Expert Report on Raffaele Sollecito's computer

Purpose

The purpose of the present report is that of verifying and evaluating the character of the activities performed on Raffaele Sollecito's laptop computer MacBook Pro in the time span from 6 pm on November 1, 2007 to 8 am on November 2, 2007 through a) direct repeatable examination of a true copy of said computer's hard disk and b) in light of the documentation produced by the Postal Police and exhibited at trial.

Said MacBook Pro laptop turned out to be powered on in Raffaele Sollecito's dwelling, connected to the Internet through a wireless router, and connected to another laptop of the Asus brand, which was performing activities of file downloading from Internet. It has not been possible to examine the hard disk of the second laptop (an Hitachi hard disk), it having proved to be unusable.

1.Methodological foreword: dating and digital timestamps.

It is very important to clarify that computers, for reasons connected to their regular workings, record on the hard disk, and on other type of memories, volatile (RAM) and not (flash memories, EPROM), large quantities of *timestamps* of various kinds, usually they have the structure of a pair (*date, time*)[1] associated to a group of data and/or an event.

Some of these *dates* are directly managed from that part of the operating system called *file system* and stored in dedicated data structures (as for instance the *dates* concerning file modifications), other *dates* are instead managed by applications coming with the operating system (as for instance the dates related to the activation/deactivation of the screensaver),or they are independently managed by various applications present on the computer (for instance the date of the playing of a song, can be stored in a different way according to which program or *player* is used to listen to it).

Since many different applications independently update the *dates*, their updating is not always coherent, particularly if the event to be recorded is

[1] Hereafter for brevity we will call *date* information made of *date (day, month, year)* and *time of the day (hour, minute, time zone)*

originated by a different program, albeit correctly used (for instance, restoring a compressed, or *zipped*, file, after the restore the file can display a date earlier than that of the computer's purchase!).

1.1Storage media for dates and formats of the dates

It is also important to clarify *where* the dates at issue are stored and in which *format*. For what concerns *dates written by the operating system*, they are stored in special data structures on the disk, called *inodes* in Unix-derived systems like MacOS, whose *format* varies according to the version of the system at issue (for instance a MacOS system may record the same information in different ways depending on the version).

For what concerns *dates written by other applications*, they usually are stored inside *ordinary files* that the applications handle in a special way, for instance to register in them the performed activities (a media player usually records how many times a song has been reproduced till the end, or the last date when it was skipped with the *skip* function, or the starting/shutting down of the application).

1.2 How activities are detected and recorded

Generally the execution of an activity can be detected through:

- the ***explicit recording of a sequence of dates/timestamps***, that is of sequences of dates concerning operations or *events* linked to activities, such sequences are stored in specific files called ***log files*** (for instance keyboard logs, plist, XML, net logs, etc.)
- ***change/overwriting of a single date/timestamp***, as for instance the ***date of a file*** involved in a given activity
- the occurrence of ***later events***[2] demonstrating a previously occurring activity (for instance the crash of an application demonstrates that it was previously running)
- besides the previous hypotheses, to correctly detect an activity, one also has to prove ***the absence of later alterations*** of the timestamps and the correct working of the date recording system.

[2] *Activities showing themselves through later events.* An activity not recorded by the system in a given time span can produce its effects at a later stage, revealing itself through an event recorded in a log or producing a modification of dates. For instance the crash of an application proves that said application was running until the time of the crash (see below for the VLC crash).

It is very important to differentiate between the two main ***ways of recording and storing the dates*** of events in IT systems:

- ***writing of sequences of dates***
- ***overwriting of a date***

In the **first case** a list of dates/events concerning a given resource is recorded.An example of this kind [of recording] is the *keyboard activation/deactivation sequence* stored in MacOs systems, that is the sequence of dates when the keyboard was activated/deactivated. Another example are the log files concerning web communications.
In the **second case** instead there is available enough space for just a single timestamp and hence only the last occurrence of an event is stored, an example of this kind [of recording] is the *date of last change of a file*. If a file is modified multiple times, only the last modification [change] occurred will remain stored in the related *date*.
There are also **halfway situations**, in which a limited sequence is available for storing (for instance some word processors, and some media players like VLC, maintain in a menu the list of the *last five*[3] *recently opened documents*).

The two typologies of event recording and storing, **sequence writing** or **overwriting** have critical consequences when one tries to prove the presence or the absence of activity in a given time frame.

1.2.1 Sequences of dates, or log files, or "records"

In the event of a storage typology as **sequence of dates** or as **log files**, unless there is tampering with the media, the presence of a timestamp is strong proof of presence, as well as of absence of activity linked to said timestamp. That is, one is in a situation akin to that of the so called phone **records**, where date and length of conversations are recorded by carriers. If in a given time interval there is no call, it is possible to conclude with reasonable certainty that no call took place, unless there has been tampering with the media, or the recording devices had a failure.

1.2.2 Date overwriting

[3] Usually this number is a customizable parameter.

In the event instead of a **date overwriting**, as one has for the dates of modification or opening of a file, what one has is on the one hand the **presence** of a timestamp at a given time is reasonably evidentiary of an event linked to it, but one also has on the other hand that the absence of timestamps in a given time span **is absolutely not conclusive** about the absence of activity, **on the contrary, almost paradoxically, such timestamps will be all the more absent if there has been an intense activity on the resource considered**.

For instance, if a user modifies the same document with a word processor many times for a month, hypothetically a graduation thesis on which he works every day, the file will have a *last modification* date corresponding to the last day of work in the month. *Last modification* dates recorded by the system at the end of each daily working session will be overwritten, hence becoming irremediably lost. It is hence manifest the impossibility of basing the evidence of "absence of activity" on the document itself, on the fact that there are *no* last modification *dates* inside the considered time interval. In other words whatever activity at a later time may delete any trace of interaction on a given file. From a practical standpoint, date overwriting may happen because of **explicit actions by the user**, for instance playing repeatedly a song in a playing list will leave as trace of last access and last opening the one related to the last time the song has been listened to (or a movie watched), deleting any trace of previous listenings/viewings.

Date overwriting may also happen in an **implicit/automatic way**, for instance the downloading of a file by remote users through [a] *peer-to-peer* [application] may modify the information about access to files made by the local user, in other words the remote users have access to the local computer and read a file, therefore modifying the date of last access.

1.3 Alteration of timestamps through overwriting of later dates

Any activity on a file recorded with the overwriting technique may therefore be masked/deleted by later openings or runnings of that file, the new timestamps **overwriting the old ones, which cannot be detected anymore (not even by tools like ENCASE)**.

Hence not detecting the opening of a file in a given time span does not necessarily mean that there has been no activity, because it may have been overwritten for many reasons at a later time.

It is then evident that the longer the time passed before the acquisition of a media which went on working and being used, the bigger the probability that individual timestamps, indicating periodical, repeated or automatic events, are progressively overwritten, deleting in this way the timestamps related to earlier times.

