Università degli Studi di Camerino

Master in Digital Forensics

Indagine difensiva e consulenza tecnica di parte

Candidato
Emilio Luchetta

Candidato
Ilaria Tiranti

Relatore
Dott. Mattia Epifani

A.A. 2011/2012

INTRODUZIONE:
TECNOLOGIA DIGITALE E MODUS OPERANDI

Il nostro vivere quotidiano è sempre più legato al digitale e a tutto ciò che comporta.
L'iperconnettività della nostra vita implica la convivenza con i suoi aspetti positivi e negativi che condizionano, conseguentemente, la gestione delle nostre azioni e dei loro effetti, in ogni direzione.
Sono quasi scomparsi i telefoni pubblici dalle piazze e dalle stazioni, ognuno di noi viaggia con almeno un telefono cellulare: chi fa uso di questi sistemi di comunicazione per lavoro ne ha almeno due, spesso con un iPad o similare in valigetta per rispondere al volo ai quesiti e agli aggiornamenti dell'ufficio.
Gli studenti li usano come supporto per lo studio e ancora sono adoperati in sostituzione della valigetta-catalogo prodotti dal rappresentante-venditore di merci, come ad esempio, occhiali, piscine, legno e prodotti per l'edilizia, ecc.
Sullo scenario non poteva e non può mancare il bisogno di investigare e di rappresentare i dati in modo forense, gli strumenti digitali sono molto utilizzati dalla malavita e da chi commette crimini, a tutti i livelli.
Un tempo di esclusivo appannaggio degli esperti del crimine "raffinato", i c.d. "white collar crime", la tecnologia digitale è ora a livello "consumer", con telefoni palmari che hanno la potenza di calcolo di un normale computer.
E' noto quanto siano difficoltose le azioni di contrasto e monitoraggio alla Criminalità Organizzata, rallentate dall'effetto dei confini e, spesso, dall'assenza di accordi bilaterali per ottenere l'autorizzazione ad agire, talvolta, a 10 metri oltre il limite fisico-legale.
Si impiegano mesi per le rogatorie internazionali che corrispondono ad "anni" per la vita quotidiana e ad "anni luce" per chi si sposta con mezzi senza problemi di fondi a propria disposizione!
Il risparmio di tempo per una persona perbene, attuato dall'uso dello strumento digitale, rappresenta un turbo ed una serie di facilitazioni incredibili per le azioni del Criminale, del Terrorista, del Killer della Camorra.
Ad esempio ora le aziende, quelle sopravvissute alla crisi e che cercano personale, prima di procedere all'assunzione in prova del candidato ne accertano le abitudini e le informazioni riservate consultando Facebook comodamente seduti alla scrivania.

Facebook è stato inserito con il noto logo nei palmari destinati ad un pubblico poco esperto ma molto interessato, tra i quali c'è chi lo usa per compiere atti di Stalking, adescamento di minori oppure azioni di raggiro contro ignari e creduloni acquirenti di autovetture mai possedute dal falso venditore, ecc.

Questi non sono che esempi di scene di problemi quotidiani, in cui il Legislatore ha avuto ed ha manforte grazie alle caratteristiche intrinseche dei sistemi digitali e degli oggetti utilizzati per il loro funzionamento.

Anche nei paesi dove è ancora possibile l'utilizzo di "cellulari usa e getta", il monitoraggio e la gestione delle reti di trasmissioni consente agli Investigatori di fare bene e presto il loro mestiere con risultati significativi che inchiodano l'utente criminale alle sue responsabilità, con prove circostanziate e inoppugnabili che ne determineranno la giusta condanna.

Si è sentito il bisogno di disciplinare l'ottenimento e la gestione delle prove digitali: i Legislatori, quello europeo e quelli delle rispettive nazioni, sono intervenuti in modo incisivo e pertinente per la trattazione forense di questi sistemi, rendendone irrinunciabile l'uso per l'addebito delle responsabilità riferite ad azioni criminali.

La trattazione forense del dato digitale consente l'ottenimento della Prova da rappresentare poi in Giudizio, assottigliando il gap tra l'azione criminosa e la ricerca e la classificazione tramite il conseguimento della copia forense, l'analisi e la rappresentazione alla Corte di Giustizia.

Una delle caratteristiche principali della Prova Digitale è la ripetitività dell'azione, nel senso che, con le dovute procedure e metodologie forensi, è possibile evitare di inquinare la scena criminis, anzi possiamo dire che è ormai un obbligo e una serie di modalità operative oggetto di check list operative che dettano l'*how to* per l'investigatore digitale forense.

Altra caratteristica fondamentale della Prova Digitale è la non ripudiabilità del dato e del suo valore intrinseco.

Coloro che hanno condotto o partecipato ad operazioni forensi in presenza del C.T. (sia esso nominato dalla Procura, dalla Difesa per l'Indagato), quando si tratta di aree digitali, si ritrovano a discutere ed a convergere con questi ultimi e, infine, sul fatto che quel metodo di tutela del dato è accettabile seppur non certificato da un Ente preposto alle opportune procedure di Test Scientifico e Tecnico.

In Italia e in Europa ancora non esiste, infatti, un'Autorità super-partes in grado di offrire un servizio di questa tipologia, come ad esempio il National Institute of

Standard and Technology Americano, www.nist.org, in grado con un proprio laboratorio scientifico di testare e valutare l'attendibilità forense dei sistemi Hardware e Software che vengono sottoposti a test.

Le garanzie che sono offerte da un Ente Governativo e, come in questo caso, non dipendente dal Dipartimento di Giustizia USA ma da quello del Commercio, sono utili per tutti gli Attori dello scenario giudiziario, per l'Inquirente che non si vedrà invalidare il risultato delle fatiche profuse con dispendio di risorse economiche ed umane, per l'Indagato e per la sua Difesa che possono contare nell'impiego di metodologie scientifiche testate e comprovate, non frutto di pareri spesso discordanti tra di loro.

Il dato digitale è di per se' "certo", si basa sul linguaggio binario che è identico per tutti, dalla fotografia digitale alla stringa di dati che viene inviata dal sistema GSM associata alla fonia voce, dall'allegato ad una e-mail inviata, all'header e footer di un file scambiato tra utenti sospetti di violare il Codice Penale.

Il punto di discussione sta nel modo di gestire questi dati da parte dell'Investigatore che si deve preoccupare da principio della loro integrità con la consapevolezza che, a differenza di un reperto di DNA dove il prelievo obbligatorio per l'analisi ne comporterà la sua distruzione parziale o totale, la prova digitale potrà essere ripetuta e copiata all'infinito.

In conclusione di questa prima parte introduttiva al tema, l'area critica dell'acquisizione della prova digitale sta nelle modalità operative che vengono poste in atto dagli operatori di Polizia Giudiziaria, sia in quanto dipendenti diretti degli Uffici Operanti sia in qualità di Consulenti Tecnici incaricati dalla Procura o Periti del Giudice, ecc..

Talvolta, in assenza di un sistema idoneo oppure fabbricato dalle aziende specializzate del settore, il buon senso ci corre in aiuto, dandoci una mano a procedere con speditezza e validità forense, un esempio di quanto detto è dato da una nostra esperienza diretta sul campo.

Si doveva procedere per conto di una Procura della Repubblica a digitalizzare un'enorme quantità di videocassette in formato VHS, in quel caso si aveva la duplice funzione di C.T. e fornitore di sistemi digitali forensi per l'Autorità Giudiziaria.

I P.M. titolari delegati per l'Inchiesta avevano richiesto e decretato di procedere alla digitalizzazione di tutte le cassette VHS, della durata media di 180 minuti ciascuna, ma reperire sul mercato dispositivi di "sola lettura" avrebbe comportato un costo

enorme per tutti; l'idea fu di associare alla scheda di digitalizzazione dei PC un lettore VHS predisposto industrialmente per la sola lettura.
La soluzione fu di usare i lettori VHS a batteria 12/24 volt costruiti per la visione di film in formato VHS a bordo di autobus.
Questo suggerimento venne prima proposto, quindi discusso e infine accettato dalla Procura ed anche dai C.T. della Difesa: una soluzione digital forensics low cost ma certamente valida.
Per le aree dei Computer, oggi è possibile fare uso di sistemi "on site" procedendo alle opportune attività di "preview" alla ricerca di file e fotografie nei casi di pedopornografia, al fine di evitare di sequestrare grandi quantità di sistemi informatici-telematici: 10-12 anni fa ciò non era pensabile.
La regola era di sequestrare tutto e di predisporre un'area di vaste dimensioni per allestire un laboratorio di copia dati a livelli industriali, con tempi biblici per ogni supporto poiché i canali di uscita dei dati dai PC erano via porta seriale oppure via LAN 10/100. Ciò comportava il blocco delle attività dell'indagato per mesi, talvolta per anni, con danni incalcolabili a causa della perdita quasi definitiva dei dati, di opportunità professionali e lavorative per poi accorgersi solo alla fine, magari, che non era lui il colpevole ma era a sua volta vittima di attività malevoli sui suoi sistemi.
Riuscire oggi a fare copia in duplice esemplare di un Hard Disc di 500 Gb in meno di 2 ore, con blocco di scrittura hardware certificato e con trasferimento via USB 3, fa pensare di essere veramente sulla luna, a confronto di 2-3 anni fa.
L'investigatore digitale che intende fare buon uso di queste tecniche non può esimersi dal diventare un *computer forensic expert* o più in generale, vista l'eterogeneità dei supporti investigabili, un *digital forensic expert*.
La definizione di *Investigatore Digitale* è derivante dal concetto di *Digital Forensics* che racchiude tutte le tecniche investigative *high tech* che vengono trattate. L'investigatore deve quindi conoscere i supporti di archiviazione che saranno oggetto della sua *investigazione digitale*, sia esso un computer fisso o un portatile, un pendrive o una SD card, una micro-SD o un iPod, un iPhone o un hard-disk esterno, uno smartphone o un cellulare comune, ecc.
Egli dovrà dapprima identificare le diverse parti hardware che compongono e consentono il collegamento fisico di ogni supporto di archiviazione da analizzare alla "*macchina forense*" utilizzata per l'analisi forense digitale.

