

D.I.M

Digital Investigation Manager

L'attività del perito forense e dell'incident responder si sta, sempre più, popolando di procedure operative e documentali complesse e rigorose, destinate a imporsi come standard nei dibattimenti forensi e nell'individuazione e identificazione delle cause che hanno provocato un incidente informatico.

Al fine di venire incontro a tali necessità la DFLabs, azienda italiana operante in Europa e Stati Uniti in ambito di Information Security Risk Management, ha creato D.I.M. (<http://dim.dflabs.com/index.html>).

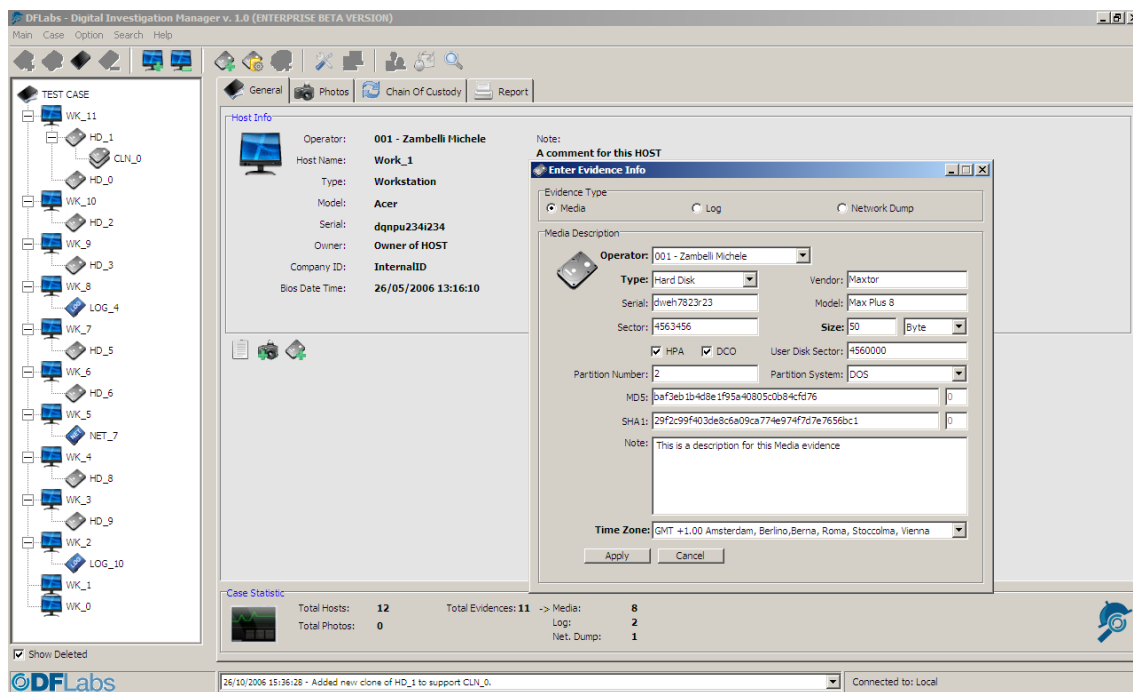


Illustrazione 1: Inserimento delle informazioni relative all'host acquisito

Acronimo per Digital Investigation Manager, identifica un'applicativo realizzato in Delphi e basato su database che guida l'operatore addetto all'indagine di computer e network forensic nei passi necessari per acquisire e documentare le fonti di prova, redarre la documentazione prevista, collezionare le informazioni aggiuntive e i risultati dell'attività di analisi.

L'interfaccia grafica presenta, oltre la consueta barra degli strumenti, due finestre:

- quella di sinistra dove con struttura ad albero vengono presentati, per ogni caso, i network dump, o gli host soggetti ad indagine ed i media ad essi collegati;
- quella di destra, dove per ogni elemento acquisito una serie di sheet consentono di raccogliere in un'unica interfaccia grafica tutte le informazioni inserite, permettendo di fare rapidamente il punto della situazione.

Relativamente ad ogni network dump, host o media acquisito si inseriscono le informazioni indispensabili ad identificare univocamente chi ha eseguito un'operazione, quando, con quali modalità, i relativi dettagli tecnici ed eventuali log in formato binario o testuale.

E inoltre possibile far caricare dal programma le immagini digitali dell'elemento acquisito, da cui verranno estratti i meta-dati Exif; l'applicativo si incaricherà quindi di ridimensionarle in formato standard, salvando gli originali nella cartella indicatagli.

La possibilità di inserire immagini digitali e log relativi agli items acquisiti e alle operazioni effettuate, conserva l'impronta specificatamente legata all'attività di indagine e validazione, infatti, all'atto di acquisire

immagini e log, viene elaborato l'hash degli stessi secondo gli algoritmi MD5 e SHA1, dati che compariranno in automatico nella reportistica.