Recording by sequence of dates **(log file or "reccord")**	***Recording by overwriting of dates*** **(acces date, modification date, etc.)**
Date Event	**Date Event**
01/10/2010 h:15:00 view film1 01/10/2010 h:15:20 viewi film2 01/10/2010 h:15:50 write text1 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 view film2 02/10/2010 h:17:00 write text1 03/10/2010 h:15:10 write text1 03/10/2010 h:17:00 play song3 04/10/2010 h.16:30 write text1 06/10/2010 h:16:00 write text1 06/10/2010 h:17:00 play song3	01/10/2010 h:15:00 view film1 01/10/2010 h:15:20 view film2 01/10/2010 h:15:50 write text1 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 view film2 02/10/2010 h:17:00 write text1 03/10/2010 h:15:10 write text1 03/10/2010 h:17:00 play song3 04/10/2010 h.16:30 write text1 06/10/2010 h:16:00 write text1 06/10/2010 h:17:00 play song3
The two tables show the different ways of recording the same sequence of events. Please notice that a "naive" analysis of the recordings by "overwriting of dates", shown on the right, the multiple repeated activities on preferred songs *song1, song2, song3, song4* on 01/10/2010 are completely lost, while on the days 03/10/2010 and 04/10/2010 there even seems to be no activitv at all.	

Fig.1 Comparison and limits of recording by "overwriting of dates"

Figure 1 shows with a very simple example how recordings made by "date overwriting" may deceive an unsophisticated analyst, who reads only the dates written in bold on the right, deducing for instance that there has been no activity in the afternoon of 10/01/2010 after 3 pm or that there has been no activity during days 3 and 4, or that the file *text1* has been written only on 10/06/2010. Paradoxically the most repeated and recurring activities are those which are less reliably recorded, as for instance the playing of "preferred songs" *song1, song2, song3 and song4.*

It is therefore necessary to integrate the analysis of overwritten dates(e.g. creation date, last access, last opening) with that of various *log files* produced by the system (crash log, keyboard monitoring log, system log, applications' logs, etc.) to obtain a complete picture of the activities taking or not taking place.

It is moreover necessary to verify that in the time interval going from the one of interest to the acquisition of the hard disk *there has been no activity that may have compromised and/or altered the timestamps or the log files related to the period of interest going from 6 pm on November 1, 2007 to 8 am on November 2, 2007*. It is pointed out, incidentally, that the computer at issue remained active until November 6, 2007.

Alterations may have been caused, for instance, by playing again music or video files, hence overwriting the dates, or they may have been caused by the resetting or deleting of log files.

3. Main critical points of the Postal Police expert report.

The first grade ruling based its considerations concerning the interactions present on Raffaele Sollecito's MacBook Pro computer on the expert report authored by the Postal Police.

Such technical activity, *cannot however be considered as methodologically correct*, since it has produced *highly incomplete results* and *conclusions not justified by the available data*, the most critical points are the following ones:

1. The Postal Police analysis is based on the **preventive selection of some files through the ENCASE software**, which operates by using only 3 system dates (among the 5 present on Mac systems), and on a **further in-depth analysis of the information contained in some of the files obtained through that selection with the use of Spotlight and or Finder**; that is the graphic interface of the operating system (see, for instance, the report on the *Amélie* movie).
2. It does not mention the **opening of the multimedia file "Naruto episode 101", which happened on Thursday November 1, 2007 at 9.26 pm .**
3. In the report **the application logs (for instance VLC) and the keyboard log are neglected**: such logs indicate the start and the stop of the activity on the computer.
4. It does not mention an **activity of song playing occurring between 5.41 am and 6.38 am on the morning of November 2, 2007** .

5. **Information outside the November 1, 6 pm - November 2, 8 am time interval are not analysed**, hence the police analysis does not discuss nor detects possible causes of alteration/overwriting of the information related to the period of interest and likewise it does not consider later events caused by actions occurred in the period of interest.
6. In the conclusions reached a **strongly erroneous methodological hypothesis** is used, namely *it is assumed that the absence of timestamps in a given time interval is evidence of the absence of activity on the computer* (see also paragraph 1), omitting to point out that any further activity on a given file may alter its date (the computer at issue has been used and has remained always powered on for as much as 4 days after the period of interest), or that there are activities which do not leave any trace (for instance reading a CD/DVD), while inside the laptop has been found one of the many music CDs owned by Raffaele Sollecito.
7. It does not mention the use of the **SAMBA application**, through which one could have network access (virtual disk) from the MacBook to the hard disk of the other Raffaele Sollecito's laptop (the Acer one), which was found unserviceable for analysis.
8. It does not mention **a sure access activity to the computer** owned by Raffaele Sollecito, the browsing of a web page, **occurred on November 5, 2007, while he was under interrogation**.
9. It is not mentioned **the alteration of dates on a sizable number of files occurred on said computer at a time following its acquisition by the judicial authority**, the alteration having concerned many video files (including the Naruto Episode 101 already mentioned at point 2).

In the forthcoming paragraphs these critical points will be examined in detail, grouping the analysis by similar [literally "omogeneous"] points.

1. Analysys limited just to the three dates considered by Encase

2. The opening of the multimedia file "Naruto Episode 101" occurred on Thursday November 1, 2007 at 9.26 pm

---

It is obvious that if one follows the method limiting the analysis of the dates to those considered by Encase, if a file is not selected in the initial selection phase (that is if the three dates do not fall in the time interval of interest), it is excluded from the results of the subsequent limited research, even if it has one of the other two dates (out of five[4]) inside the period of interest.

This incorrect methodology produced highly incomplete results, indeed, as a result of further in-depth analysis made by the defense consultant, after the first grade ruling, using for the first time an operating system of the same *version* and *build*[5] as the one used by Raffaele Sollecito, namely Mac OS X **10.4.10 (Build 8R2232)**, it has been possible to obtain the correct visualization of the data, acquiring in this way information of fundamental importance to prove activity [on the PC in the period of interest].

---

[4] In the Mac OS X systems time information (date and time) marking the principal operations made on files, are in part stored on the HFS+ file system in structures called *inodes* and in part in other storage areas.
Specifically, inodes store:
ACCESS, the last read or write access made on the file, for instance to copy it
MODIFY, the last modification (write) made on the file's content
CHANGE, the last modification to the inode
CREATE, the creation date.
Other storage areas store instead further information on the use of the file, different from the previous ones, as the date of LAST OPENING, that is the time when the file has been opened with a tool, for instance a player. It must be noticed that if the file is opened for reading in a different way (for instance by the Unix command line), the LAST OPENING date is not modified. The LAST OPENING date ia accessible through the operating system's graphic interface tool *Spotlight*, while it is hidden to the command line. Information about files are available through *specific software* (like ENCASE), through *speficic commands* (like *stat*) or also through the *graphic interface tool Spotlight*, which can be used by whatever user. If the information is read with a version of the operating system different from the one used to write it, information may appear as different from the correct one, or be totally unreadable. This is particularly true for the extended data or for data managed by applications, like the LAST OPENING date. It is specifically pointed out that the ACCESS date refers to the closing of a song or a movie, while the LAST OPENING date refers to the start of the listening/viewing.
It must moreover be remembered that, as already said, besides these dates, some programs keep information on the activity performed in specific files in XML format, called *plist* on MacOS systems, or in dedicated log files.

