

«Back|Track-[IT]

www.backtrack.it



(c) 2009 dr4kk4r
(c) 2009 keeley
dr4kk4r@backtrack.it
keeley@backtrack.it

Forensics



C omputer Forensics

Il nostro mondo, come è noto, è sempre più interconnesso: Miliardi di comunicazioni viaggiano ogni giorno in forma elettronica nei dispositivi più disperati, pensiamo ad esempio quanti apparecchi sono coinvolti in una comunicazione che può avvenire in una conversazione via cellulare piuttosto che una video chiamata in instant messenger.

Per quanto complessi essi siano, ciò che li riconduce ad una base comune sono le informazioni o, per meglio dire, i dati stessi che essi trasportano.

Ogni dato che viaggia sotto forma elettronica, lascia per così dire una traccia del suo passaggio, a volte volontaria, pensiamo ad esempio ad operazioni di log, ed altre volte involontaria come operazione di lettura/scrittura sul supporto digitale stesso.

Infatti non sono rari i casi annessi ai reati informatici o quanto meno reati che includono dispositivi digitali; pensiamo ad esempio reati di scambio/detenzione di materiale pedo-pornografico, di phishing o di reati non ascrivibili direttamente nei reati informatici quali ad esempio la rapina.

Difatti ogni scena del crimine pullula di dispositivi High-Tech, e la loro rilevanza molte volte fa la differenza, fra colpevolezza o innocenza dell'indagato stesso.

Ed proprio in questa fase che nasce l'analisi forense, o per meglio precisare Computer Forensics, ovvero la disciplina che studia il processo di analisi dei dispositivi aventi memoria digitale sia che essi siano computer, cellulari, router, pda o navigatori gps.

Il compito del computer forensic specialist, ossia colui che si occupa della Computer Forensic, è quello di individuare, estrarre, analizzare, conservare e documentare le digital evidences ovvero le prove digitali.

Il Codice di Condotta prevede che gli esaminatori debbano:

- Mantenere il più alto livello di obiettività in tutti gli esami forensi e presentare accuratamente i fatti che sono accaduti;
- Esaminare ed analizzare accuratamente le prove di un caso;
- Condurre gli esami basandosi su principi fondati e legittimi;
- Presentare relazioni fondate su basi logiche;
- Non trattenere indebitamente qualsiasi informazione (accusatoria o assolutoria) che potrebbe portare a distorcere o travisare gli avvenimenti di un caso;
- Mai fare false dichiarazioni di credenziali, educazione, formazione, esperienza o appartenenza.

Le procedure di esame forense richiedono tre requisiti essenziali:

- Eseguire un'Analisi conforme agli standard;
- Conservare l'integrità del supporto originale;
- Stampe, copie di dati e reperti risultanti dall'esame devono essere contrassegnati, controllati e trasmessi in maniera corretta.

Quindi gli esaminatori devono:

- Identificare i sospetti e le fonti dell'evidenza. Nel caso in cui non siano disponibili informazioni, si deve considerare il sospetto come un soggetto esperto, ritenuto capace di installare contromisure contro Analisi Forensics.
- Preservare l'evidenza digitale
 1. Analizzare l'evidenza
 2. Presentare le scoperte
 3. Il lavoro deve essere svolto in maniera tale da essere ritenuta ammissibile presso un'aula di Tribunale.

Gli strumenti considerati prove devono essere documentati per il ricevimento ed il trattamento. La documentazione deve riportare una descrizione fisica ed una notazione dettagliata di qualsiasi irregolarità, peculiarità, segno distintivo e numerazione.

Quando si esamina un computer, dal BIOS dovrebbero essere annotati data e ora (e confrontati con un affidabile time source, annotare lo scostamento); parametri del disco; l'ordine di boot; i numeri di serie del sistema e dei componenti, ed in fine gli hash dei componenti hardware.

Non dimenticarsi di predisporre gli esami su una delle copie forensi e mai sull'originale, annotare su un documento ogni singolo passo per poter permettere alla difesa di ripetere le stesse operazioni e cercare di partire da dove le prove potrebbero essere facilmente reperite.

La prassi prevede di effettuare le seguenti operazioni:

- Annotare i file system, i sistemi operativi e gli applicativi installati, il numero e la tipologia del disco fisso, di un eventuale disco ottico ed il numero di sessione;
- Effettuare, eventualmente, una directory listing per includere la struttura della cartelle, i nomi dei files, time stamp, dimensioni logiche dei files;
- Esaminare i files creati dall'utente con le applicazioni native, visualizzatori di files o esadecimali (documenti di testo, fogli elettronici, data base, dati finanziari, posta elettronica, foto digitali, files multimediali);
- Controllare i files creati dalle applicazioni e dal sistema operativo (files di boot, files di registro, file di swap, files temporanei, cache files, history files, files di log);
- Utilizzare il confronto tra i files di hash per includere od escludere i files dall'esame;
- Esaminare lo spazio allocato ma non utilizzato, alla ricerca di files cancellati, cartelle rimosse, dati nello slack space, dati aggiunti intenzionalmente ed annotarlo;
- Eseguire ricerche per parole chiave per identificare informazioni a valore probatorio;
- Annotare le anomalie nell'area del sistema del volume;
- Richiedere l'esame dei media non normalmente accessibili.

Alla fine dell'esame deve essere prodotta la necessaria documentazione delle procedure e dei processi eseguiti, degli output prodotti identificati secondo gli standard forniti.

Nel caso di un'analisi di un disco fisso, si può provvedere allo smontaggio dei dischi oppure eseguire una copia via rete per poter acquisire anche il drive logico. Secondo la nomina del PM, eseguire la copia "bit-a-bit", provvedere ad eseguire sui files l'algoritmo di hash. Le copie (almeno 3) potranno essere verificate sia con md5 sia con sha1. Nel frattempo verranno preparati i media destinati all'analisi del contenuto degli Hard Disks posti sotto indagine, utilizzando software licenziato od Open Source (dd, netcat).

Esaminare il pc, descrivendolo e prendere precauzioni per prevenire il trasferimento dei virus, software distruttivi o scritte involontarie. Verificare il contenuto del CMOS. Eseguire una copia bit-a-bit con relativa documentazione. Analizzare la copia, esaminare il settore di boot, i files di configurazione (.bat, .sys), recuperare i files cancellati. Stilare un elenco di files con indicazione se possano contenere prove. Cercare i files persi o nascosti nello spazio allocato, nello slack space, i files utenti, sbloccare i files con password, eseguire una stampa dei files trovati. Produrre una dettagliata documentazione.

Esami limitati

Nel caso di esami limitati devono essere riportati i motivi di tale indisponibilità riconducibili a:

- Lo scopo dell'esame è limitato dal mandato di perquisizione del Tribunale;
- L'esame deve avvenire in loco;
- L'analisi completa è impossibile a causa delle dimensioni;
- Le prove trovate sono talmente schiaccianti, che non occorrono ulteriori ricerche;
- A causa delle limitazioni hardware, del sistema operativo od altre condizioni non riconducibili all'esaminatore.