UDIENZA del 14.3.09 - 09-03-2009 -

domanda sulla continuità

PREMESSA

Il Compartimento Polizia Postale di Perugia è stato delegato dalla Procura di Perugia all'analisi dei supporti informatici sequestrati nel corso dell'attività di P.G., attività delegata svolta in **due fasi** ben distinte: **l'acquisizione** dei dati dai supporti informatici sequestrati e **analisi** vera e propria dei dati acquisiti.

Al fine di consentire alle parti di eseguire proprie analisi sui dati presenti nel materiale sequestrato, si è concordato con la Procura di eseguire l'acquisizione di tutti i dati presenti nei supporti informatici, mettendo poi a disposizione i dati ottenuti.

La **prima fase** di attività è stata eseguita **avvisando formalmente** tutte le parti interessate (indagati e legali)ed invitando le stesse a presenziare alle operazioni tecniche svolte poi successivamente presso i locali del Compartimento.

A dette operazioni aderivano solamente **i legali dell'indagato SOLLECITO Raffaele**, che nominavano nell'occasione quale loro consulente tecnico il sig. **FORMENTI Fabio**, persona che **presenziava** poi a tutte le fasi di **acquisizione** del materiale sequestrato a tutti gli indagati, **senza mai obbiettare alcun ché su procedure applicate o strumentazione utilizzata, come riportato nei verbali di acquisizione .**

ACQUISIZIONE 15 e 16 Novembre 2007

Le operazione di acquisizione dei dati, per quanto concerne i dati contenuti nei supporti magnetici, è stata condotta semplicemente eseguendo **una copia dei dati presenti nei supporti**, **comprese le parti non allocate o non utilizzate del medesimo**, materialmente il tutto viene condotto **collegando il supporto ad un PC**.
Questa attività, al fine di **rendere ripetibile l'atto**, deve essere effettuata senza apportare alcuna modifica ai supporti informatici in argomento **interponendo** a tal fine **tra la fonte di prova il PC utilizzato per l'acquisizione idonea strumentazione**.

Nel caso specifico tutti i supporti analizzati sono stati acquisiti collegando gli stessi ad apposito hardware per la protezione in scrittura denominato "**Desktop Write Protect**" (SLIDE 1-foto Fastblok) per gli hard disk e "**Omniport**"(SLIDE 2-foto Omniport) per le periferiche USB, prodotti entrambi dalla **LOGICUBE** e facenti parte della **dotazione tecnica** forniti al Compartimento dal Servizio Polizia Postale e delle Comunicazioni. Per quanto concerne il software utilizzato per le acquisizioni, in detta fase è stata utilizzata la **versione 6.7** di **ENCASE**, software prodotto dalla **GUIDANCE SOFTWARE**, anche questo facente parte della dotazione tecnica del Compartimento. Il software in questione, al fine di validare la copia eseguita, al termine della fase di acquisizione effettua in automatico una verifica sull'hash calcolato nei dati acquisiti, con quello calcolato nel supporto sorgente (slide 3-report acquisizione hd sollecito con ingrandimenti stringhe **Hash acquisizione** e **Verifica Hash**).

IL PROGRAMMA ENCASE ESEGUE IL CALCOLO DELL'HASH PER LA VALIDAZIONE DELLE EVIDENZE DIGITALI MEDIANTE L'USO DELL'ALGORITMO CRITTOGRAFICO DI HASHING MD5.
QUESTA FUNZIONE MATEMATICA PROCESSA UN DATO ARBITRARIAMENTE GRANDE, E PRODUCE COME RISULTATO UNA STRINGA CON LUNGHEZZA FISSA COMPOSTA DA 32 VALORI ESADECIMALI .

→ IL PROGRAMMA SE NON È DELL'ULTIMA VERSIONE PUÒ PRODURRE ERRORI ? → COMPUTER ROMANELLI

GENUINITÀ della COPIA

HARD DISC non funzionanti 1 dei 2 di Sollecito
1 Amanda
1 Meredith

Le operazione di acquisizione sono state possibili per tutto il materiale sequestrato ad eccezione di 3 hard disk installati nei notebook di Meredith KERKHER, Amanda KNOX, e del portatile marca ASUS di SOLLECITO Raffaele.