[5] Operating System
Operating Systems are continuously updated, the one used by Raffaele Sollecito was verion 10.4.10 (Build 8R2232) of Mac OS X, code name Tiger. Of the Tiger Mac OS X 12 versions have been produced (from 10.4, 10.4.1 to 14.4.11), for a sum total of 29 different "builds" (a "build" is a recompilation of the version with minor differences). The result quoted concerning the Naruto Episode 101 movie has been obtained by analyzing the hard disk with the same exact version of the operating system present in Raffaele Sollecito's Mac OS X.

One reads instead in the State Police report dated November 19, 2007, protocol number 1975/207, concerning the analysis of the seized asset and addressed to the Office of the Prosecution of Perugia that

ANALYSIS OF THE DATA

The quest for interactivity on the pc has been performed by extrapolating all the files created, written, modified, deleted and for which there had been a last access, between 6 pm on 11/01/2007 and 8 am on November 2

all the files which could have modified such information, since access/modification/writing occur with date overwriting, have hence been explicitly excluded by the analysis.

There is detected only an activity until 9.10.32 pm [on November 1] related to the Amélie movie

From the analysis it was possible to state that there was interactivity on the machine in the late afternoon of November 1, when, between 6.27.15 pm and 9.10.32 pm the movie Amélie was watched with the VLC software.

such information is said to have been also verified through an "Apple laptop with technical characteristics **similar** to those of [the pc belonging to] the person under investigation"

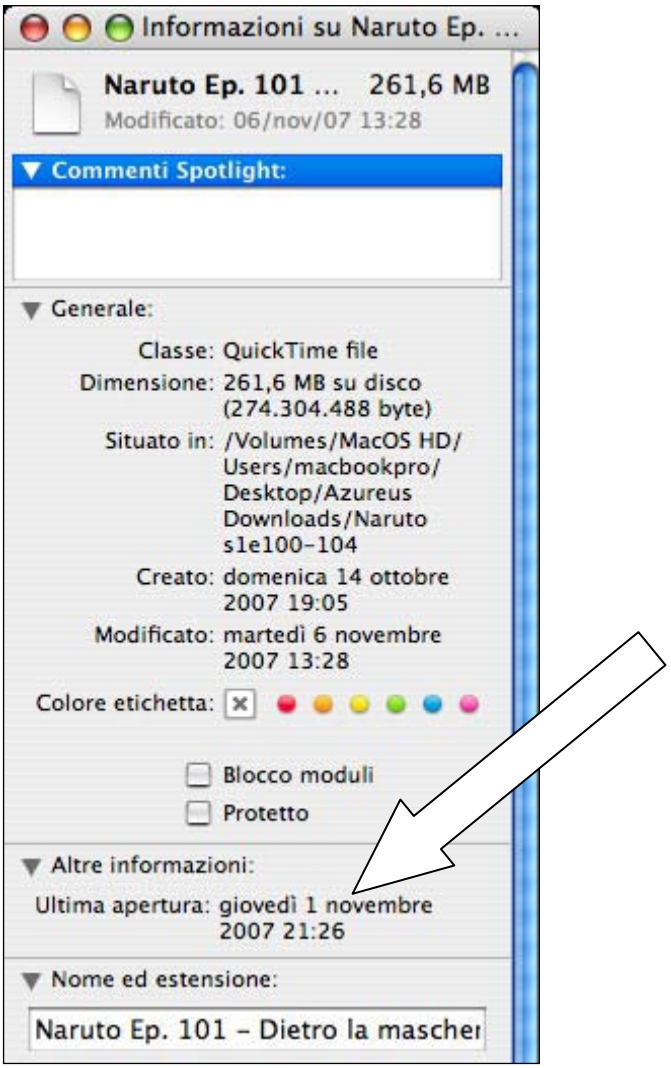
In confirmation of what is written above the hard disk of the peson under investigation has been restored on a suitable magnetic storage medium through the "Restore Drive" feature of Encase, with said storage medium an Apple laptop with technical characteristics similar to those of [the pc belonging to] the person of investigation was started. Once started the pc the video file named "Il favoloso mondo di Amelie" ["Amélie"], identified by the path HITACHI\1 Merged_Untitled\MacOS HD\Users\macbookpro\Desktop\aMuleDownloads\Film Visti\[DivX - ITA] - Il Favoloso Mondo di Amelie.avi, has been looked for. From here [once found the file], by controlling the properties of the file, it was possible to verify that the last opening of the same dated indeed 6.27 pm on 11/01/2007 and had been indeed made through the VLC program (see attachment number 03).

It is important to notice that the appealed ruling [Massei], grounding its conclusions on this analysis, set at **9.10.32 pm** the last operation made by Raffaele Sollecito on the day of November 1, 2007.

In truth in Raffaele Sollecito's hard disk there is at least a file, "Naruto ep. 101.avi", which is excluded from the analysis because its dates of modification are outside the limited time interval in which the Postal Police performed the search, the file generated by Encase showing

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

Performing instead a search with *Spotlight* in the Mac OS X 10.4.10 version, said file **"Naruto ep 101.avi"** shows as last opening date Thursday November 1, 2007 at **9.26 pm** (that is inside the time interval considered by the Postal Police: 6 pm on November 1, 2007 - 8 am on November 2, 2007).
See the following Spotlight's window:



Such file was not found at all by the Postal Police, which also added:

> *From the analysis it was possible to state that there was interactivity on the machine in the late afternoon of November 1, when, between 6.27.15 pm and 9.10.32 pm the movie Amélie was watched with the VLC software.*
>
> *[omitted]*
>
> *In the following hours there have been no operations made by the user until 5.32.08 am, when the VLC program was run to play some audio files.*

