartelle diverse, il fatto che sia stato semplicemente cliccato con il tasto destro del mouse quando il puntatore è sopra di esso o esaminato da un programma. Ognuna di queste attività modificherà la data e l'ora di ultimo accesso al file in questione.

Al fine di stabilire l'ora in cui l'utilizzatore del computer oggetto d'analisi abbia interagito sul predetto file, e quindi collocare temporalmente l'inizio e la fine della predetta attività, gli scriventi hanno creato un clone dell'hard-disk dell'indagato, e, dopo averlo usato per avviare un notebook con architettura identica a quella del computer in sequestro, inserendo la password "*palmiottosollecito*" hanno constatato, visionando quello che i consulenti della difesa chiamano "stamping digitale" del file, che il film in questione è stato aperto alle ore 18:27 del 01/11/2007 e che l'applicazione ad esso associata per default è il software VLC (quindi, a meno che non si decida di far aprire il file da altre applicazioni, la sua riproduzione avviene mediante VLC). La riprova di quanto asserito è a pagina 1, punto 8 del report "*Files ultimo accesso*", allegato all'analisi del 19.11 u.s. in cui si evidenzia che alle ore 18.27.15 è stato attivato l'applicativo VLC agendo sull'icona "*vlc.icns"* identificata dal percorso HITACHI \HITACHI\1 Merged_Untitled\MacOS HD\Applications \VLC.app\Contents\Resources\vlc.icns .-

Si evidenzia che la prova in questione è stata, pertanto, condotta sul clone dell'hard disk in sequestro (e non su un altro computer con identiche caratteristiche) e con lo stesso file in esame (e non soltanto su un file con medesima estensione .avi come hanno ritenuto di fare i c.t.p.).

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.**

## L'inesistente attività di navigazione sul web

Gli scriventi affermano che non vi è traccia di interazione umana sul Computer del SOLLECITO dalle ore 21:10:32 del 01/11/2007, quando si interagisce per l'ultima volta sul file avi citato nel punto precedente, sino alle ore 05:32:08, quando il sistema registra da prima alcuni crash del programma VLC, e pochi minuti dopo la riproduzione di file musicali.

Nel lasso di tempo compreso tra le ore 21:10:32 e le ore 05:32:08 , gli unici file creati (*File Created*), scritti l'ultima volta (*last Written*) di cui Encase ha dato responso, sono nr.04 file attestati nelle cache del browser di navigazione Firefox e nr.02 file generati dal Sistema Operativo; nessun file è stato trovato in quelli di ultimo accesso (*Last Accessed*) tra le ore 21:10:32 e le 05:32:08 .

Giova precisare che, come già evidenziato, si tratta di file generati in automatico dal sistema e in particolare dal browser di navigazione FIREFOX di Mozilla all'interno della sua cache: ciò che caratterizza detti file è che risultano generati ad intervalli regolari (esattamente a distanza di 30min. l'uno dall'altro). Qualora vi fosse stata navigazione, all'interno della cache sarebbero stati rinvenuti anche riferimenti a indirizzi web (www.nomedominio.estensione, ad esempio www.poliziadistato.it), con i relativi componenti quali foto, testi o altri elementi.

Nella relazione prodotta dalla difesa si afferma, poi, che la cadenza fra un aggiornamento e l'altro del safe browsing (un applicativo integrato nel browser Mozilla Firefox) si interrompe più volte, a testimonianza del fatto che sia intervenuta un'interruzione nel collegamento internet o la chiusura del browser predetto: ebbene detto assunto risulta, a parere degli scriventi, confutato da quanto esposto nei due punti seguenti:

1) Nei file di log forniti da FASTWEB, il traffico verso Google (ovvero verso l'url http://sb.google.com/safebrowsing/update?client=api... che identifica la ricerca di aggiornamenti di safe browsing) risulta essere regolarmente generato con cadenza di 30 minuti senza soluzione di continuità, a dimostrazione inconfutabile che il PC, oltre ad essere stato sempre connesso alla rete, ha mantenuto sempre aperto il browser;
2) L'interruzione della continuità degli aggiornamenti in parola è riscontrabile soltanto nei dati relativi alla cache di FIREFOX poiché, trattandosi di componenti per la funzionalità dell'applicazione web-browser, non vengono riscritti sulla cache se già scaricati al precedente aggiornamento: in buona sostanza sulla cache si potrà notare la presenza di un file solo se il sistema ha trovato un aggiornamento di cui la macchina non era dotata; qualora, invece, non c'è nulla di nuovo, risulterà il traffico generato tra il computer e il server (ed infatti si ha traccia di traffico nei file di log di Fastweb), ma, non avendo nuovi dati da aggiungere, nulla verrà scritto sulla memoria del computer, e in particolare sulla cache di Firefox.

