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

Prot. 1975/07 Perugia, 19 Novembre 2007
Cat. Q 2.2 – Polpost

OGGETTO: Procedimento Penale Nr. **9066/07** R.G.N.R. mod.21 iscritto presso la Procura della Repubblica del Tribunale di Perugia.-==========
-Perizia Tecnica relativa all'analisi dei supporti magnetici sequestrati a SOLLECITO Raffele- Parte 1^-==========

AL SIGNOR DIRIGENTE S E D E

^^^^^

Il sottoscritto **Ass.te Capo TROTTA Marco** in servizio presso la Squadra di P.G. di questo Compartimento, unitamente agli **Ass.ti GREGORI Mirco e TRIFICI Claudio**, riferisce alla S.V. che in data 17 Novembre c.a., in esecuzione alla delega d'indagine relativa al procedimento penale in oggetto indicato, è stato dato inizio all'analisi del materiale sequestrato a SOLLECITO Raffele, in altri atti generalizzato, indagato dalla Procura della Repubblica presso il Tribunale di Perugia nel Procedimento Penale nr.9066/07 R.G.N.R. mod.21.

Il materiale analizzato è composto da dati acquisiti dall'hard-disk del pc portatile MacBook Pro, e da nr.02 Pen Drive della capacità ciascuna di 128 Mb.

PREMESSA

L'analisi dei dati presenti nei supporti magnetici è stata condotta collegando i supporti ad un PC usato per l'analisi probatoria di materiale informatico, interponendo, tra i due, idonea strumentazione deputata alla protezione da qualsiasi alterazione dei supporti magnetici analizzati. Tale apparecchiatura, denominata, nel caso degli hard-disk **DESKTOP WRITE-PROtect e OMNIPORT**, entrambi prodotti dalla società **LOGICUBE**, è stato assegnato a questo Ufficio, specificatamente per detta tipologia di attività di P.G., dal Servizio Polizia delle Comunicazioni.

L'attività è stata poi condotta, da prima, acquisendo i dati presenti nei supporti magnetici, e successivamente eseguendo l'analisi vera e propria sui dati acquisiti; il tutto è stato eseguito mediante l'uso del programma denominato "**ENCASE**", nella versione **6.x**, software prodotto dalla software-house americana "**GUIDANCE**

SOFTWARE", usato per l'acquisizione delle evidenze probatorie in campo informatico, che permette di effettuare la lettura dei dati da analizzare, preservandoli dalla scrittura, e rendendo quindi l'atto **ripetibile in ogni momento**

L'analisi è stata condotta effettuando da prima una ricerca nei file riscontrati all'interno degli hard-disk, e successivamente nei "**cluster non allocati**", ossia in quella parte fisica dell' hard-disk contenente informazioni relative a file non più nella disponibilità del Sistema Operativo (S.O.) in quanto cancellati, ma comunque, almeno in parte recuperabili.

L'attività di analisi è stata divisa in due parti, la prima, di cui questa relazione ne è l'esito, relativa all'acquisizione di riscontri tesi 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; la seconda, relativa all'estrapolazione dei dati in chiaro di file di testo, immagini, video e ricerca con parole chiave, il tutto per la successiva visione da parte di personale della locale Squadra Mobile, eseguita successivamente, stante il bisogno di un maggiore lasso di tempo per l'esecuzione.

ANALISI DEI DATI

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

L'analisi dei dati dava **esito negativo** in ordine a **file modificati** e **cancellati** in quel lasso di tempo nel sistema.

La ricerca dei **file creati** (File created) permetteva di verificare che nell'arco di tempo in questione sono stati prodotti dal sistema solamente nr.09 file, di cui due creati entrambi alle ore 03:15:07 del 02/11/2007 dal sistema in automatico, ed i restanti relativi a file generati in automatico dal browser di navigazione Mozilla Firefox all'interno della sua cache, file caratterizzati dall'esser stati creati ad intervalli di 60-120 minuti l'uno dall'altro. Detti file, mediante una delle peculiarità di del software di analisi ENCASE venivano estrapolati e riprodotti all'interno di una cartella denominata "file creati" contenuta nel CD-Rom allegato alla presente relazione, e ne veniva creato il relativo "report" (vedi allegato nr.01).

La ricerca dei **file scritti** (Last Written) permetteva di verificare che nell'arco di tempo in questione sono stati prodotti dal sistema nr.**17** file, di cui uno posto all'interno di un cluster danneggiato, per il quale non era possibile acquisire alcuna informazione. Dei rimanenti:

-nr.**08** sono riconducibili a file scritti in automatico dal browser di navigazione Mozilla Firefox all'interno della sua cache, file caratterizzati dall'esser stati creati ad intervalli di 60-120 minuti l'uno dall'altro;

-nr.**02** erano relativi a file generati in automatico dai programmi di "files sharing" al termine del download dalla rete;

-nr.**03** sono relativi a log generati in automatico dal sistema;

-nr.**03** sono relativi a crash di programmi per la riproduzione di file audio video.

Questi ultimi, che prevedono l'interattività di una persona che ne mandi in esecuzione l'applicativo, sono stati scritti dal software per la riproduzione di file

audio e video denominato "VLC" alle ore 05:32:09, 05:32:12 e 05:32:13 del giorno 02/11/2007.
Detti file, mediante una delle peculiarità di del software di analisi ENCASE venivano estrapolati e riprodotti all'interno di una cartella denominata "file scritti" contenuta nel CD-Rom allegato alla presente relazione, e ne veniva creato il relativo "report" (vedi allegato nr.02).

La ricerca dei file sul quale vi era stato un **ultimo accesso** (Last Accessed) permetteva di verificare che nell'arco di tempo in questione ne sono stati prodotti complessivamente nr.124, di cui uno posto all'interno di un cluster danneggiato, per il quale non era possibile acquisire alcuna informazione.

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

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

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

Tutti i file sul quale vi era stato un **ultimo accesso**, mediante una delle peculiarità del software di analisi ENCASE venivano estrapolati e riprodotti all'interno di una cartella denominata "file ultimo accesso" contenuta nel CD-Rom allegato alla presente relazione e ne veniva creato il relativo "report" (vedi allegato nr.04).

L'analisi dei dati presenti in entrambe le pen drive non consentiva di individuare alcun file sul quale vi era stata interazione tra le ore 18:00:00 del 01 Novembre 2007 e le ore 08:00:00 del 02 Novembre 2007(vedi allegato nr.05 e 06).

Si fornisce unitamente alla presente nr.04 allegati cartacei ed un supporto ottico non riscrivibile CD-R, facenti parte integrante della presente relazione tecnica.