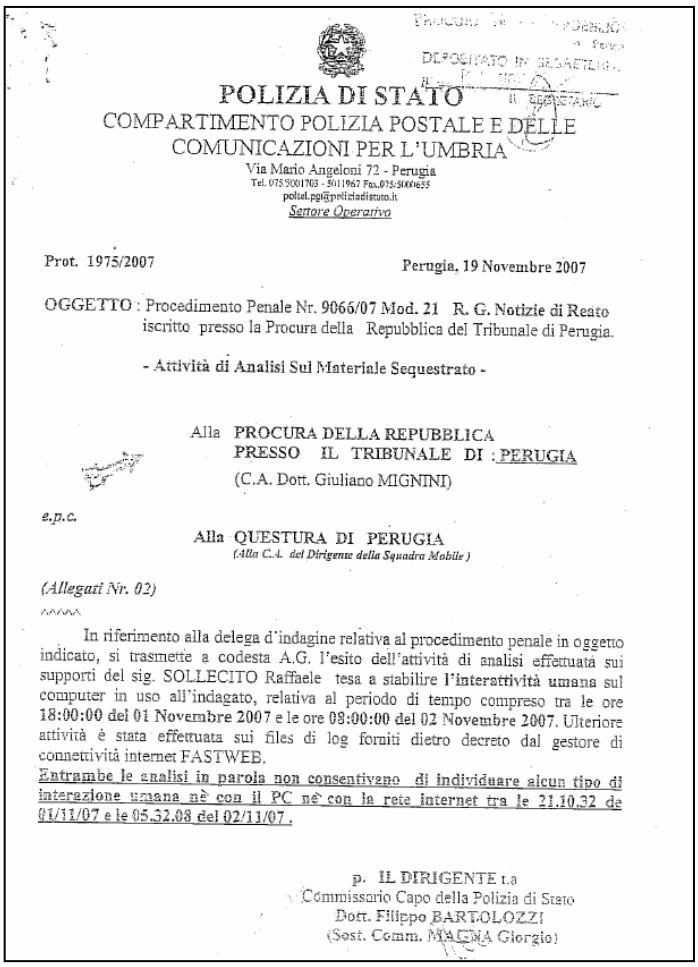
It is evident that that file was not detected above all because of the serious methodological error consisting in limiting the interval of file dates considered by ENCASE to an upper boundary of 8 am on November 2, 2007, and in not having verified through Spotlight (using the **same exact version** present on the computer of the person under investigation and not with a **"similar" version**). The fact that ENCASE displays a last access date of November 6, 2007 is not in contradiction with said result, because:

- the date of last opening visualized by Spotlight is managed among the *Other Information*, which means that it is modified by the applications (for instance when one watches a movie), while the dates shown by ENCASE are limited to file system dates (which are modified, for instance, by copying or reading the file with a program).

An unknown activity occurred on November 6, 2007 has hence surely modified the last access date and the last modification date of the "Naruto Ep. 101" file, without, however, modifying the "last opening" date, which instead was still available.

It must be moreover pointed out how the last access date (Tuesday November 6, 2007, 10.18.38 am) and the last modification date (Tuesday November 6, 2007, 1.28.09 pm) of that file correspond to *a time coinciding with the seizure of the laptop at Raffaele Sollecito's dwelling, a time when many other activities on said laptop, vouched for by the system log files, were detected*.

It has to be finally noticed that the duration of said animation movie episode is of about 20 minutes. It is not possible to know if the movie has been watched in its entirety or not, since alterations at a later time have overwritten this information, as for instance have the alterations that occurred on Tuesday November 6, 2007, at the time of the seizure of the computer, and later.



POLIZIA DI STATO
COMPARTIMENTO POLIZIA POSTALE E DELLE COMUNICAZIONI PER L'UMBRIA
Via Mario Angeloni 72 - Perugia
Tel. 075/5001703 - 5011967 Fax.075/5000655
polstat.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 Sul 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 05.32.08 del 02/11/07 .

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

---

3. In the [Postal Police] expert report the keyboard logs, indicating the start and the end of the activities on the computer and the logs of important applications used during the time interval at issue, among them the VLC logs, are neglected.

In the Postal Police expert report log files of some applications, particularly the VLC log files and the keyboard log files, which allow to illustrate important activities during the period of interest, are not mentioned.

VLC log files

The *plist* (property list) file of VLC contains among other information the list of the last multimedia files played.

Usually these files are shown to the user who opens the application in a drop-down menu, so that they can be more easily referenced.

In detail this list presents, in a reverse order from the most to the least recently played the following list of movies:

	Path of last file viewed with 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 1(incompleta)/[XviD - ITA-ENG] South Park - 1101 - With Apologies to Jesse Jackson.avi

One can notice some interesting information, (this one also absent from the Police's analysis):

a) the movie "Amélie" **is at a path different from that shown by ENCASE** and by the Postal Police report
b) there are consistent activities concerning **5 different versions of the movie "Stardust"** subsequent to the viewing of the movie "Amélie

a) the movie "Amélie" is at a path different from that shown by ENCASE and by the Postal Police report

Particularly one notices that, while VLC (which is a media player) put it at:

MacOS_HD/Users/macbookpro/Desktop

On the analysed hard disk the file is at the path

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

The relevant information one can deduce is that, at time of viewing, the file at issue was directly on the "Desktop", while it was subsequently put in the "Film visti" ["viewed movies"] directory, showing a behavior consistent with a full viewing of the movie, while at multiple times doubts have been expressed about it having been watched in its entirety, since it could have been played without anyone watching it. Actually, these two pieces of information about the path suggest that the 9.10.02 pm interaction is in all probability due to the act of moving the movie [file] after the viewing was over.

> *video file named "Il favoloso mondo di Amelie" ["Amélie"], identified by the path* ***HITACHI\1 Merged_Untitled\MacOS HD\Users\macbookpro\Desktop\aMule Downloads\Film Visti\[DivX - ITA] - Il Favoloso Mondo di Amelie.avi****, has been looked for. From here [once found the file], by controlling the properties of the file, it was possible to verify that the last opening of the same dated indeed 6.27 pm on 11/01/2007 and had been indeed made through the VLC program (see attachment number 03).*

b) there are consistent activities concerning 5 different versions of the movie "Stardust" subsequent to the viewing of the movie "Amélie"

The files at issue, from most to least recently viewed are:

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

Please notice that such behavior of viewing multiple copies is typical of those who download multiple copies of a given movie to keep the best ones, or those downloaded first, avoiding fake copies (spam).
One previews the various copies and keeps the best ones.

Notice also that the last writing of the file "(Divx-Ita) Stardust Ok.avi" shown by ENCASE is at 7.18 pm on 11/01/2007

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

the time when presumably its downloading from the net through the peer-to-peer software aMule finished, and indeed the file is presently in the "downloads" directory of aMule at path:

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

Once more it is not possible to know with certainty whether it has been accessed and viewed at a time immediately following the end of the downloading because, as you may notice, at 2.47 am of November 6, 2007, (a time when the person under investigation was detained under interrogation) the previous "last access" date was overwritten.

Finally an unusual circumstance is pointed out, according to the information coming from ENCASE, all the other "Stardust" files shown in the VLC menu do not appear to be among the files present on the disk nor among those deleted.