Non meno importante è l'apprendimento del funzionamento e la competenza nell'utilizzo dei diversi software che permettono l'analisi, nonché il continuo aggiornamento delle tecniche alle nuove tecnologie, ai nuovi dispositivi, ai nuovi software, essendo la materia in costante, quasi giornaliera, evoluzione.

Le principali fasi operative sono 4:

1. identificazione della prova digitale o del supporto da analizzare,
2. acquisizione/formazione della copia forense,
3. analisi dei risultati e valutazione,
4. rappresentazione finale dei risultati dell'indagine forense con il report finale.

Va sottolineato che i software di analisi forense consentono, come primo *step,* la creazione di una copia forense del supporto preso in esame, vale a dire che verrà creata una copia perfettamente identica all'originale evitando in tutti i modi l'alterazione o la modifica del supporto originale. La corretta esecuzione di questo step viene garantita dal calcolo di due algoritmi di calcolo[1] del "*numero hash"*.

Tale numero, univoco per ogni settore e per l'intera "*digital evidence*" (così si chiama la prova originale dalla quale andremo ad ottenere la "*forensic copy*") *potrà* e *dovrà* essere confrontato con il *numero hash* che l'investigatore digitale otterrà ad ogni apertura/avvio della copia forense. Attenzione: *questi due numeri dovranno sempre essere esattamente identici, a garanzia della inviolabilità del dato originale, ottenuto in modalità automatica al momento della formazione della copia forense* ed *il mantenimento della caratteristica forense durante tutte le future attività di recupero, ricerca e analisi di dati sulla copia forense che verrà elaborata con l'uso di Tools di analisi PC forensic, siano essi di natura Free come CAINE, Helix, DEFT, oppure di natura commerciale, a pagamento, come EnCase, FTK, X-Ways Forensic, ecc.*

Queste garanzie, universalmente riconosciute ed accettate da quasi tutte le Corti di Giustizia, sono di natura industriale, cioè costruite in tal modo all'origine dalla fabbrica, testate da istituti di misura esterni al mondo giudiziario, permettendo così di considerare attendibili al 100% i risultati estrapolati che trovano impiego nell'interno del processo giuridico sia penale che civile.

[1] MD5 e/o SHA1

L’investigatore digitale, con l'analisi scrupolosa della copia forense sarà in grado di recuperare i dati cancellati nelle aree normali ed in quelle non utilizzate dal dispositivo, quindi catalogare, valutare e confrontare qualsiasi “azione umana” effettuata sul dispositivo di memoria analizzato.

Il processo investigativo di analisi computer forensic è generalmente lungo, meticoloso e comporta conoscenze informatiche approfondite in quanto, spesso, è importante comprendere in anticipo il contenuto dei codici telematici ed informatici di un dato documento. Esso può infatti spiegare e/o provare la presenza o no di un dato soggetto in un dato luogo a seconda che il documento sia stato inviato da un dispositivo fisso oppure mobile. E a quel punto stabilire se quanto trovato è da considerarsi una prova a carico o a discarico dell’assistito ovvero, dell’indagato.

È evidente che quanto detto rappresenta la esatta collocazione dei dati e codici riservati, per cui, nel caso l'Operatore sia dipendente di un'Agenzia Governativa o Consulente Tecnico nominato dall’Autorità Giudiziaria, ottenere tali dati per Motivi di Giustizia sarà automatico. Nel caso invece, l'operatore sia un Consulente Tecnico di Parte, incaricato di condurre accertamenti per Indagini Difensive, l'ottenimento dei dati sarà sottoposto all'autorizzazione del Giudice titolare dell'Indagine su istanza dell'Avvocato che ha incaricato il C.T. di Parte medesimo.

Le macro aree basilari in cui l’investigatore digitale svolge la sua attività sono:

a) Aree di Intelligence
b) Area Giudiziaria
c) Litigation Support e Indagini Difensive
d) Area Corporate.

DUE CASI A CONFRONTO, CASO NR. 1:
INDAGINE DIFENSIVA E C.T. DI PARTE
A FAVORE DI DUE FUNZIONARI DI UN COMUNE

Trattasi di un caso realmente avvenuto e concluso a favore dei clienti difesi in collaborazione con lo studio legale che ha conferito l'incarico di indagini difensive e di C.T. di parte ai fini difensivi.

La Procura della Repubblica competente aveva delegato la P.G. promotrice, dal punto di vista di spunto investigativo, della N.D.R. (notizia di reato) al sequestro di quasi tutti i personal computer in uso ai dipendenti del Comune XY.

Il C.T. di parte veniva coinvolto immediatamente dopo questa fase dell'Inquirente.

Di comune accordo con lo studio legale e con gli indagati abbiamo atteso che il C.T. nominato dal P.M. eseguisse tutte le attività tecniche – investigative e che la Procura potesse procedere al dissequestro degli strumenti informatici.

In effetti, dopo pochi giorni la Procura della Repubblica ha ordinato il dissequestro dei suddetti pc.

L'attività difensiva e la relativa Consulenza Tecnica di parte si è potuta avviare, ma non conoscendo l'Iter tecnico – investigativo seguito dal C.T. nominato dal P.M., come ad esempio quali PC siano stati analizzati in modalità forense e con quali risultati ottenuti, ciò dovuto ovviamente al segreto istruttorio che verrà poi sciolto a chiusura delle indagini preliminari, si è proceduto come di seguito:

1. Copia forense di tutti i PC sequestrati e poi riconsegnati all'ente proprietario;

2. Uso di sistema Hardware e Software forense con blocco di scrittura fisico, in questo caso era stato scelto il Fastbloc FE ed il software forense Encase V.4 della Guidance Software Americana.

3. I PC originali sono stati immediatamente riconsegnati all'ente al fine di garantire l'immediata operatività lavorativa.

4. Le copie forensi immodificabili sono state prodotte in duplice copia al fine di garantirne la sicurezza del data storage.

A questo punto si è attesa la risposta d'ufficio del P.M. su indicazione del C.T. incaricato, risposta che puntualmente è arrivata allo scadere dei sei mesi.
Questi indicava nella sua consulenza tecnica il richiamo a dati presenti ed incrociati dal Server Linux della Gestione Oracle del Protocollo informatico dell'ente. Dati i tempi stretti concessi dall'avviso della conclusione delle indagini preliminari ex art. 415 bis del C.P.P., abbiamo immediatamente concordato e proceduto alla copia forense dell'Hard Disk SCSI III del Server Linux del Comune di(omissis).
A seguito di questa ulteriore attività forense condotta a scopi difensivi, abbiamo potuto valutare e confutare le conclusioni tratte dal P.M., a sua volta giuntovi a seguito delle risultanze e delle conclusioni delle attività tecnico – investigative condotte dal C.T. incaricato, il quale aveva proceduto all' analisi della copia dati del backup dati del Server Linux.
Non si sapeva per quale motivo il C.T. incaricato avesse svolto le suddette attività forensi limitandosi ad "analizzare" il backup dati del Server Linux.
La copia forense prodotta dal Team di difesa, creata in modalità immodificabile, ha consentito di effettuare il contro-esame giudiziario in maniera puntuale, potendo così confutare le conclusioni del C.T. incaricato dal P.M., il quale erroneamente concludeva che quella precisa operazione di inserimento di protocollo fosse avvenuta fuori dall'orario di lavoro.
Il termine primario di paragone forense che si ottiene realizzando la copia forense immodificabile in modo corretto è la comparazione tra le date e orari del cosiddetto PC-Target e quello del PC-Forense: nel nostro caso la differenza era di **49** minuti esatti.
La conclusione è stata che il richiamo della maschera d'inserimento di protocollo attraverso il PC dell'indagato è stato eseguito in orario di lavoro e non fuori da questo ambito spazio-temporale che sarebbe stato considerato anomalo e/o sospetto.
A questo punto il sottoscritto C. T. di parte ha evidenziato il fatto nella propria consulenza tecnica elaborata per lo studio legale di difesa il quale a sua volta ha

potuto chiedere e ottenere l'archiviazione delle accuse a carico dei propri assistiti.

Di seguito alleghiamo la Consulenza Tecnica, con i dati identificativi cancellati per motivi di Privacy:

CONSULENZA TECNICA DI PARTE:

Spett. le
1.1.1 *STUDIO LEGALE*
[*omissis*]
[*omissis*]

Rif. P.P. N. [*omissis*] R.G.N.R. Procura della Repubblica di [*omissis*].

Egr. Avv. [*omissis*],

Il giorno [*omissis*] a seguito di convocazione diretta, al sottoscritto veniva conferito incarico per investigazioni difensive, dall'Avv. [*omissis*] del Foro di [*omissis*], con riferimento al Procedimento Penale Nr. [*omissis*] R.G. della Procura di [*omissis*], a carico dei Sigg. [*omissis*] e [*omissis*].

Presi accordi sulla linea difensiva e sugli atti da compiere, si decideva di procedere alla "copia forense" dei dati contenuti nei Personal Computer sequestrati dalla Polizia Giudiziaria, al momento a scopo precauzionale per future attività di analisi tecnico-investigativa, esame ed eventuale contro esame giudiziario, nei tempi e nei modi da valutare e decidere al momento opportuno.

Dette attività venivano effettuate nelle date 10-11-12-13 [*omissis*] ed il [*omissis*] presso il Comune di [*omissis*], con l'uso del programma EnCase Forensic Edition Versione 4 che il sottoscritto conosce approfonditamente a seguito di corsi di addestramento, aggiornamento e fornitura e supporto alle FF.OO. ed alle Autorità Giudiziarie italiane, con il supporto della società InSide S.r.l. di Porto Recanati.

Il metodo di acquisizione e di analisi dei supporti informatici utilizzato dallo scrivente, EnCase Forensic Edition, garantisce la non alterazione dei dati originariamente presenti nel supporto stesso e consente al tempo stesso la conservazione dell'evidenza di prova per eventuali approfondimenti di natura Tecnico - Investigativa da effettuarsi in via immediata e/o successivamente, nonché la natura forense di prova cosiddetta provata.

Si precisa altresì che tali strumenti sono conformi alle disposizioni emanate al riguardo dalle maggiori Agenzie Governative U.S.A., Europee e dalle relative Corti di Giustizia competenti, con particolare riguardo alla non alterazione del dato informatico ed alla non ripudiabilità dell'evidenza di prova. Il Software EnCase della Guidance Software Inc. di Pasadena – California.