**Si rileva, poi, come la difesa non abbia evidenziato la presenza di alcun file, attinente la navigazione nel web, creato, modificato o cancellato nel sistema tra le ore 21:10 del giorno 01/11/2007 e le ore 05:32 del 02/11/2007.**

A tal proposito i c.t.p. asserivano che "la combinazione del sistema operativo Mac OS x 10.8.4 e il programma usato per navigare in internet FIREFOX di Mozilla, hanno creato per il software un filtro tale da non rendere accessibili tutte le informazioni utili all'analisi in oggetto", rafforzando tale assunto con l'attribuzione, per uno di essi, della qualifica di "rappresentante per l'Italia della casa Guidance Software, produttrice di Encase, e che in contatto con la sede ha ricevuto istruzioni in merito all'approfondimento di problematiche Mac".

Utilizzando la medesima versione del software di analisi forense (Encase 6.8, aggiornato subito dopo le operazioni di acquisizione eseguite con la 6.7) gli operanti riuscivano, tuttavia, a generare la internet history (ossia un report contenente le tracce di navigazione presenti nel computer sequestrato collocate nel tempo), il cui esame non evidenziava alcuna navigazione (vd. *Allegato 1* consistente in un estratto di tale report)

## L'analisi dei file di log Fastweb

Come già accennato, al fine di verificare la presenza di tracce di navigazione è stata ricavata la History di navigazione tramite apposita applicazione prevista dal software ENCASE, dalla quale si evince che non vi sono tracce di navigazione nell'arco di tempo oggetto dell'indagine che facciano supporre la presenza di una persona davanti al notebook.

A conferma di quanto appurato mediante ENCASE, si è poi proceduto all'analisi dei file di log forniti dal gestore di telefonia FASTWEB tentando di individuare tutti gli indirizzi IP relativi a sistemi in grado di erogare pagine web (porta 80 e 443), posta elettronica (25 e 110) porte relative a servizi di comunicazione interpersonale quali Chat, e telefonia via internet.

La ricerca dava esito negativo in quanto i soli risultati presenti erano relativi alla porta 80, ma, vista l'esiguità dei byte scambiati e la loro già menzionata regolare periodicità, tale traffico era da attribuire esclusivamente ad attività di aggiornamenti funzionali e/o informativi.

**Pertanto prima di affermare che non vi fosse stata attività in internet riconducibile a navigazione, è stata sempre cercata una conferma ad ogni dato emerso dall'analisi effettuata mediante ENCASE.**

## 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***.

Giova, infine, sottolineare che i sistemi utilizzati dai c.t.p. hanno loro consentito di identificare, quale sistema operativo istallato sul MacBook Pro di SOLLECITO Raffaele, il sistema operativo Mac OS X **10.8.4**, rilasciato da Apple: ebbene detta versione del sistema operativo non esiste ancora, poiché la casa costruttrice ha rilasciato, quale ultima versione del Mac OS X la 10.5 (denominata "Leopard").

In realtà la versione installata sul computer in sequestro è la 10.4.10, come si evince dal report generato dallo script "*initialize case*" (vd. Allegato 2).

## CONCLUSIONE

**Alla luce di quanto sopra esposto si ribadiscono le conclusioni cui questo Ufficio era pervenuto in data 19.11 e cioè che tra le ore 21.10 del 01.11.2007 e le ore 05.32 del 02.11.2007 non è stata rinvenuta traccia di interazione umana sul computer sequestrato a Raffaele SOLLECITO.**

Si allega alla presente anche un filmato realizzato unitamente a personale del locale Gabinetto di Polizia Scientifica, in cui sono documentate le operazioni tecniche che hanno permesso di ribadire che il sistema Mac OS X dà informazioni inerenti l'ultima apertura di un file (nel caso in esame l'avvio della riproduzione del film) mentre il software Encase del momento dell'ultima interazione del sistema sul file stesso (nel caso di specie avvenuto alle 21.10 del 01.11.2007).