This issue was detected also by the Postal Police, which about the disappearance of these and other files downloaded through aMule gave the following explanation:

> ***The deleted files***
>
> *The [defense] technical consultants have attached to their counteranalysis a portion of the log of Amule [sic] (the version for the users of the FASTWEB network of the well known P2P software Emule [sic]), concerning the time interval between 5.01.56 pm and 9.28.25 pm of 11/01/2007, from which one infers that the Amule [sic], during said time interval, performed the full download of 3 out of 6 files requested for download: they are files ascribable to a movie named "Stardust".*
>
> *The hypothesis proposed in the report of the c.t.p [party technical consultants] is that two out of three of the files whose download was completed "have been manually deleted by an operator directly from the Amule interface after 9.28 pm" (end time of the last download).*
>
> *It is opinion of this bureau that it is true that those files have been removed from the system, but not through the Amule interface, since, in this case, indications about the time of date of the deletion would have been found in the log produced by the same application (the program would have produced a log line with the following fields: Date, Hour, File deletion and "filename", as it happened for the download of the following file, extrapolated from the same log:*
> *2007-11-01 17:04:02 Download of Stardust.2007.iTALIAN.MD.TC.XviD-SILENT-CD2.avi*
> *2007-11-05 13:05:33: File deletion: Stardust.2007.iTALIAN.MD.TC.XviD-SILENT-CD2.avi*
>
> *Moreover the deletion made with the ordinary file deletion operations provided by the operating system, occurred* ***between 9.28 pm of 11/01/2007 and the time of impoundment of the computer, occurred on 11/06/2007.***

The circumstance has in our opinion two other possible explanations, not mutually exclusive:

- ENCASE is unable to completely reveal the files deleted by the Mac OS X system in the version used by Raffaele Sollecito's laptop

- the files were on a virtual disk external to the laptop (see point 5 [rectius:7] concerning the SAMBA application)

However it is proved from the VLC [log] file that those files have been viewed subsequently to the viewing of the “Amélie” movie.

The keyboard log

In the Postal Police analysis an information source of fundamental importance is neglected, [a source] containing information stored as a *list of timestamps* and not with *date overwriting*, this [source] is the **keyboard log**, contained in the *windowserver.log .*

This file is very important because the Mac OS X system records on it the main events concerning the activation/deactivation of the keyboard. This excess of information has also been widely discussed by Apple users as exaggerated, this for instance is a comment on Apple users’ blog at a time close to the one of interest (July 2007)

Substantially, in this file are stored the keyboard activities of the user through a simple “switched on/switched off” sequence. When the keyboard is deactivated

(“switched off”) surely there was no human interaction with the keyboard or the mouse. The first time the keyboard or the mouse are used an activity of “switched on” is recorded, that is it is pointed out that the system is active. After a certain period (four minutes in this case) if there is no activity the keyboard goes in “standby” and, if configured, the screensaver kicks in.
Some programs, as for instance VLC or other media players, leave the keyboard and the computer in the “switched on” position so that viewing or listening is never suspended or disturbed.

Hence the analysis of the *windowserver.log* log file is fundamental to analyse **the periods when the computer has been used or when it certainly has not been used**.

From the analysis of Raffaele Sollecito's windowserver.log [file] for the time interval considered by the Police, it turns out a log sequence identifying the following periods:

1-Nov-2007	17:03:34		**keyboard wakes up**
	system active for 0:49:44		
	17:53:18		keyboard disabled
	inactive for 0:32:56		
	18:26:14		keyboard wakes up
	system active for about 11 hours		
2-Nov-2007	5:32:04		VLC crash
	5:36:18		keyboard disabled
	inactive for 5 minutes and 16 seconds		
	5:41:34		keyboard wakes up
	system active for 0:04:18		
	5:45:52		keyboard disabled
	5:46:02	inactive for 0:00:10	keyboard wakes up
	5:50:16	**active for 0:04:14**	keyboard disabled
	5:56:34	inactive for 0:06:18	keyboard wakes up
	6:00:46	**active for 0:04:12**	keyboard disabled
	6:06:38	inactive for 0:05:52	keyboard wakes up
	6:14:37	**active for 0:07:59**	keyboard disabled
	6:18:16	inactive for 0:03:39	keyboard wakes up
	6:22:28	**active for 0:04:12**	keyboard disabled
	inactive for 5:55:56		
	12:18:24		keyboard wakes up
	12:26:33	**active for 0:08:09**	keyboard disabled
	inactive for 18 h circa		
3-Nov-2007	5:42:12		keyboard wakes up

It has to be noticed that in the time interval between 6.26.14 pm on November 1 and 5:36:18 on November 2, 2007, the system is active without interruption, presumably a multimedia player, as for instance VLC, or other players for CD and DVD, keeps it active. The disabling of the keyboard occurring at 5.36.18 am is caused by a VLC crash at 5:32:04 am and is immediately followed by a new interaction after 5 minutes and 16 seconds. Then comes a sequence of short interactions due to the playing of songs until 6.22.28 am. The system then remains inactive for about 6 hours until 12.18.24 pm.

The analysis of the keyboard activity was not present in the report of the Postal Police.

4. There is no mention of an activity of song playing occurred between 5.41 am and 6.38 am on the morning of November 2

The Police report does not mention an activity of song playing, occurring in the time interval at issue. This activity can be observed from various data sources, both from ENCASE reports containing the dates of access to files, and from the log files contained in the iTunes musical library, “iTunes Music Library.xml”. The analysis of iTunes is important because it records the last time a song has been fully played, recognizing if it has been played only partially (“skipped”). The songs played are:

Song	**Start time according to ENCASE**	**End time according to iTunes**
10 Stealing fat.mp3	11/2/2007 5:44:45	Not Available
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	Not Available
32 Prelude.MP3	11/2/2007 6:06:41	Not Available
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	Not Available

Once more it is pointed out that the usual way users listen to song is that of *repeated listening* of preferred songs. Since the information are recorded through overwriting of dates, of the repeated listening of the same songs in the same evening it would remain just the date of the last listening. The iTunes file also shows that many songs were owned [by Sollecito] since 2005.

Finally it is pointed out that among the last operations made on the computer before 8 am on November 2, 2007, boundary of the time interval of interest, there is an

interaction due to activation/deactivation of Front Row, which is able to play songs and videos by downloading them from the web on temporary files which are then deleted.

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

A few minutes after the deactivation of the keyboard at 6.22.28 am on November 2, that is at 6.38 am, an interaction with the "DVDPlayback" file is detected, which hints at the presence in the laptop of a DVD containing videos or music, clearly undetectable by programs like ENCASE

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

since the related files and their dates are not modified.