Dall'esame della relazione del Sig. [*omissis*], C.T. nominato dal P.M. e dalla comparazione delle attività compiute, emergono i seguenti dati inconfutabili:

1. Vero è che nella lista della registrazioni della tabella [*omissis*] contenente l'intestazione del protocollo, si trova, alla stringa corrispondente al nr. [*omissis*] "[*omissis*]", la riga relativa all'**identificativo** [*omissis*] collegato al protocollo numero "[*omissis*]", è stata effettuata il giorno [*omissis*] [Cfr. Pagina 2 di 4, voce "1. Allegato 1)"].

2. Vero è che nella lista delle registrazioni della tabella [*omissis*] (e non [*omissis*]) si possono visualizzare i mittenti ed i destinatari dei documenti protocollati.

3. Vero è che nella cartella [*omissis*], la riga relativa all'identificativo [*omissis*] indica che l'inserimento del protocollo numero "[*omissis*]" è stata effettuata alle ore [*omissis*]. Vero è anche che detto orario corrisponde a quello indicato dal "Server" Linux della rete informatica-telematica interna del Comune di [*omissis*]: questo orario è "immodificabile" da qualunque utente, di fatto ciò è possibile unicamente operando in maniera diretta sul PC - Server e da personale con elevate conoscenze tecnico-informatiche oltre che l' "ID" e "Password" per potervi accedere.

4. Vero è che da questa lista presente nel PC-Server descritto, si può agevolmente rilevare che l'operazione seguente a quella compiuta alle ore [*omissis*] del [*omissis*], è quella effettuata nel giorno seguente, il [*omissis*] alle ore [*omissis*].

5. Non è vero che la registrazione del protocollo nr. [*omissis*] è avvenuta, come dichiara il C.T.: "*l'operazione è stata effettuata alle* **ore** [*omissis*]" (pagina [*omissis*] della sua relazione) e ne', come si legge testualmente alla pagina 3 di 4 penultimo capoverso, della sua relazione tecnica: "*Per cui la registrazione del protocollo numero* [*omissis*] *è avvenuta effettivamente in data* [*omissis*] *verso* **le ore** [*omissis*]", in quanto quell'orario corrisponde all'accesso al PC-Server dall'utente identificabile come "(USER=[*omissis*]), come si può bene evincere **nell'allegato 4**, alla pagina [*omissis*] penultima riga, sempre della relazione tecnica depositata dal Consulente Tecnico del P.M., non necessariamente implicante l'operazione di registrazione, così come prospettato dal C.T., anche in considerazione del fatto che l'impiegato in questione, per quanto consta al deducente, non aveva alcuna specifica competenza in materia di gestione del Protocollo del Comune di [*omissis*].

6. A riprova di quanto sopra detto, si allega il documento nr. [*omissis*], estratto dai documenti presenti nel fascicolo, "XXXXXX.: [*omissis*], dal quale si può rilevare che detto *utente* [*omissis*] (User: [*omissis*]) nel giorno [*omissis*] è *entrato* al lavoro alle *ore* [*omissis*] ed è *uscito* alle *ore* [*omissis*].

7. Ad ogni buon conto, l'orario del P.C. Server Linux del Comune di [*omissis*] è impostato di *49 minuti in avanti*. Ciò è rilevabile dal rapporto di acquisizione forense, che alleghiamo alla presente, in cui al momento dell'acquisizione – copia forense integrale dei dati di detto P.C. - Server, abbiamo potuto riscontrare che l'orario qui pre-impostato corrispondeva alle ore 05:05:23 del pomeriggio del 15 [*omissis*], mentre l'orario effettivo

era corrispondente alle ore 04:16:23, sempre del pomeriggio del [*omissis*]. Lo scrivente ha potuto constatare direttamente quanto sopra detto, alla presenza di altre persone.

Dall'esame delle copie forensi dei computer acquisiti, abbiamo rilevato i seguenti dati di rilievo, utili all'indagine:

a) Dal PC Server Linux, acquisito il [*omissis*]: vi è una differenza di impostazione di orario del server a differenza di quello reale di 49 minuti. Il risultato è che, ad esempio, quando il Software Oracle presente nel Server Linux imprime nel suo file di Log che sono le ore 14:46,17, di fatto sono le ore 13:57,17, e quando si rileva le ore 14:36, da qui dobbiamo tornare indietro di 49 minuti, e sono esattamente le ore 13:47.

b) Dal PC in attuale uso all'Utente [*omissis*], di fatto in uso al [*omissis*] al tempo del [*omissis*], abbiamo rilevato che il file denominato "[*omissis*].", contiene al suo interno il documento di cui trattasi il cosiddetto "Pseudo-Protocollo [*omissis*] del [*omissis*]". Dall'analisi della "Timeline" caratteristica della tipologia di Sistemi Operativi Windows, del quale con il SW EnCase possiamo verificare le date di creazione, ultima modifica, ultimo accesso ed eventuale cancellazione di un file in esame, abbiamo riscontrato che l'ultima modifica "storica" apportata a questo file è stato il [*omissis*] alle ore 11:17:56, mentre l'ultima stampa di questo file è stata effettuata nel giorno medesimo alle ore 11:00:00.

c) All'uopo si allega fotografia dei dati presenti ed estrapolati dal normale comando di Word di Windows, dove si evidenziano i dati descritti alla voce precedente, "b".

d) Sono state effettuate delle ricerche mirate sugli spazi "Unallocated Clusters" nella copia forense del PC-Server Linux, e si sono evidenziati i seguenti risultati di riscontro:

   1. si sono evidenziati risultati inequivocabili della presenza delle tracce di registrazione, degli oggetti e dei protocolli corrispondenti a numeri prima e dopo al Protocollo nr. [*omissis*].

   2. Le tracce dell' oggetto, collegato al numero di protocollo [*omissis*], sono stati rinvenuti (quello collegato alla lettera recante l'oggetto "offerta di collaborazione tecnica per la richiesta di finanziamento…" dell'[*omissis*]).

   3. *Le tracce* informatiche-telematiche interne alla rete, dell'ipotizzato *Protocollo* [*omissis*], (quello collegato alla lettera recante l'oggetto: "[*omissis*]" ricercato in varie forme, *non sono state rilevate*).

Lo scrivente ritiene opportuno sottolineare che questa è una ricerca compiuta e mirata a verificare, come ipotizzato dall'Inquirente, in caso di inserimento di un

primo protocollo [*omissis*] con uno specifico Oggetto, se ciò fosse avvenuto, si sarebbero rinvenute le tracce di almeno nr. 2 Protocolli [*omissis*] con 2 rispettivi e differenti Oggetti di Protocollo.
Il programma ORACLE installato nel server [investigato con l'analisi delle copie forensi ottenute] per mezzo del quale viene registrato il flusso cartaceo della posta in entrata e quella in uscita (operazione di protocollo), come tutti i programmi di elaborazione di dati, nei momenti di elaborazione crea dei files di elaborazione temporanea.

Detti files temporanei, vengono normalmente utilizzati come una matrice di dati volatile, ricca di dati da rielaborare, dove altrettanto normalmente sono essi stessi frutto di elaborazioni più o meno complicate dei dati di origine. Una volta giunti all'elaborazione finale e successivamente salvati, i dati contenuti in questi files temporanei vengono automaticamente "cancellati" dallo stesso programma, in quanto non necessita più di passaggi intermedi ma ha già realizzato l'elaborazione finale.

Questi files temporanei, prima di essere trasformati agli occhi del sistema come spazio vuoto e riscrivibile, vanno ad occupare temporaneamente solo gli spazi vuoti dell'Hard Disk.
Nell'HDA3 del server Linux, ovvero la partizione dell'hard disk contenente il programma di elaborazione gestionale ORACLE, attraverso indagini approfondite sono stati rinvenuti rilevanti quantità di "unallocated clusters" ovvero spazi dell'hard disk attualmente liberi ma che in precedenza hanno ospitato dei files temporanei di elaborazione.
Tali frammenti riportano frequentemente tracce di scritti riportanti l'oggetto "comunicazione di servizio", ma risultano preceduti o avvicinati da numeri di protocollo totalmente estranei al [omissis], oppure in altri casi la parola chiave di ricerca "comunicazioni di servizio" è solo una parte dell'oggetto, es. "*comunicazione* [omissis]*:* **"**[omissis]" evidentemente non collegati al protocollo in questione.

Negli stessi casi citati in precedenza, come esempio l'oggetto del protocollo immediatamente prima a quello contenente il frammento "comunicazione di servizio", e sia quello immediatamente dopo, non sono simili a quelli riportati prima e dopo l'oggetto di protocollo contestato, presenti nella lista di protocolli estratti dalla tabella "[*omissis*]" e prodotti nell'allegato 1 presentato dal consulente tecnico [*omissis*], nominato dal P.M.