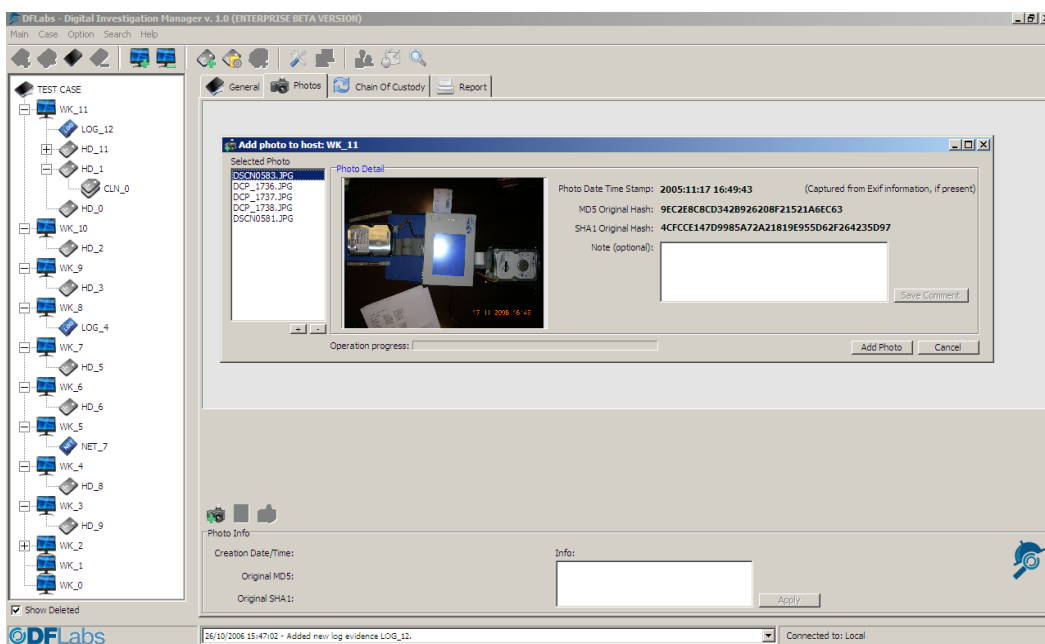


Illustrazione 2: Inserimento delle immagini digitali, con relativi hash e time stamp

Il DIM genera automaticamente la time-line delle operazioni effettuata. Sebbene sia possibile inserire manualmente nuove entry, per salvaguardare la coerenza dell'investigazione quelle generate in automatico non sono modificabili.

L'acquisizione o cessione fisica delle evidenze va sempre documentata, affinché sia sempre possibile identificare chi ha consegnato e chi ha ricevuto un host o un media da esaminare. La Chain of Custody (la catena di custodia) relativa ai diversi items viene aggiornata tramite nuovi inserimenti che compariranno automaticamente all'atto di generare la reportistica.

La sheet relativa ai reports viene in aiuto all'investigatore, permettendogli di generare in automatico, attingendo a quanto inserito nel data-base, tutta la modulistica da presentare in forma cartacea, o digitale, al committente. Sarà quindi possibile documentare gli articoli acquisiti, la time-line delle operazioni relativa al caso, all'host o al singolo media, i costi sostenuti, la catena di custodia e i dettagli tecnici delle operazioni.

I report, sui quali è prevista la possibilità di personalizzare il logo, o l'intestazione, possono essere stampati o generati in formato PDF.

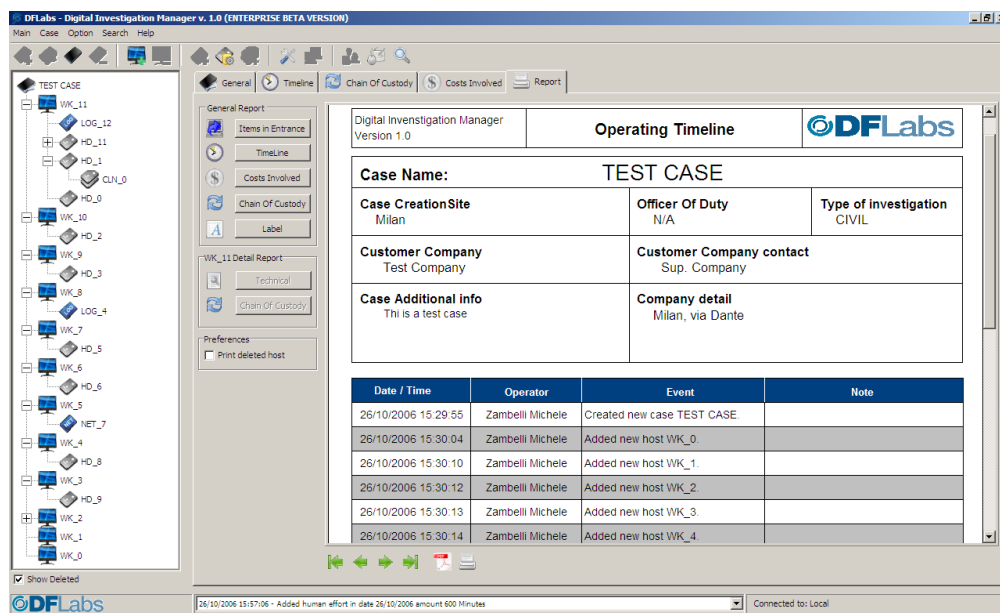


Illustrazione 3: La sheet relativa alla reportistica

Il DIM, nato dall'esperienza fatta sul campo dai consulenti DFLabs, è pensato per evitare dimenticanze ed errori che possano invalidare il lavoro di acquisizione ed analisi effettuato. In fase di acquisizione sarà infatti obbligatorio inserire alcune informazioni, quelle essenziali dal punto di vista della forensic, senza le quali il programma non completerà la fase di inserimento.