---

5. **<u>Information outside the time interval going from 6 pm on November 1, 2007, to 8 am on November 2, 2007, is not analysed</u> hence the police analysis does not discuss nor detect eventual reasons for alteration/overwriting of the information related to the period of interest, and likewise later events caused by actions occurred during the period of interest are not detected.**
6. **the assessment is made using a <u>highly incorrect methodological hypothesis</u>, namely *it is assumed that the absence of timestamps in a given period is proof of absence of activity on the computer* (see also paragraph 1), omitting to point out that any later activity on a file can alter its date (the computer at issue has been used and has remained continuously switched on for 4 days after the period of interest.**

The examination of the Powerpoint slides shown during the trial confirms the methodological setup noticed in the first point above, seriously undermined by its limiting the analysis to files with dates in the period of interest, for instance the write and modification dates of the “iTunes Music Library.xml” file as shown by ENCASE are

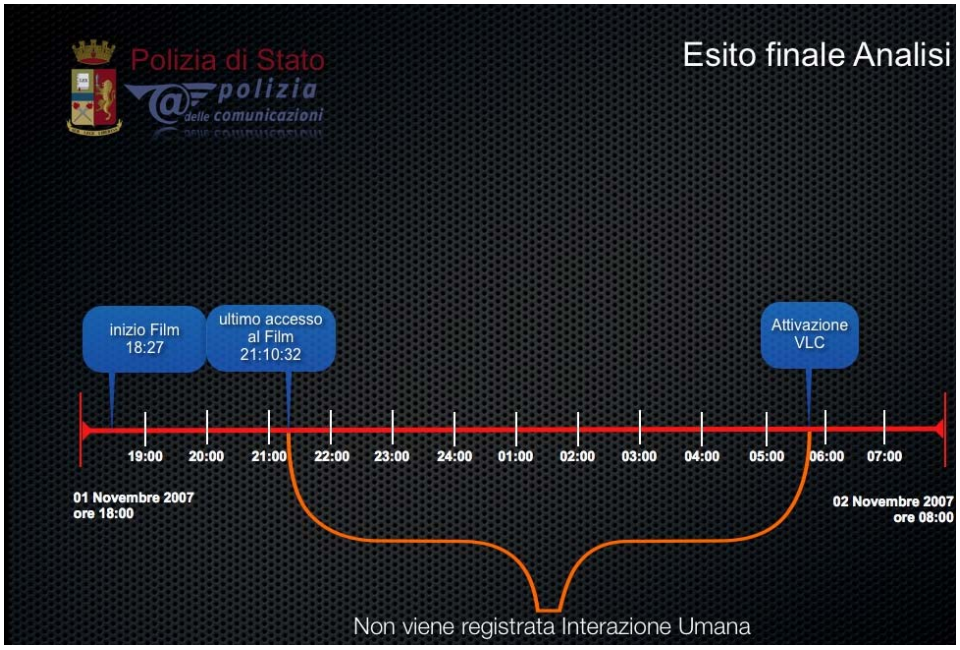
1	Name	Last Accessed	File Created	Last Written
7147	iTunes Music Library.xml	5-nov-07 13.35		6-nov-07 0.58

respectively on November 5 and November 6, 2007, hence being excluded by the Postal Police analysis.

While it is well known that “iTunes Music Library” contains the dates of important interactions during the period under examination, as for instance the dates concerning the playing of the aforementioned songs.

Hence the assertion that *“no files modified and/or deleted during the time span of interest for the survey have been found*, while literally correct in the sense that *it is true that the [Police] consultants have not found such files*, is proof of a serious methodological malpractice, since it is manifest that the “iTunes Music Library.xml” file was modified exactly during the time span of the survey, since it contains recordings of events occurring during that period (the dates of songs’ playing). Yet it has been also modified at a later time, and for this reason it displays a later modification date. The criterion of limiting oneself to analyse the files [whose dates fall in] the narrow period required [by those who commissioned the expert report to the Postal Police] is misleading, especially considering that the computer was left switched on for a further four days and even slightly more.

In the [Powerpoint] presentation of the conclusions [of the Postal Police report] it is said that “no human interaction has been recorded”



while it is totally omitted that:

- the keyboard remains always active during the whole time interval at issue (9 pm - 5.44 am approximately),
- the viewing of the **"Naruto Ep.101.avi"** file started at 9.26 pm (the video lasts for about 20 minutes);
- the fact that the keyboard is **reactivated immediately after the VLC crash**, while a generic "VLC activation" is mentioned, (it is not VLC which is activated by the user, but the user who gets active after its crash!);
- the human interactions related to song playing occurring from 5.44 am onwards are not mentioned;
- **the VLC's plist is not analysed**, while it reports the viewing of other songs [rectius:video files] after "Amélie";
- **the moving of the "Amélie" file from the "Desktop" to the "film visti" ["viewed movies"] directory is not mentioned**;
- it is not taken into consideration the that the **"recording of human interaction"** during the period at issue may have been **overwritten** at a later time, as it occurred for the "iTunes Music Library.xml" file or for the last access to "Naruto Ep.101";
- it is not taken into consideration the possibility of **listening/viewing of CD/DVD**, even if a music CD of the band "Blind Guardian" was inside the seized laptop, an activity leaving no trace on the hard disk.

Furthermore on the acquisition report about the IT material impounded from Raffaele Sollecito, dated November 15, 2007, and signed by Postal Police officers Bartolozzi, Trotta, Trifici and at the presence of technical consultant Formenti, one reads that

From the check of the optical player [CD/DVD unit] of the slot-in type it was possible to find inside said optical player a music CD of the band BLIND Guardian.

The hypothesis that the PC may have played a CD during the period under examination is not considered and the finding [of a CD] inside the PC is not mentioned [in the Postal Police report].

It should be noticed how the slide presented during the trial displaying a "gap" captioned with the sentence "no human interaction recorded", is semantically misleading, since it suggests that the absence of traces of interaction is proof of the lack of interaction. Aside from not all traces having been detected, as seen before, the overwriting of dates, as shown in figure 1, can create paradoxical effects, by "deleting" explicit traces precisely during periods of intense repeated activities. There has moreover been a semantically ambiguous use of the term "ENCASE records", assimilating them to the more common "phone records" and not pointing out that, while the latter store *"sequences of events"*, where a gap indeed corresponds with certainty to a lack of activity, the Encase records are instead lists of dates [recorded] by overwriting and the many temporal "holes" are no proof at all of a lack of activity during those periods.

Summing up

During the time interval going from 9.26 pm on November 1 (starting of the viewing of Naruto Ep.101) and 5.41.34 am (keyboard wakeup after the VLC crash), there are multiple and different activities which may have *reasonably occurred* and whose date may have been overwritten, between the moment of occurrence and the time of the impoundment of the laptop (November 6, 2007) or that may have left no trace on the hard disk because of their intrinsic nature:

- **song playing through iTunes or FrontRow or other players**, repeated at later times (actually at the end of the night and during the following days many songs owned since a long time are played, see iTunes dates);
- **viewing of videos like Naruto Ep.101**, whose date has been overwritten later at the time of the seizing of the computer (actually the access dates of many .avi video files have been overwritten on November 6 at 10.18 am or after 1 pm);
- **viewing of movies like Stardust, subsequently deleted** (the Stardust files have surely been viewed in an undefined period after the viewing of "Amélie" and before the impoundment of the computer, as proven by the log of the VLC plist);