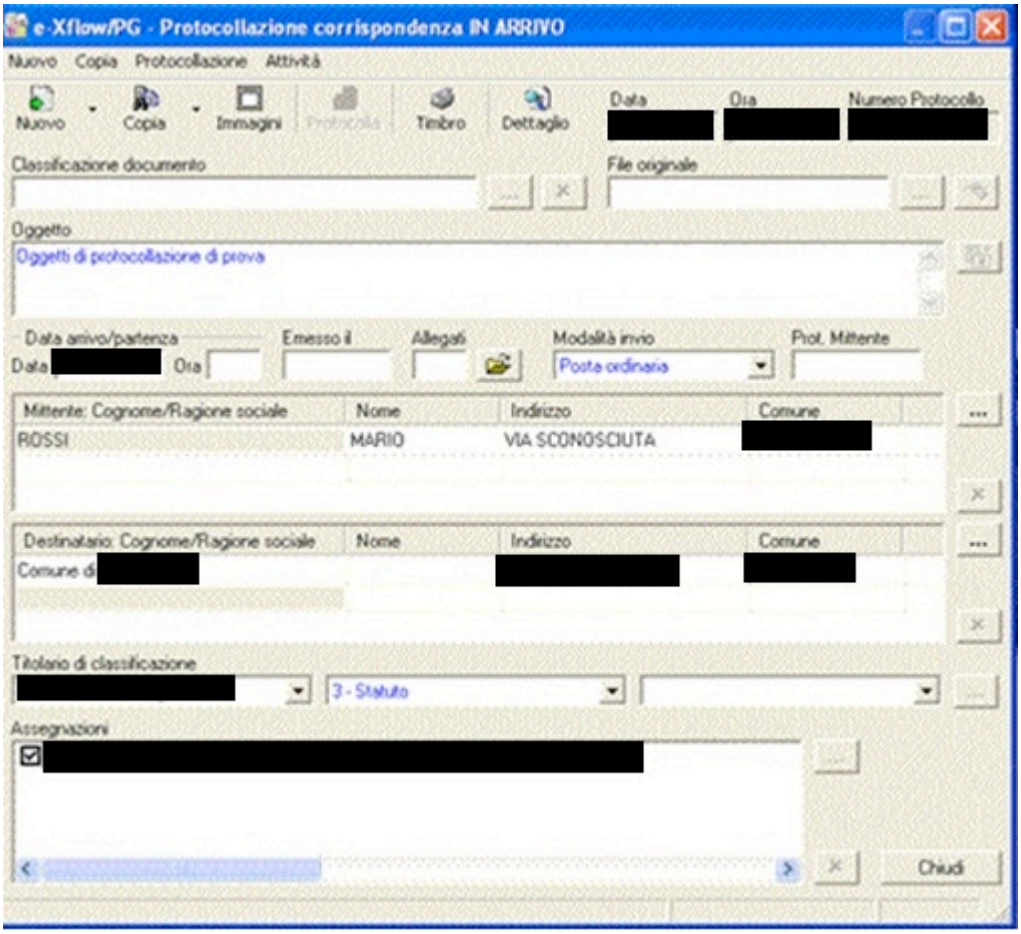
I medesimi frammenti di informazione di cui sopra, presentano ciclicamente il medesimo concatenamento di dati, ovvero la correlazione di dati vicina e puntuale tra un numero, il [omissis]ed il relativo oggetto: "[omissis]"
Relazionando questo concatenamento di dati in un contesto più ampio, la dicitura appartenente al protocollo "[omissis] ai sensi del D.P.R. 10.03.1998 n°76" non solo viene spesso immediatamente preceduta dal numero [omissis]come poc'anzi detto, ma viene anche immediatamente preceduta da un'altra dicitura "Lavori [omissis]", che a sua volta è preceduta dal numero [omissis].

Lo stesso oggetto del protocollo [*omissis*]viene costantemente seguito dal numero [*omissis*], che a sua volta viene seguito dalla dicitura "[*omissis*]- presa di servizio il [*omissis*]", confermando la sequenza di inserimento protocolli riportata nell' Allegato 1 della relazione tecnica del C.T. nominato dal P.M., Sig. [*omissis*].

Si evidenzia, infine, il rilevamento di numerose tracce di concatenamento sequenziali riportanti solo gruppi di scritte, senza essere precedute da numeri. All'interno di questi gruppi è possibile notare la costante consequenzialità tra le scritte: "[*omissis*]", "[*omissis*]ai sensi del D.P.R. 10.03.1998 n°76" e "[*omissis*]", probabilmente frutto di azioni di elaborazione automatica diversa rispetto a quelle che hanno generato le stringhe di testo contenenti anche i numeri di protocollo.

e) CHIARIMENTI DEL FUNZIONAMENTO PROTOCOLLO [omissis]

I dati della scheda del protocollo vengono memorizzati nella tabella [omissis], la quale è collegata mediante il campo ID alle altre tabelle [omissis] (che contiene i dati relativi ai mittenti e/o destinatari). La tabella [omissis]non contiene i dati relativi alla variazione del protocollo bensì i dati relativi allo smistamento del protocollo nei vari uffici e tale tabella è collegata alla [omissis]sempre attraverso il campo ID. Per ulteriore chiarezza illustro un esempio pratico. Carichiamo un protocollo in archivio mediante l'utilizzo del programma. Il protocollo, una volta registrato (solo con i dati necessari), si presenta nel seguente modo:



Sulla tabella [*omissis*]viene scritto quanto segue (illustro solo i dati principali per ragioni di spazio)

ID	NUMPROT	DATAPROT	ORAPROT	TIPOCOM	OGGETTO
[*omissis*]	[*omissis*]	[*omissis*]	93336	1	OGGETTO DI PROTOCOLLAZIONE DI PROVA

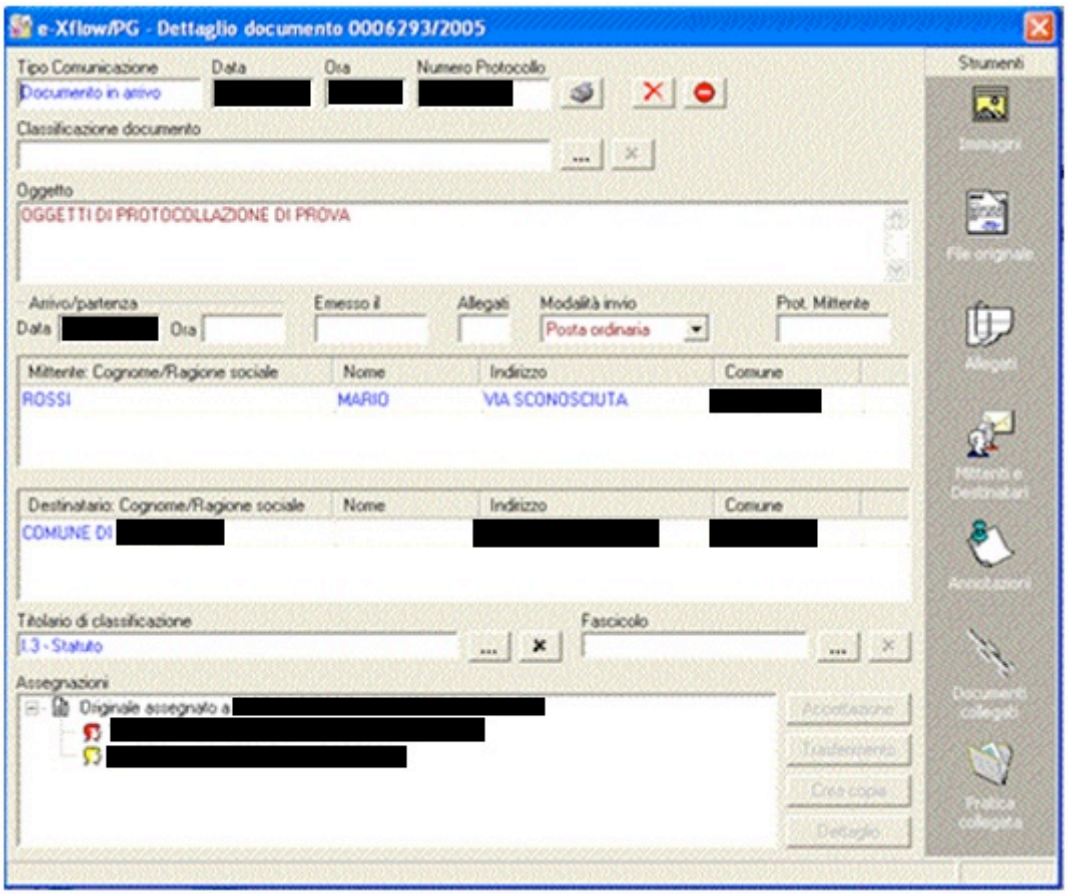
Sulla tabella PG_DREF compare invece il seguente contenuto:

IDDOC	TIPOREF	IDREF	TIPOPER	COGNOME	NOME
[*omissis*]	2	0	F	[*omissis*]	
[*omissis*]	1	[*omissis*]	F	[*omissis*]	[*omissis*]

Sulla tabella [*omissis*]in questa situazione compare il seguente risultato

IDDOC	NUMCOPIA	DATAINI	ORAINI	DATAEND	ORAEND	CODFUNZASS	TIPOTRASF
[*omissis*]	0	[*omissis*]	[*omissis*]	0	-1	138	

Facciamo il caso adesso che [*omissis*] (a cui è stato destinato il documento originale) invii il documento per visione a [*omissis*]. Quindi richiamando il protocollo la maschera si presenterà nella seguente maniera:



In seguito a questa operazione le tabelle [*omissis*] e [*omissis*] risulteranno completamente invariate mentre la tabella [*omissis*] subirà la seguente variazione:

IDDOC	NUMCOPIA	DATAINI	ORAINI	DATAEND	ORAEND	CODFUNZASS	TIPOTRASF
[*omissis*]	0	[*omissis*]	100606	0	-1	102	0
[*omissis*]	0	[*omissis*]	93336	[*omissis*]	100606	138	

In conclusione la tabella [*omissis*] registra solo l'assegnazione del documento già protocollato da un ufficio all'altro.

Per quanto riguarda il file di oracle OPT\Oracle\app\product\8.1.7\network\log\[*omissis*], questi registra tutti gli accessi che un eseguibile effettua al database, sia in modo diretto (accedendo al database) sia in maniera indiretta (ad esempio apro il programma del protocollo per effettuare una consultazione).

f) dalle ricerche effettuate nel PC "Uff. Protocollo [omissis]", sono emersi una lunga serie di File ".TMP", file temporanei che il sistema Windows crea automaticamente. Nei file evidenziati in giallo nei tre fogli corrispondenti ai nr. 17-18 e 19, dal nr. [omissis], si possono notare i file temporanei creatisi durante la giornata del [omissis]. L'ultimo di questo file porta l'ora 01:01:34 e facendo attenzione ai dati di acquisizione riportati nel foglio nr. 1 di questo allegato, dell'acquisizione-copia forense del PC Utente [omissis], l'orario di è corrispondente a quello vero, senza alcuno sfasamento di ora.

Porto Recanati, [*omissis*].

I.P.- C.T. *Emilio Luchetta*

ALLEGATI:

Si allegano i seguenti documenti:

I. Dati relativi all'acquisizione-copia dati forense e risultati di analisi Tecnico-Investigativa del PC Utente [*omissis*] e PC [*omissis*], rilegati insieme.

II. Dati relativi all'acquisizione-copia dati forense e risultati di analisi Tecnico-Investigativa del PC Server Linux del Comune di [*omissis*].