Tutti i **dati acquisiti** sono stati poi riversati in **duplice copia** in alcuni supporti magnetici, una copia a disposizione dell'AG procedente e una copia a disposizione della PG. .-

Copia del materiale acquisito dai supporti sequestrati a Raffaele SOLLECITO sono stati poi consegnati al consulente tecnico Fabio FORMENTI

ANALISI

Tutta l'attività di analisi, per quanto riguarda i supporti magnetici, è stata eseguita **sui dati acquisiti**, **e non sui supporti sequestrati**, e prima di dare inizio all'attività vera e propria è proceduto **all'aggiornamento della versione di ENCASE portando la versione in dotazione dalla 6.7 alla 6.8, rilasciata dalla GUIDANCE Software pochi giorni prima**.

Per quanto concerne quella che è l'attività di analisi, giova fare una premessa su quelle che sono le caratteristiche che identificano un file; **il nome**, **le dimensioni**, **locazione del file** all'interno del supporto analizzato e **l'estensione,** che consente di individuare il formato del file e l'applicativo ad esso associato per leggere, scrivere e interpretare il contenuto del file stesso.

Ogni file è altresì caratterizzato da:

- ***data di creazione****data e l'ora di creazione del file all'interno del supporto*
- ***data di modifica*** *data e l'ora in cui il file è stato modificato*
- ***ultimo accesso*** *ultima volta che vi è stata interazione sul file*
- ***data di cancellazione*** *data e ora in cui il file è stato eliminato.*

che differenza c'è tra ultimo accesso e ultima scrittura?

Sulla base delle disposizione impartite dalla Procura, si sono andate a cercare all'interno del **notebook** di proprietà di **Raffaele SOLLECITO**, tracce di **interazione umana tra le ore 18:00 del 01 Novembre 2007 e le ore 08:00 del 02 Novembre 2007**.

A tal fine mediante l'uso di ENCASE sono stati analizzati tutti i file **creati** (created), **cancellati** (deleted), **modificati** (Last written), e su cui vi era stato **ultimo accesso** (last accessed) nell'arco di tempo sopracitato.
Il software permetteva di verificare che **non vi erano stati file modificati o cancellati** nell'arco di tempo sopracitato.

La ricerca di **FILE CREATI** (created) permetteva di verificare che nell'arco di tempo in questione sono stati creati nel supporto analizzato **nr.09 file**, risultati poi **generati** tutti in **automatico** dal browser di navigazione **MOZILLA FIREFOX** ad intervalli di **60-120 minuti (SLIDE 4-report Encase file creati)**.

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 ;
-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.
(SLIDE 5-report Encase file Scritti)

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 (SLIDE 6-estratto da report Encase file Scritti con i due files)

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**(SLIDE 7- report Encase file creati)**..

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" (SLIDE 8-estratto da report Encase)

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" (SLIDE 9-Propietà del file ottenute con Mac Os)**

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**.

PROIEZIONE DEL FILMATO REALIZZATO PER IL RIESAME

Per finire viene mandato il filmato realizzato per stabilire definitivamente che mentre Mac Os certifica l'ora in cui il film è stato iniziato a vedere.....Encase certifica l'ora in cui è stato definitivamente abbandonato !!!!

2 USB PEN

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.

* Da chi hanno preso in consegna i computer?
Quando (in che data)? → verbale di consegna 13 ~~[illegible]~~ nov

(prima scremata + impronte latenti)

*GENUINITÀ COPIA (clone) si riproducono anche per errori

*SOFTWARE utilizzato x copiare (modernissimo)
(il sistema ridicolo dai CT non esiste (10-8-4)).

* MARCO TROTTA
* CLAUDIO TRIFICI
* MIRKO GREGORI

HARD DISK non funzionanti
- 1 dei 2 di Sollecito
- 1 Amanda
- 1 Meredith

* Come si fa a dire che Sollecito ha utilizzato solo uno dei due computer? FILE di log / DI FASTWEB

le attività del telecomando è registrato??
Consegnata copia al CT di parte.

MAC certifica l'apertura
ENCASE la chiusura

*ANALISI

Che cosa cercavate? Tutto ciò che era successo dalle 18,26 del 1° nov alle 8 del mattino successivo.
(fa film ma già stato scaricato il 28 ottobre)

Programma VLC

* CORRISPONDENZA degli ORARI (VERIFICA DATA/ORARIO) 5,32 del mattino (fallito un tentativo di connessione)

CONTROANALISI dei CT di parte (hanno interpolato i dati dell'ENCASE con quelli di MAC OS)

browser di aggiornamento della navigazione su Web ad intervalli regolari (a 60 o a 120 minuti)
FILE DI CRASH

— file NARUTO | BLOG di Sollecito | PENNETTA

— favoloso mondo di Amelie ultimo acceso alle 21,10,32 sec
i CT di parte hanno preso l'orario di chiusura e lo hanno letto come orario di apertura.