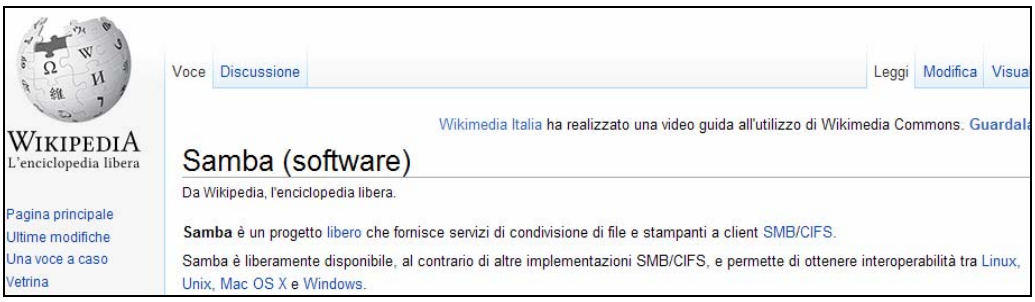
- **playing of video/music on virtual disk** from the Asus computer through SAMBA, the physical hard disk [of the Acer computer] is not available anymore;
- **playing of video/music on CD/DVD storage media**, which intrinsically do not leave trace (actually at 6.38 am on November 2 FrontRow and DVDPlayback have been activated and at the time of the impoundment a **CD of the band Blind Guardian was found inside the computer** of Raffaele Sollecito, who owns lot of them).

In favor of a continuous viewing of videos or playing of music is the fact that the keyboard never goes in *standby* mode, therefore an application or a human interaction kept it active (FrontRow? iTunes? VLC?). Besides, the VLC application crashes at 5.32.04 am and a few minutes after the following standby the computer is awakened again at 5.41.34 am through an interaction testifying to a continuous human presence near the computer and the crashed multimedia application, whose crash is presumably detected and remedied by restarting it. Moreover there are no interactions with FrontRow or the DVD reader after the night of November [1-]2.

---

7. **There is no mention of the use of the SAMBA application, through which one could have network access (virtual disk) from the MacBook to the hard disk of the other Raffaele Sollecito's laptop (the Acer one), which was found unserviceable for analysis.**

It is ascertained that Raffaele Sollecito was using the old Acer computer only as a sort of "workhorse" to download movies/songs from the Internet. The problem of moving the files from said Acer to the Mac for viewing/listening was solved using the SAMBA application, which allows the mounting of a remote disk as if it were a local disk on another computer.



In other words, through SAMBA it was possible to open a file on the Apple computer without this leaving trace on this computer, since the file was on a virtual disk/directory of the Apple computer while in truth physically residing on the Acer.

On the other hand, if a file was moved to the Apple's "Trash", it was [physically] deleted [on the Acer computer], but it could not certainly be found among the deleted files on the Apple computer with an ENCASE analysis limited only to the hard disk of the Apple computer.

The use of SAMBA, documented on Raffaele Sollecito's computer, would also explain the "disappearance" without leaving trace of the "Stardust" files, please notice that at least two of them are shown by VLC as moved to Trash (.Trash):

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

Samba was regularly used and of its periodic automatic updating there is also trace in the ENCASE file:

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. There is no mention of **a sure access activity to the computer** owned by Raffaele Sollecito, the browsing of a web page, **occurred on November 5, 2007, while he was under interrogation**

While Raffaele Sollecito was under interrogation, there was with certainty an access activity to the computer under examination. This activity is proven both by the ENCASE files produced for the Postal Police expert report and by the windowserver.log file recording the activities on the keyboard, and also by the log files of the Internet provider.

Sure enough, the keyboard, which previously deactivated at 4.34 pm on November 5, 2007, suddenly reactivated at 10.04 pm, going again into standby mode at 10.14 pm

```
Nov 05 16:34:46  [57] Hot ket 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
```

not to get activated again until the next morning, at 10.17.04 on November 6, 2007, when the laptop was seized.

There is no mention of <u>the alteration of dates on a sizable number of files occurred on said computer at a time following its acquisition by the judicial authority</u>, the alteration having concerned many video files (including the Naruto Episode 101 already mentioned at point 2).

From the Postal Police report and from the presentation at the trial, surprisingly no indication has been given about steps taken to guarantee the integrity of the laptop and of the hard disk from the moment of impounding (on November 6 at about 10.20 am) to the time of acquisition of the data at the presence of the technical consultants (November 15, 2007), the focus mainly being on the guarantee given by the hash or "fingerprint" of the hard disk. From the reports it is not clear whether the hard disk has been extracted from the laptop in front of the consultants or whether it had already been previously extracted.

There are indeed available data showing how the impounding occurred with debatable technical procedures, and they prove with certainty and repeatability how there was subsequently an alteration of the dates of many files, at a time when the computer was already in the hands of the authorities. In at least one case said alterations have concerned a file (Naruto Ep.101) proving an important human interaction during the period of interest.

The main sources of reference for such assertions are three:

- the keyboard activity **windowserver.log** file;
- the **system.log** file dealing with the start-up/shutdown activities of the system;
- the **files generated by ENCASE** (available also to the Postal Police, but they do not mention those alteration because they consider only the files in the November 1 - 2 timeinterval).

Impounding procedure

From the windowserver.log one infers that the computer reactivates from standby at 10.17.04 am, while it had remained inactive since 10.14.38 pm on the previous evening (an interaction occurred when Raffaele Sollecito was detained by the Police).

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

From the timeline it can be deduced there was no activity, since after exactly 4 minutes (the preset waiting time) the system enters standby at 10.20.56 am; the laptop then goes back to active mode 4 seconds later, from the system.log file one learns on the other hand that it begins to activate the “hibernate” mode at 10.20.57 am.

The “hibernate” mode allows the system to save the memory [RAM] and the present state of the computer on the disk, then executing a “virtual shutdown” to economize energy.

Among forensic specialists there is an open debate about which is the best procedure to acquire a computer [“supporto”, literally a storage medium, but more correctly it means “the computer, its memory and its storage media”]. In many cases one opts for a “sudden shutdown”, when it is not possible or interesting to perform a “live” analysis on the powered on computer. A “sudden shutdown” may consist, for a laptop, in the extraction of the power chord and of the batteries, thus preventing a regular shutdown from altering dates inside the computer. In this case most probably the laptop’s screen [lid] was shut on the case, believing that this action would have shut down the computer, which instead went in “hibernate” mode.

The ENCASE analysis shows that there are file modifications until 10.20.57 am.

Data alterations after impounding

At 1.27.36 pm according to the *windowserver.log* file, that is about three hours after the impoundment, the keyboard reactivates

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

this is the last entry in the windowserver.log file, while the system remains active for more than 8 minutes, until 1.35.45 pm, without deactivation of the keyboard, hence with presumable interaction or with programs keeping the keyboard active.

Also the analysis of the *system.log* file confirms that the system awakened at that time

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

Thirteen seconds later the computer tries to connect to the wireless network of Sollecito’s dwelling, not finding the network, presumably because it is now at another place.

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

the computer tries then to scan, without finding them too, the networks it usually connects to, among them those at the University, "informatica" and "dip-open".