III. Dati relativi all'acquisizione-copia dati forense e risultati di analisi Tecnico-Investigativa del PC Utente [*omissis*]- Ex Utente [*omissis*].

IV. Dati relativi all'acquisizione-copia dati forense e risultati di analisi Tecnico-Investigativa del PC Utente [*omissis*], dalla pagina 1 alla pagina 632.

V. Dati relativi all'acquisizione-copia dati forense e risultati di analisi Tecnico-Investigativa del PC Utente [*omissis*], dalla pagina XXX alla pagina XXXX.

VI. [*omissis*], documento originale rinvenuto nel PC in uso attuale all'Utente [*omissis*], a quel tempo in uso all'Utente [*omissis*], rinvenuto a seguito di ricerca e analisi forense mirata, esportato integralmente e così stampato, allegato ai documenti alla voce "xxx";

VII. [*omissis*], idem come sopra, come visibile da livello di memoria con il sistema di analisi di PC, il Sofware EnCase, allegato ai documenti alla voce "xxx" .

VIII. Documento di Foglio elettronico "Excel", contenente il totale dei file presenti e visualizzabili con Word di Windows, ed anche tutti i File temporanei dei

medesimi, qui salvati in automatismo dal Sistema Operativo in uso. Si precisa che quelli evidenziati in giallo sono "visionabili" normalmente, tutti gli altri sono considerati "Unallocated Clusters" dal Sistema Operativo Windows: quelli infine evidenziati in verde, alle pagine 4 e 5, rappresentano le attività formulate dall'utente nel suo PC in uso, nei giorni [*omissis*], allegato ai documenti alla voce "xxx".

IX. Fotografia informatica delle Proprietà del file "[*omissis*]", allegato ai documenti alla voce "xxx" (Allegato anche alla presente relazione tecnica).

X. Copia del "Report" di acquisizione del Server Linux del Comune di [*omissis*], avvenuta il [*omissis*], con le note esplicative relative all'orario pre - impostato, di 49 minuti in avanti, allegato ai documenti alla voce "II" (Allegato anche alla presente relazione tecnica).

XI. Foglio "Excel", rappresentante l'elenco dei File Temporanei rinvenuti a seguito di ricerca, nel PC Utente [*omissis*], allegato ai documenti alla voce "I", nei dati di pertinenza "PC Utente [*omissis*]".

Name: TecnoGeneral Suse Server 2 Quantum SCSIIII
Description: Physical Disk, 35880960 Sectors, 17,1GB
Logical Size:
Physical Size: 512
Starting Extent: 0S0
File Extents: 1
Physical Location: 0
Physical Sector: 0

2 Evidence File: TecnoGeneral Suse Server 2 Quantum SCSIIII

Full Path: [omissis]\TecnoGeneral Suse Server 2 Qu SCSIIII
File Extents

Start Sector	Sectors	Start Clus	Clusters
1			

Device
Evidence Number: [omissis]
File Path: D:\ [omissis]\ [omissis
Examiner Name: Luchetta
Actual Date: 03/15/XX 04:16:23
Target Date: 03/15/XX 05:05:23
Total Size: 18.371.051.520 bytes (17,1GB)
Total Sectors: 35.880.960
CHS: 1023:255:63
File Integrity: Completely Verified, 0 Errors
EnCase Version: 4.20
System Version: DOS 7.10
Acquisition Hash: EB5A507092FC06A48B270D2C0160xxxx
Verify Hash: EB5A507092FC06A48B270D2C0160xxxx
Notes: Scsi raid su scheda Mylex AcceleRaid 170

Partitions

Code	Type	Start Sector	Total Sectors	Size
83	Linux EXT2	0	48.195	23,5MB
82	Linux Swap	48.195	1.317.330	643,2MB
83	Linux EXT2	1.365.525	34.507.620	16,5GB

NOTE:

- Per "Actual Date" si intende la data corrente in cui è stata effettuata la COPIA FORENSE dell'Hard Disk Server Linux del Comune di [omissis].

- Per "Target Date" si intende la data settata nel Server Linux del Comune di [omissis].

CONCLUSIONI:

- Da quanto sopra detto si evince che l'orario del Server Linux, che è il sistema che appone in automatico la data sul file di inserimento dati al momento che l'Utente Periferico effettua operazioni tipo quella interessata, è, per così dire, in "AVANTI" di 49 minuti esatti.

- Nel Server Linux del Comune di [omissis]si trova il Sistema Operativo Linux SUSE, del quali i tecnici della Ditta [omissis] che hanno effettuato il settaggio originale, dichiarano che non prevede l'automatismo di cambio automatico dell'ora, da quella SOLARE all' ora LEGALE.

COMMENTI DEL CASO:

Quello appena concluso e allegato rappresenta un tipico caso forense trattato per indagini difensive.

In sostanza le tecniche usate dal nostro Team investigativo e dal C.T. nominato dal P.M. sono identiche, come identico è l'iter della ricerca dei supporti e poi della formazione della copia forense con sistemi di salvaguardia e tutela dei dati originali, quindi dell'analisi forense e, infine, della relazione tecnica con la rendicontazione dei risultati ottenuti.

DUE CASI A CONFRONTO, CASO NR. 2: INDAGINE AZIENDALE INTERNA AL FINE DI IDENTIFICARE L'ANONIMO UTENTE CHE CANCELLAVA DATI DAL SERVER AZIENDALE E VI POSTAVA IMMAGINI PORNO.

Queste tecniche sono state adottate in entrambi i casi trattati. Questo secondo caso tratta di un'attività condotta circa 10 anni fa a favore e su richiesta di un'azienda con oltre 400 dipendenti, con una forte presenza sindacale interna. Il problema era la ricezione di attacchi al server aziendale da persone ignote con problemi conseguenti principalmente dal rischio della perdita o della cancellazione di dati e, ovviamente, della buona immagine dell'Azienda.

Da non trascurare inoltre il fatto che il o i soggetti che commettevano queste azioni criminose si preoccupavano sempre di operare, in modo diretto o indiretto che poi scopriremo, da postazioni informatiche di impiegati che in quel momento non si trovavano al loro pc oppure erano assenti.

Le fasi operative sono state condotte agendo alla ricerca delle tracce dei file postate nel server aziendale procedendo su gruppi di client di circa un terzo dei totali alla volta.

Nella terza fase di lotto di client, prima copiati poi analizzati, alla ricerca delle suddette tracce abbiamo potuto concludere che il o i soggetti agivano senza fare uso del proprio computer di ufficio.

La soluzione del caso è stata ottenuta e preparata a dovere, in concomitanza della consegna di un computer portatile ad un nuovo funzionario assunto: il sospetto, che poi accertammo essere una singola persona, non resistette ad infettare il computer portatile del suo nuovo collega impiegato, inserendovi immagini pornografiche di varia natura.

Il riscontro forense si ottenne dall'averlo lasciato come unica forza lavoro presente in azienda nell'esatto momento della violazione del pc portatile suddetto.

La prova si acquisì dall'incrocio dei dati relativi alle presenze con, ovviamente, i tempi e le modalità di accesso abusivo al pc portatile in seguito identificato, copiato in modalità forense e dal quale vennero estrapolati i dati a seguito di opportuna analisi forense.

In conclusione il Consulente Tecnico poté porre l'azienda in condizione di scegliere la soluzione legale più adeguata al caso, tra le seguenti:

1. Denunciare il dipendente infedele all'Autorità Giudiziaria in via penalistica;
2. Denunciare il dipendente infedele all'Autorità Giudiziaria in via civilistica e del diritto del lavoro;
3. Trattare il caso in via stragiudiziale con il coinvolgimento dei sindacati di categoria.

L'azienda optò per la terza soluzione e, anche su consiglio del C.T., una volta ottenute le dimissioni volontarie del dipendente infedele, il giorno seguente riassunse il dipendente a tempo indeterminato con mansioni non più di livello impiegatizio ma in qualità di operaio.
Come disse Napoleone nel modus di trattamento dei soldati, bisogna punirne uno per educarne mille.

Di seguito alleghiamo la relazione tecnica oscurata nelle parti non citabili con "omissis" per motivi di Privacy.

CONSULENZA TECNICA DI PARTE:

Spett.le
[*omissis*] **S.p.A.**
Via [*omissis*]
[*omissis*]

Oggetto: Trasmissione di relazione da **Analisi Tecnico-Investigativa** effettuata per Vostro nome e conto su **supporti di massa (dischi rigidi)**, di una parte dei PC acquisiti presso la Vostra Sede ed analizzati con tecnologie Forensi avanzate.-

3 RAPPORTO FINALE

Spettabile Direzione,

Premesso che,

A seguito di contatti e relativi accordi, vedi nostra del 28 [*omissis*]2002, siamo stati chiamati ad esprimere un parere professionale a seguito di reiterati attacchi informatici e telematici al Vostro sistema informatico strutturato in rete aziendale (LAN Aziendale), dei quali non si era a quel tempo riusciti ad individuare chi, come, da dove, quando avesse effettuato le seguenti azioni delittuose:

- AVER CARICATO ABUSIVAMENTE, DA PARTE DI IGNOTI, SUL SERVER DELLA LAN AZIENDALE, CARTELLE E FILES CONTENENTI IMMAGINI E FILMATI PORNOGRAFICI, GIOCHI COPERTINE PER "CD", OLTRECHE' INTERE RACCOLTE DI FILES IN FORMATO "MP3" CON LA CONSEGUENTE OCCUPAZIONE DI CENTINAIA DI MEGABYTES DI SPAZIO SUL SERVER

- AVERE EFFETTUATO DA PARTE DI IGNOTI, RIPETUTI ACCESSI ABUSIVI E CONTINUATI ALLA LAN AZIENDALE (PERIODO STORICO 2001 ED ULTIMO EVIDENTE ATTACCO DIRETTO AL SISTEMA LAN E RELATIVE CARTELLE DI AMMINISTRAZIONE)

- AVERE EFFETTUATO DA PARTE DI IGNOTI, RIPETUTI ACCESSI ABUSIVI E CONTINUATI AI P.C. DEI SINGOLI OPERATORI

Dopo una approfondita analisi e colloqui con le Vostre maestranze e considerato che non eravate in grado di identificare da chi e a dove queste azioni delittuose venivano perpetrate (se dall' interno o dall' esterno dell'Azienda via modem o via Internet),
Vi abbiamo indicato la possibilità di procedere all'analisi forense TECNICO-INVESTIGATIVA di TUTTI I SUPPORTI DI MEMORIA DI MASSA (dischi rigidi) dei singoli operatori.