Il Digital Investigation Manager non è, tuttavia, un semplice gestore della documentazione relativa ai casi affrontati, consente infatti un'ottimale gestione del "magazzino/laboratorio" del perito. Le features disponibili a tal proposito consentono, infatti, di documentare l'hardware e il software di cui l'operatore, o agenzia, dispone, di tener traccia di eventuali cessioni o rientri e di abbinare, con una semplice spunta, i tools disponibili ad uno specifico caso, vedendoli quindi comparire nella reportistica.

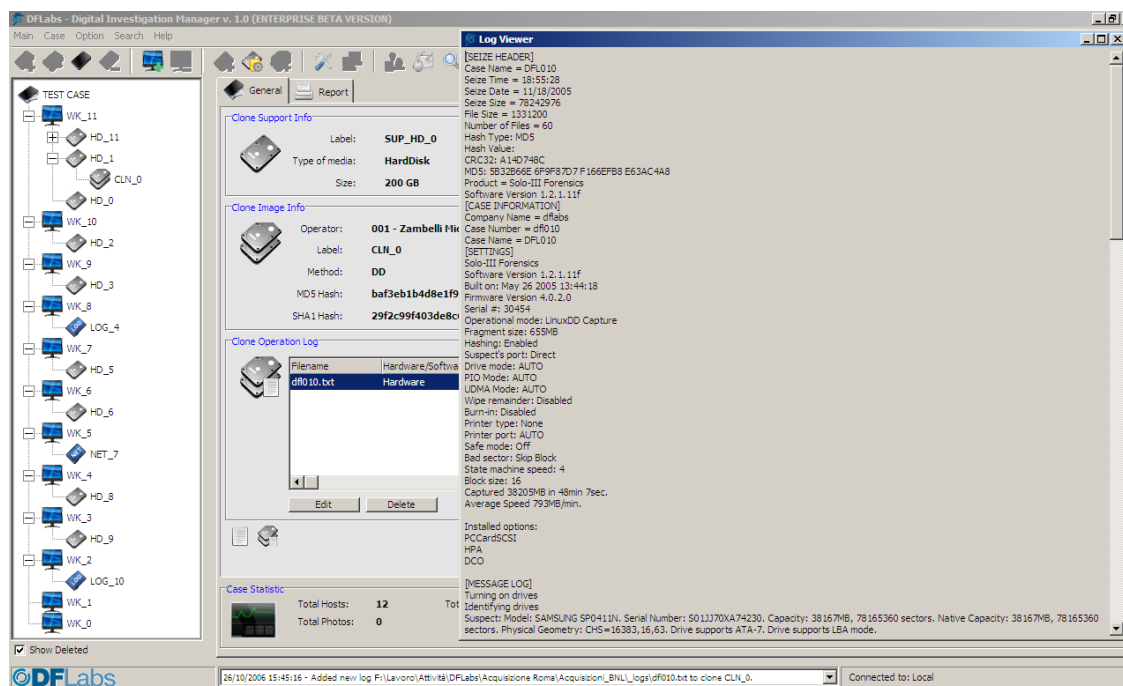


Illustrazione 4: Consultazione dei log inseriti

Il data-base del DIM contiene, come ovvio, dati sensibili e riservati. Il DIM viene venduto unitamente al dongle che, oltre a permettere la gestione della licenza ed eventuali subscription, consente un'ottimale forma di sicurezza. Il programma è infatti avviabile unicamente inserendo il dongle nella porta usb del computer su cui è installato. In tal modo si impedisce la consultazione del data-base, attraverso l'utilizzo indebito del programma, rendendo sicure le informazioni in esso contenute, anche in caso di sottrazione del computer su cui il DIM è installato; a patto ovviamente che computer e dongle non vengano sottratti insieme!

Il DIM è disponibile in versione Stand Alone, per un solo investigatore, con data-base locale. In versione Workgroup, supporta fino a dieci investigatori, consente la gestione di un data-base centralizzato, disponibile con db MySQL e prossimamente Oracle, con il quale gli investigatori possono sincronizzarsi. La versione Enterprise, che supporta un numero illimitato di operatori, include il modulo Supervisor, opzionale nella Workgroup, che permette la gestione e la supervisione di tutti i casi e degli investigatori.

Il software di gestione delle investigazioni digitali realizzato dalla DFLabs, può quindi essere un valido aiuto, non solo per agenzie ed enti, ma anche per il singolo perito che, ad un prezzo (circa 350 euro per la Stand Alone) relativamente contenuto, può dotarsi di un valido ausilio non solo per una corretta raccolta dei dati, ma anche per l'esecuzione delle operazioni standard, la generazione della reportistica e per un'ottimale gestione del proprio equipaggiamento.