There are no more information on the *system.log* file, proof of the fact that the computer is subsequently shut down or shuts down abruptly. It is however possible to deduce from the ENCASE files that, during the next 8 minutes, while the keyboard is still activated, modifications occur to some files and [these modifications] go on until 1.35.45 pm. Among the others, the dates of the following video files are modified:

	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

specifically you may notice that among them there is also the aforementioned "Naruto Ep.101" and both previous and following episodes.

Unfortunately the dates these files had at the time of the impounding have been irreparably overwritten because of the procedure used after the seizure, the surprising thing being that said modifications occurred before the intervention of the parties' [defense and also civil parties] consultants.

It is possible to formulate various hypotheses explaining these modifications in an innocent way:

- incompetence and ignorance of the workings of the *hibernate* [mode] and of *aMule*, which could have automatically saved the files immediately before the hibernate and immediately after a reopening [of the lid] of the laptop, modifying their dates;
- lack of skill and careless examination of the files someone could have attempted to open, or of aMule which they could have attempted to close;
- accidental shutdown of the just restarted laptop because of lack of charge of the batteries (theory backed up by the strings in the following table, extracted from Encase and highlighting the calling of a system function pointing to the imminent system shutdown due to a dead

battery), in such cases the system, while attempting a “clear shutdown”, tries to close automatically all the applications, which in turn close the open files, modifying their dates. Said files could have been open because available for downloading to other users of the peer-to-peer software 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

It is evident that the modification of the dates of the previous files, as well as that of more than 520 other files (as testified by the ENCASE report) prevent the implementation of a complete analysis of the original dates. In the case of “Naruto Ep.101” they have been recovered rather by chance through Spotlight, but other interactions could have been overwritten the dates of the other episodes of the Japanese series [literally “character”].

It is moreover at the very least amazing the employment of procedures modifying evidence during the impounding and the switching on again of the computer without the presence of the parties’ consultants.

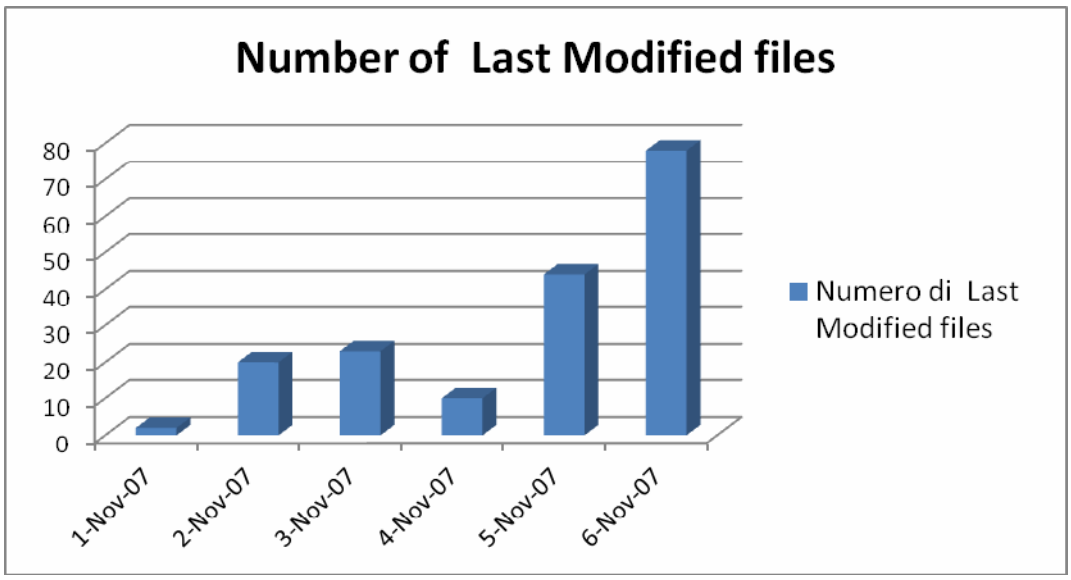
4. Conclusions

In conclusion it is possible to point out a set of new elements having an impact on the formation of a decision about the case:

- the certain viewing of the file Naruto Episodio 101 at a time never before noticed, 9.26 pm, supports the hypothesis of a presence lasting at least as much as the movie (20 minutes), therefore until 9.46 pm;
- the certain moving of the "Amélie" file from the Desktop to the "FIlm visti" directory, *backs up the hypothesis of a continuous presence during the viewing of "Amélie"*;
- the keyboard that remained active from 6.26 pm on November 1 until the VLC crash, and which then deactivated at 5.36.18 am on November 2 to reactivate about 5 minutes later thanks to a user interaction, *supports the hypothesis of a continuous presence/activity* (unless one supposes that the defendant came back home exactly five minutes after the computer crashed);
- there is a reasonable doubt that other activities on the computer occurred after 9.26 pm, whose traces were overwritten by repeated activities (for instance the playing of songs), or completely deleted because virtual (SAMBA);
- there is a reasonable doubt that those activities involved music files or videos, given that FrontRow and the DVD unit were used, given the presence in VLC [logs] of the files of the movie "Stardust", which cannot be found in any other place, and given the certainty of the presence of a CD of the band Blind Guardian inside the PC;
- the certainty that there has been an access to the computer when its owner was absent on the night of November 5, 2007.
- the certainty that there have been alterations on more than 520 files after the impoundment of the laptop which changed the dates of important files.

We want once more to point out the semantically misleading use of the term “record” for information like that generated by ENCASE, which comes in the form of tables, but which report only the last modification of a file and not the “sequence” of the modifications. The fact that repeated activities may cause the overwriting of dates produces, as said above, the paradoxical result that users who are very active, but who often repeat the same actions, appear to have modified just a few files.

For this purpose we report as an example the following bar chart, showing the number of “avi” and “mp3” files modified on Raffaele Sollecito’s computer on each day from November 1 to November 6, 2007. The chart is based on the real data from ENCASE.



The chart could induce a naive analyst to surmise that, getting close to November 6, 2007, one has a crescendo of accesses to avi/mp3 files, while there have been few or none in the past.

Actually, if one reckons that the *Last Accessed* date is overwritten and if one reasonably surmises that the user has a certain level of “reutilization of multimedia file”, it is manifest that the most part of the overwritten files must be recent. While few files seem to have been modified in the past, since their dates have been almost completely overwritten by later use.

To have unequivocal and complete traces, a “phone record” of sorts, in a system based on the *overwriting of dates*, the user should do ever-changing

actions and never repeat them, as, for instance: never to listen twice to the same song, never to read multiple times the same thesis, never to check multiple times the movie one is downloading, never to use multiple times the same word processor, etc., practically the exact opposite of most users' behavior.

Professor Alfredo MILANI

This report takes advantage of the fundamental investigative results and of the precious collaboration of Doctor Antonio d'Ambrosio.

The report also uses the suggestions and the results of the work performed by Doctor Engineer Andrea Chiancone, Doctor Paolo Bernardi, Doctor Emanuele Florindi, Doctor Marina Latini and Doctor Engineer Valentino Santucci.