Il metodo di acquisizione e di analisi dei supporti informatici utilizzato dalla scrivente, GARANTISCE LA NON ALTERAZIONE DEI DATI ORIGINARIAMENTE PRESENTI SUL SUPPORTO STESSO, E CONSENTE AL TEMPO STESSO LA CONSERVAZIONE DELLA EVIDENZA DI PROVA PER EVENTUALI APPROFONDIMENTI TECNICO-INVESTIGATIVI DA EFFETTUARSI SUCCESSIVAMENTE.

PRECISIAMO CHE TALI STRUMENTI SONO CONFORMI ALLE DISPOSIZIONI EMANATE AL RIGUARDO DALLE MAGGIORI AGENZIE GOVERNATIVE U.S.A. , EUROPEE E RELATIVE CORTI DI GIUSTIZIA, CON PARTICOLARE RIGUARDO ALLA NON ALTERAZIONE DEL DATO INFORMATICO E ALLA NON RIPUDIABILITA' DELLA EVIDENZA DI PROVA.

A seguito dei nostri accordi, abbiamo proceduto con l'acquisizione del primo gruppo di supporti di memoria di massa dei primi 5 PC della LAN, il 9 febbraio [*omissis*].

A fronte della elaborazione tecnico-investigativa dei supporti acquisiti, al fine di recuperare i dati cancellati, la organizzazione e l'incrocio con gli altri rilevati e quindi, abbiamo chiesto ed ottenuto dalla S.V. di riaccedere ai Vostri locali per acquisire la parte condivisa del disco "C" del server; ciò lo abbiamo effettuato, sempre in Vostra presenza, il giorno 11 maggio [*omissis*].-

Da questa acquisizione, da noi denominata "[*omissis*]" e relativa analisi approfondita non sono emersi ulteriori dati utili alle investigazioni, anche perché, come abbiamo appreso poi da Voi, la Ditta che effettua il servizio della manutenzione della Vostra LAN Aziendale aveva proceduto qualche giorno prima dell'11 maggio alla cancellazione delle cartelle oggetto di verifica.
Dal punto di vista della Acquisizione ed Analisi Forense, abbiamo considerato il fatto che il Vostro server utilizza Hard Disk in Raid.
Questo significava un costo molto oneroso da sostenere per la acquisizione dei dati:
valutato il tutto abbiamo deciso di comune accordo di non procedere in questa direzione.

Il 29 maggio [*omissis*]dopo le ore 10,00 il Dott. [*omissis*] ci ha chiamato al telefono informandoci che nel PC della vostra LAN Aziendale in uso alla Signora [*omissis*], si era verificata una INTRUSIONE INFORMATICA E TELEMATICA con la conseguente ALTERAZIONE DEL CONTENUTO DI COMUNICAZIONI INFORMATICHE, chiedendoci indicazioni sul da farsi.

Ci siamo immediatamente accordati per procedere alla verifica del relativo PC, poi denominato [*omissis*]: durante il nostro colloquio telefonico ci informavate anche che nel frattempo un Vostro collaboratore Vi aveva "stranamente" domandato ed ottenuto un permesso di uscita alle ore 15 del pomeriggio del giorno precedente. A questo punto abbiamo insieme valutato la opportunità di procedere all'analisi tecnico investigativa anche del supporto facente capo al PC in uso a questa persona.

Ci avete poi avvisato che, a seguito di questo comportamento giudicato sospetto, avendo Voi deciso di procedere alla verifica "a caldo" dei "MENU' DOCUMENTI RECENTI DI WINDOWS", è emerso che in questo PC collegato in rete LAN Aziendale è stato ritrovato un link al file abusivamente installato nel PC della Signora [*omissis*] (Evidence [*omissis*]).

Nei giorni a seguire abbiamo proseguito con il lavoro a suo tempo avviato il 9/2/[*omissis*], proseguendo nella acquisizione e poi analisi tecnico-investigativa, accedendo con la Vostra assistenza e presenza con altri PC della Vostra LAN Aziendale, i giorni 10 e 11 giugno [*omissis*].

Il giorno 15 del mese di [*omissis*] [*omissis*], dietro Vostra chiamata telefonica, abbiamo appreso che un ulteriore "ATTACCO INFORMATICO E TELEMATICO" è stato effettuato ad un PC della Vostra Azienda, ed il 16 giugno ci siamo accordati con il Dott. [*omissis*]prima e il Dott. [*omissis*]poi di procedere ad ulteriori acquisizioni della memoria di massa del PC che ha subito ciò da persona

sconosciuta, probabilmente della vostra Azienda. Cosa che abbiamo effettuato e concluso alle ore 24,00 del giorno 16/06/[*omissis*].-

Note esplicative:

1. Il primo foglio in ordine, intitolato "Encase Report" contiene i dati di acquisizione del supporto, in questo caso [*omissis*].e01, riferito al PC in uso all'operatore [*omissis*] e questa è la 2^ acquisizione effettuata sul PC in uso a questo operatore in quanto dall'Analisi effettuata abbiamo riscontrato che il soggetto evidenzia una grande tendenza a collegarsi

   attraverso la Rete LAN Aziendale a molti PC collegati, come quello in uso al Dott. [*omissis*], [*omissis*], ecc. nonché possiamo dire l'ABITUDINE all'uso delle cartelle, la creazione, la cancellazione e via proseguendo di files musicali, fotografie pornografiche ecc. sul disco "C" del Server della LAN Aziendale.-

   Alla voce "File Integrity" in cui troviamo scritto in inglese "Completely Verified", "0 errors", queste tre parole significano tecnicamente che il sistema di acquisizione a basso livello del disco rigido non è incorso in alcun errore e che è stato copiato interamente su un nostro supporto, firmato digitalmente con il sistema "Acquisition HASH" e poi un "numero" digitale lungo che rappresenta la firma digitale indelebile, attraverso un calcolo preciso, il quale corrisponde come si vede al "Verification HASH" e ciò rappresenta LA GARANZIA TECNICA INDUSTRIALE che nessuno ha modificato il contenuto TOTALE DEL DISCO C, in caso contrario il secondo numero (il Verification HASH) sarebbe stato differente dal primo (l'Acquisition HASH).

   Alla voce "Drive Geometry" troviamo l'esatta misurazione in settori del Disco rigido "C" in esame, in questo caso 16.498.944 settori.

   Alla Voce "Partitions" troviamo le partizioni logiche in cui il Disco "C" è stato "partizionato", suddiviso al momento dell'installazione originaria dei programmi di Sistema Operativo, Drives, ecc.

2. Il secondo gruppo di fogli che sono intitolati "EnCase Report" e vanno da Pagina 1 a Pagina 41, rappresenta i Parametri del Volume "C", con le relative misurazioni "logiche" e la totale elencazione delle cartelle di sistema, in uso, cancellate, contenenti sia programmi che files di vario tipo:

   - vedi nella Page 1, la 15^ cartella nella prima fila a sinistra con scritto "musica", in cui si può notare che le cartelle in esso contenute sono: "[*omissis*]", "[*omissis*]", "[*omissis*]", "[*omissis*]", "[*omissis*]", "DISK-1", "DISK-2, quindi "My Music";

- vedi nella Page 1, la 19^ cartella nella 3^ fila a destra, un quadrato con una "x" dentro che sta a significare che questa cartella è stata cancellata, con la scritta a fianco "Harry Potter Creative CD", la cartella sotto e sotto ancora che rappresentano le informazioni per l'installazione e quindi il numero di matricola del CD installato;
- Analizzando e proseguendo nella visione, possiamo riscontrare tante cartelle aperte non pertinenti all'attività aziendale, come si vede a Page 11 fila a sinistra, vedi nel cerchio rosso "[*omissis*]", "[*omissis*]", "Game Boy – [*omissis*]", "[*omissis*]";
- La abitudinaria, consequenziale visitazione di cartelle in PC condivisi in qualche modo nella Rete LAN lo rileviamo a Page 4, a Page 14 e 15
- Dalla fila centrale della Page 32 in poi fino alla Page 41 di questo documento rappresentante "l'Albero delle directories del Disco C", possiamo riscontrare una serie innumerevole di otre 1.300 cartelle usate dall'utente di questo PC, poi cancellate e recuperate dal nostro sistema di analisi;

3. Il terzo gruppo di fogli intitolati "EnCase Report" Volume "D" Parameters, rappresenta graficamente l'Albero delle directories della seconda parte logica del Disco in esame, formato da 4 fogli da Page 1 a Page 4:

   - Notare la Page 1 fila di sinistra, le cartelle rappresentate con una "x" dentro un quadratino stanno a significare che dopo l'uso, trattamento informatico come la lettura, la modifica, la stampa ecc. sono state cancellate e vi troviamo le solite canzoni, FATTURE [*omissis*], SERVIZI ANNO [*omissis*], SERVIZI ANNO [*omissis*]E CODICI DI [*omissis*], SUBITO SEGUITI DA "[*omissis*]", "[*omissis*]PRETA", "[*omissis*]", "[*omissis*]", "[*omissis*]" CON SUB-CARTELLE "DISK-1" E "DISK-2";
   - Notare nella Page 2 nella fila di sinistra in basso dove ritroviamo oltre alla presunta stampa dell' " [*omissis*]" come Sotto-cartella del "[*omissis*]", dentro al "FOLDER020" ritroviamo cancellati i nomi del calendario con inizio AGOSTO e fine SETTEMBRE che ritroviamo anche in altra parte dell'analisi, presumibilmente inviati alla propria stampante e poi opportunamente cancellati;

4. Nei 6 gruppi di fogli a seguire troviamo:

   - il primo numerato da 1 a 60, la Cronologia dei Link, delle "connessioni" via LAN aziendale compiute da questo PC. Sono tutte rilevanti al fine di stabilire che da questo PC sono partiti gli ordini di visitazione di tutti quei files-immagini hard

   - il 2° da 1 a 2, visitazione del PC_[*omissis*]

   - il 3° da 1 a 2, visitazione del PC_[*omissis*]/TLQ/test

   - il 4° da 1 a 4, visitazione di [*omissis*] cartella APPOGGIO/[*omissis*]/Documenti/Immagini/perrelazionepres/[*omissis*].jpg

ciò avvenuto esattamente alle ore 13:50:29, e poi l'operazione a seguire avvenuta sempre da questo PC alle ore 13:57:07 in cui l'utente "[*omissis*]" compie fisicamente l'azione di porre il file:///C:WINDOWS/Menu di Avvio/Esecuzione Automatica del file/[*omissis*].jpg attraverso il suo "Browser" di "Internet Explorer" presente nel Dektop del suo PC, di trasferire il detto file "[*omissis*].jpg" in un dato percorso che riscontreremo più avanti definitivamente .-

- il 5° da 1 a 20, qui si evidenziano vari collegamenti attraverso il detto PC in esame, come la voce 3,4, alla famosa cartella [*omissis*] _SERVER ed [*omissis*] _SERVER/APPOGGIO, quindi la voce 5 ad una RELAZIONE GIURATA RELATIVA AD UNA STIMA (evidentemente una cartella per così dire CONDIVISA), poi le voci 6, 7, 8, 9, 10, 13, 14, 15, 16, 17 e e 20 lasciano chiaramente rilevare le visitazioni telematiche (via Rete LAN) ed informatiche (ai rispettivi PC di [*omissis*] e [*omissis*]);

- il 6° da 1 a 31: in questo gruppo di Cronologia Storica dell'Internet Explorer usato dal PC in esame, ritroviamo altre e numerose azioni telematiche e informatiche relative ad immagini Porno, files animati, ecc.;

5. In questa pagina intitolata "PICTURES" , ritroviamo l'immagine usata alle ore 13:50:56 sul proprio PC, poi cancellata dall'utente;

6. In questa pagina troviamo la descrizione del file "[*omissis*].jpg" con la allocazione fisica di dove si trovava nel disco C del PC in esame poco prima di venire cancellato;

7. In questa pagina troviamo le tracce del LINK del file "[*omissis*].jpg"

8. In questo gruppo intitolato "TEXT FRAGMENTS", con sotto-voci che vanno da 1 a 13 possiamo individuare:
   - 8.1: frammenti di testo rinvenuti nel disco "C" del PC in esame che dimostra la residenza nel PC del file "[*omissis*].jpg"
   - 8.2: dimostra l'esecuzione del comando dal PC in esame della ESECUZIONE AUTOMATICA
   - 8.3: dimostrazione dell'accesso al PC di [*omissis*] e l'aver inviato nella cartella "[*omissis*]" il file "[*omissis*]
   - 8.4: dimostrazione dell'accesso al PC [*omissis*] ed altri;
   - 8.5: dimostrazione dell'accesso dal PC [*omissis*] a delibere e documenti del C.d'A.;
   - 8.6: dimostrazione dell'accesso dal PC [*omissis*] al PC [*omissis*] e qui
     la documentazione relativa ad appalti a [*omissis*];
   - 8.7: dimostrazione dell'accesso dal PC [*omissis*] alla cartella [*omissis*]

     _SERVER e poi riferimenti a "[*omissis*] [*omissis*].jpg" da riscontrare a che cosa possa corrispondere;

- 8.8: dimostrazione del sospetto trasferimento del file "[*omissis*].jpg" sul PC [*omissis*];
- 8.9: dimostrazione ulteriore dell'apertura del detto file "[*omissis*].jpg";
- 8.10: dimostrazione di visitazione dal PC in esame, PC_ [*omissis*] \[*omissis*] \[*omissis*].ARJ (della quale al momento presente non conosciamo la natura ed il contenuto);
- 8.11: dimostrazione di apertura di immagini "hard" sul PC in esame
- 8.12: dimostrazione di visitazione e apertura dal PC in esame [*omissis*] sul PC_[*omissis*] e correlazione a presa visione di documenti relativi [*omissis*];
- 8.13: dimostrazione di "navigazione" dal PC in esame, [*omissis*]" su [*omissis*], APPOGGIO DI [*omissis*], PER RELAZIONE [*omissis*] cartella a sua volta contenente il File "[*omissis*].jpg" e contemporaneamente APERTURA DEL PC_[*omissis*] ed ESECUZIONE AUTOMATICA DI WINDOWS.

9. Le "IMMAGINI" che vanno dalla Pagina 1 alla Pagina 49 sono quelle recuperate nel PC in esame, e sotto ognuna è stato indicato il percorso "LOGICO", la cui quasi totalità era stata cancellata. Si noti alla Pag. 1, la n. 1 rappresenta la "videata" di un videogioco, la due la "[*omissis*].jpg" nei vari momenti in cui è stata trattata attraverso questo PC, la n. 3 [*omissis*], la 4 ancora la "[*omissis*].jpg", da pag. 40 a 44, le foto n. 106/107/108/109/110/111/112/113/114 del calendario (tra l'altro bene in vista stampato ed esposto vicino alla postazione del PC del [*omissis*], come [*omissis*]);

10. Le "RECOVERED GRAPHIC FILES" , ancora immagini che vanno da Pag. 1 a Pag. 10 inclusa, che erano state diciamo "dimenticate" dal sistema in zone "disallocate" del disco C del PC in esame .-

Fatto, letto e sottoscritto in buona fede.

Porto Recanati, 16/06/[*omissis*].-

Emilio Luchetta

REPERTO TEST EnCase v6.19.4

Name	**REPERTO TEST**
Description	Volume, Sector 0-62655, 30,3MB
File Acquired	25/06/12 13:06:30
Logical Size	0
Initialized Size	0
Physical Size	16.384
Starting Extent	0 REPERTO TEST-S512
File Extents	1
References	0
Physical Location	262.144
Physical Sector	512
Evidence File	REPERTO TEST
File Identifier	0
Code Page	0
Full Path	**REPERTO TEST\REPERTO TEST**
Serial Number	0000-0000
Heads	2
Sectors Per Track	32
Unused Sectors	64
Number of FATs	2
Sectors Per FAT	243
Boot Sectors	26

Volume

File System	FAT16
Sectors per cluster	1
Bytes per sector	512
Total Sectors	62.656
Total Capacity	31.801.344 Bytes (30,3MB)
Total Clusters	62.112
Unallocated	6.944.768 Bytes (6,6MB)
Free Clusters	13.564
Allocated	24.856.576 Bytes (23,7MB)
Volume Name	Tiger
Volume Offset	0
Drive Type	Removable

Device

Actual Date	25/06/12 13:06:30
Target Date	25/06/12 13:06:30
File Path	C:\Documents and Settings\Desktop\REPERTO TEST.E01
Case Number	REPERTO TEST
Evidence Number	REPERTO TEST
Examiner Name	Luchetta Emilio
Notes	SD CARD 32 MB
Label	Tiger
Drive Type	Removable
File Integrity	Completely Verified, 0 Errors
Acquisition MD5	**81ae3c18d05679db21fc00060bd60504**
Verification MD5	**81ae3c18d05679db21fc00060bd60504**
GUID	8239e3b20a1c034cb9a7689143d4e5d4
EnCase Version	6.19.4
System Version	Windows XP
Raid Stripe Size	0
Error Granularity	64
Process ID	0

FOTO 1: RAPPRESENTA IL DOCUMENTO DI COPIA FORENSE CHE VIENE FORMATTATO AUTOMATICAMENTE, E' IMMODIFICABILE DALL'OPERATORE.

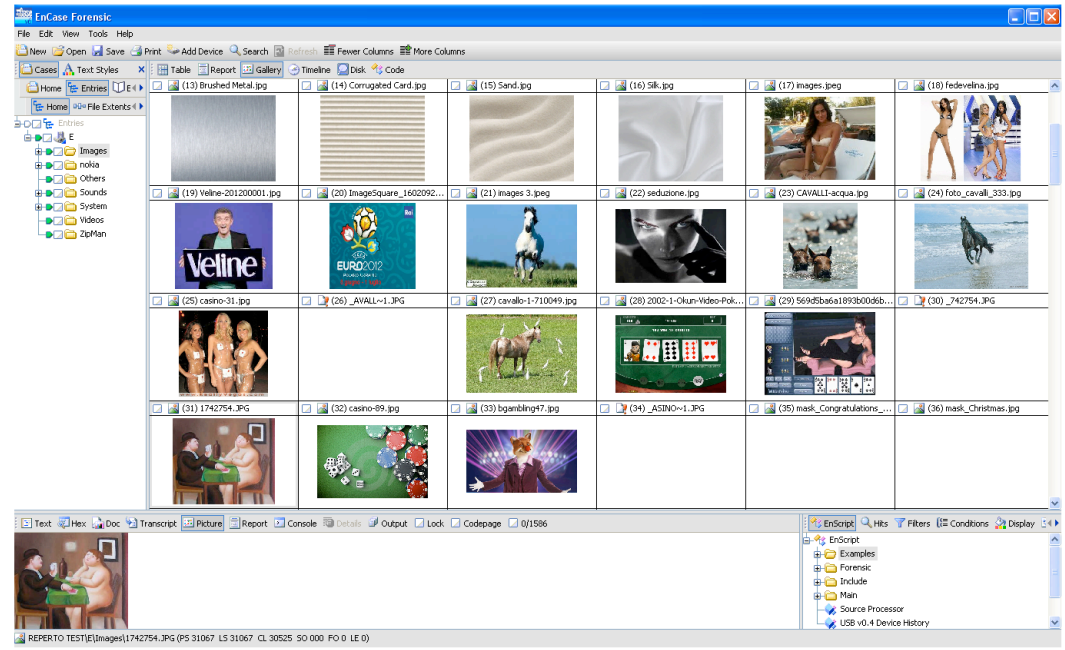


FOTO 2: RAPPRESENTA LA VISUALIZZAZIONE DELLA GALLERIA IMMAGINI.

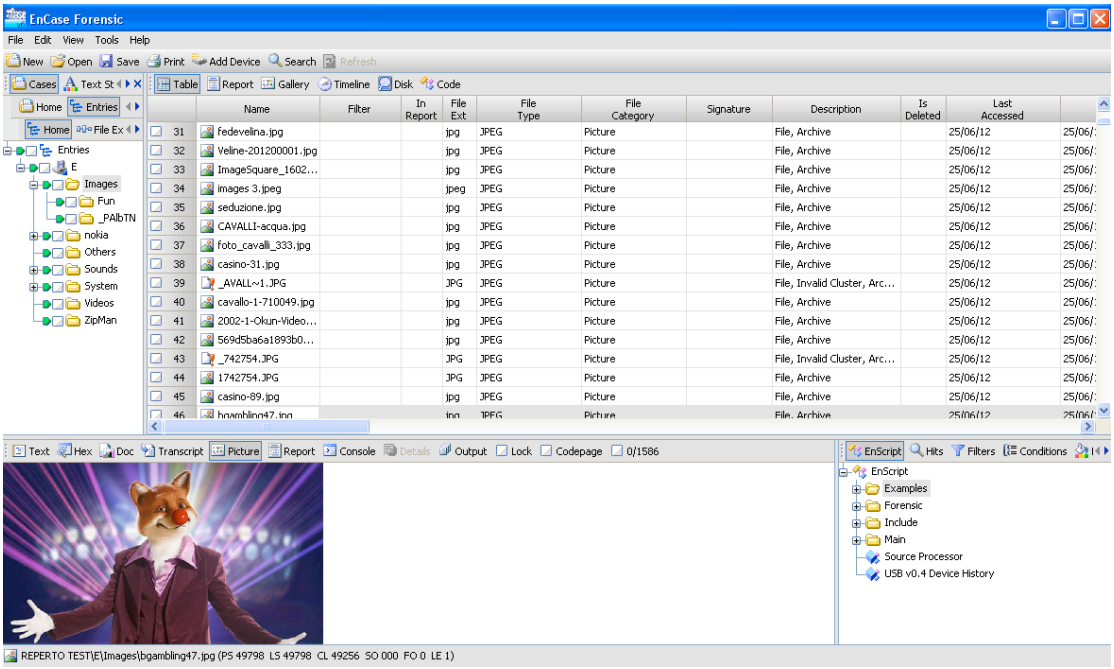


FOTO 3: RAPPRESENTA LA VISUALIZZAZIONE DEI DETTAGLI DELLA SINGOLA IMMAGINE ANALIZZATA.

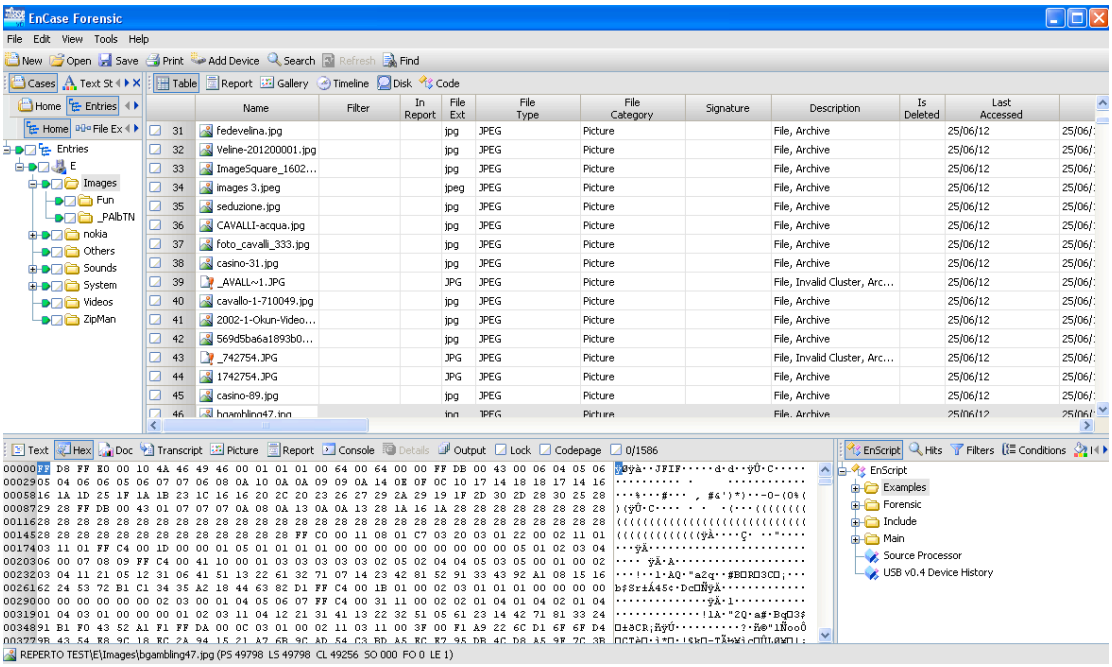


FOTO 4: RAPPRESENTA LA VISUALIZZAZIONE DELL'IMMAGINE IN ESADECIMALE NELLA COLONNA IN BASSO A DESTRA, NELLA COLONNA AL CENTRO I DETTAGLI HEADER DEL FILE.

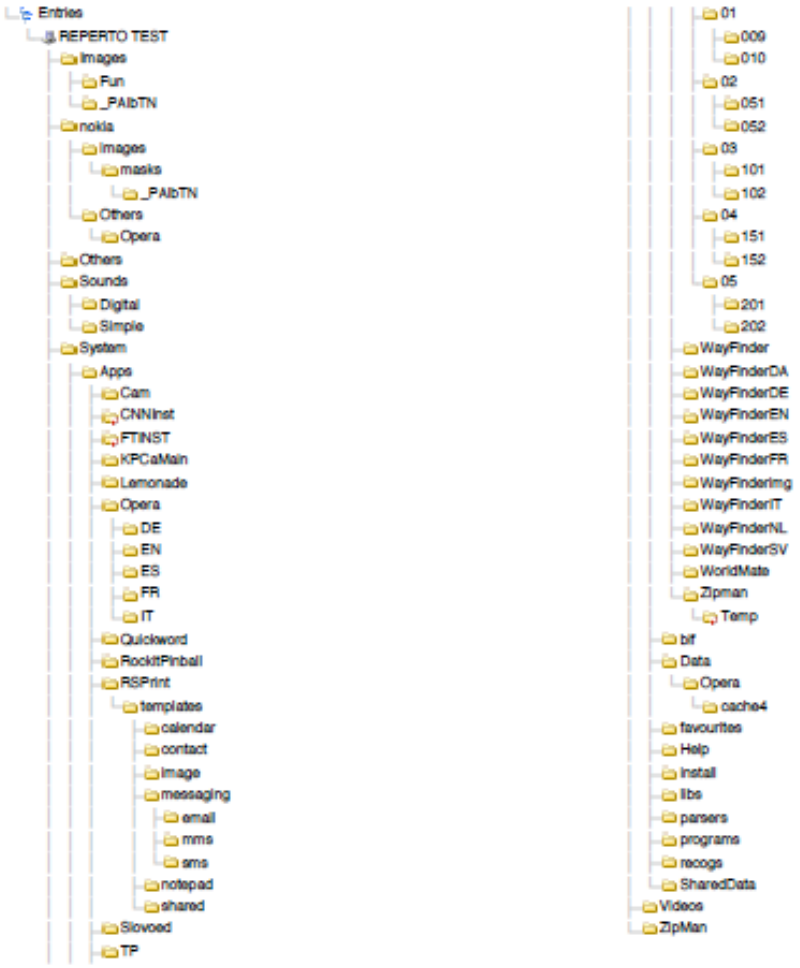


FOTO 5: RAPPRESENTA IL TREE ESPLOSO DEI FILE E FOLDER PRESENTI NELL'EVIDENCE CHE SI STA ANALIZZANDO.

CONCLUSIONI

La funzione delle operazioni forensi su supporti digitali è quella in definitiva di produrre la Prova di un fatto.

I guanti e la maschera dell'operatore della Polizia Scientifica sono parificabili ai sistemi di blocco di scrittura nell'area digitale, entrambi insostituibili e da interfacciare in modo organico e dinamico al fine di ottenere il massimo effetto positivo della ricerca della verità, reale e processuale.

Aver fatto parte di questa evoluzione e di questa metodologia acquisita nelle attività forensi è la conferma che siamo sulla buona strada, seppur spesso vengono a mancare le risorse per garantire un'operatività diffusa sul Territorio Nazionale di tutti gli addetti in tutti i settori Giudiziari.

La diffusione della metodologia e dell'uso dei sistemi garantisce la buona opera, investigare è non solo giusto ma indispensabile, in una società giusta, per garantire attività preventive e di intelligence, perché è un dato di fatto che prevenire è meglio che curare.

Luchetta Emilio

Tiranti Ilaria

BIBLIOGRAFIA:

Computer Forensics e Indagini Digitali - Manuale Tecnico-giuridico e casi pratici
di S. Aterno, F. Cajani, G. Costabile, M. Mattiucci, G. Mazzaraco
Ed. Experta

Manuale di Informatica giuridica e diritto delle nuove tecnologie
di Massimo Durante e Ugo Pagallo
Ed UTET

EnCase Computer Forensics - EnCase Certified Examiner
Di Steve Bunting
pubblicato da John Wiley and Sons Ltd

ANALISI FORENSE CON PHOTOSHOP
di George Reis
Apogeo Editore

I NUOVI REATI INFORMATICI
M. Cuniberti, G.B. Gallus, F. P. Micozzi, P. G. DEmarchi
G. Giappichelli Editore, 2009

A. Ghirardini, G. Faggioli (2009), "Computer Forensics"
nuova edizione - Apogeo

G. Costabile (2008), "Information Security in Azienda" -
Experta edizioni

Manuale istruzioni EnCase Advanced Computer Forensics v 4-5-6
Guidance Software

Nanni Bassetti (2011) “Indagini Digitali”
Settima Edizione

Incident Response and Computer Forensics, 2^ Ed.
By Chris Prosise, Kevin Mandia, Matt Pepe

LINKOGRAFIA:

http://www.dfrws.org

http://www.nist.org

http://www.marcomattiucci.it

http://www.garanteprivacy.it

http://www.deftlinux.net/

http://www.guidancesoftware.com

http://www.accessdata.com

http://www.htcia.org/

http://www.cellebrite.com

http://www.caine-live.net/

INDICE