Indice delle definizioni forensi…

- *Informatica Forense o "Computer Forensic":*

Cenni storici:

La disciplina ha origine negli Stati Uniti e in Gran Bretagna, paesi altamente tecnologici e in cui vige un sistema giudiziario di "common law". L'anno di nascita della Computer Forensic è il 1984; il laboratorio scientifico dell'FBI e altre agenzie investigative americane iniziarono a sviluppare programmi da utilizzare nell'esame dei dati presenti nei computer. Fu cretao inoltre, sempre all'interno dell'FBI, il Computer Analysis and Response Team(CART) con il compito specifico di procedere nei casi in cui si rende necessaria l'analisi di un computer. Una data importante nell'evoluzione della materia è il 1994, anno in cui il Dipartimento della Giustizia degli Stati Uniti ha pubblicato un insieme di linee guida che hanno fissato uno standard e sono divenuti un riferimento per studi e atti successivi(Federal Guidelines for Searching and Seizing Computer, US Department of Justice, 1995). In Italia, oltre ai nuclei nei corpi di polizia, sono nate aziende di servizi di sicurezza informatica che offrono per l'appunto prestazioni di informatica forense(nel 1996 fu creato il Nucleo Operativo di Polizia delle Telecomunicazioni; nel 1998 venne istituito il Servizio di Polizia Postale e delle Telecomunicazioni dove confluirono le risorse del Nucleo Operativo di Polizia Postale e della Divisione della Polizia Postale).

Introduzione:

Per Informatica Forense o "Computer Forensics" si intende quella disciplina che studia tutte le attività rivolte all'analisi e alla soluzione di casi criminali realizzati con l'uso di un computer, diretti a un computer o in cui il computer rappresenta una fonte di prova. Acquisire, conservare, identificare, documentare ed interpretare i dati presenti su un computer sono gli scopi primari di questa materia. Si tratta quindi di utilizzare le modalità migliori per acquisire le prove senza alterare il sistema informatico in cui si trovano, garantire che le prove siano identiche a quelle originali ed infine ma non ultimo di analizzare i dati senza che essi ne risultino alterati. Quando si utilizza un dispositivo elettronico si lasciano sui dispositivi di memorizzazione ad esso collegati delle tracce, artefatti dovuti all'interazione di un utente con il computer. Queste tracce sono chiamate tracce informatiche o tracce digitale e comprendono:

- File di sitema
- File prodotti da applicazioni di varia natura
- Informazioni relativi ai file gestite direttamente dal sistema operativo
- Dati trasmessi da due o più computer collegati ad Internet.

Una caratteristica fondamentale delle tracce digitali è l'immaterialità; non esistono come oggetto fisico ma sono sequenze di bit memorizzate su dispositivi di archiviazione dati. Per accedere ad una traccia occorre dunque accedere al dispositivo su cui essa è memorizzata. I dispositivi di memorizzazione sono di due tipi:

- Persistenti: non necessitano di alimentazione per mantenere i dati memorizzati (penne USB, Hard Disk, nastri, schede di memoria).
- Volatili: interrotta l'alimentazione, i dati vengono persi (memoria RAM, telefonino, palmare).

Una traccia digitale assume valore probatorio quando essa è autentica, cioè si è certi della sua provenienza; veritiera, ottenuta grazie ad un'attenta e corretta interpretazione e analisi dei dati; integra, priva di alterazione; completa, cioè sono stati raccolti ed interpretati tutti i dati ad essa relativi e legale, raccolta cioè nel rispetto delle leggi vigenti.

Metodologie dell'investigazione informatica:

L'indagine informatica si suddivide in due punti:

Acquisizione delle evidenze: i supporti originali vanno congelati, cioè non devono più essere collegati ad un computer senza che sia utilizzato un dispositivo che garantisca il blocco delle operazioni di scrittura; essi devono essere poi sigillati in modo opportuno cosicché è possibile documentare la catena di custodia(che garantisce l'inalterabilità dei dati dal momento del sequestro fino al momento del dibattimento e per tutte le fasi dell'iter processuale). Durante il congelamento è di vitale importanza annotare la data e l'ora impostata nell'orologio di sistema per stabilire con certezza una linea temporale degli eventi. Per garantire che non siano introdotte modifiche dopo il "congelamento" si raccomanda l'utilizzo di algoritmi di hash crittografici che producono un codice(sequenza di caratteri) avente una lunghezza prefissata; questi codici godono di alcune proprietà:

1. Due sequenze di input identiche danno luogo allo stesso codice hash; al momento del congelamento del dispositivo si calcola il relativo codice hasch. Per verificare l'assenza di alterazioni dall'originale, si ricalcola il codice hash e si verifica che lo stesso sia uguale a quello calcolato all'atto del congelamento.
2. La probabilità che sequenze diverse diano luogo allo stesso codice è praticamente nullo. Per preservare l'integrità delle evidenze digitali, si raccomanda di effettuare tutte le operazioni di analisi su copie identiche dei dispositivi originali. A tal fine è necessario acquisire tutte le parti del dispositivo. Prima di effettuare la copia del dispositivo è necessario calcolare il codice hash dell'originale e confrontarlo con quello ottenuto all'atto del congelamento. Al termine dell'acquisizione si calcola il codice della copia appena effettuata che deve essere identico a quello dell'originale. L'operazione di acquisizione produce un file di immagine contenente una copia di tutti i bit memorizzati nel dispositivo. In seguito, mediante opportuni software di analisi forense, il file viene interpretato ed analizzato.

Analisi delle evidenze digitali: scopo dell'analisi è individuare quelle tracce digitali che consentano una ricostruzione delle attività del computer cui il dispositivo era collegato e l'individuazione di elementi probatori. L'analisi viene effettuata con l'aiuto di appositi software forensi. Si effettuano diversi tipi di analisi:

Analisi a livello del file system: si prendono le tracce informatiche prodotte dal sistema di gestione dei file(file system) o contenute nei file. Ai fini probatori è rilevante prendere in considerazione i tempi MACE(Modified/Accessed/Created/Entry Modified) che consentono di ottenere una timeline delle attività effettuate sui file.

Analisi a livello del sistema operativo: si prendono gli artefatti prodotti dal sistema operativo durante il suo funzionamento. Vengono presi in considerazione file di log, file di configurazione, snapshot della configurazione di sistema utilizzate per un eventuale ripristino. Ciò consente di evidenziare l'uso del computer da parte degli utenti; di determinare quando specifici file sono stati aperti dall'utente; di individuare le periferiche che sono state collegate, i file stampati e su quale stampante; identificare le reti cui il computer è stato collegato.

Analisi delle applicazioni: si prendono gli artefatti prodotti da programmi applicativi. Estrazioni di contenuti "embedded", metadati applicativi(file MS Office, file PDF, file grafici,attività di navigazione su Internet, scambio di email, attività di Istant Messaging e Chat, attività di file sharing).

Negli ultimi anni il numero di dispositivi quali Smarth Phones, iPod e iPhone, navigatori satellitari, telefoni cellulari di ultima generazione, riproduttori mp3 e consolle per videogame è cresciuto notevolmente ponendo nuove problematiche di non facile soluzione a cui la comunità scientifica ha da poco iniziato a dare soluzione che ad oggi appaiono solo parziali.

Didattica:

Negli U.S.A e in altri paesi europei vi sono numerosi corsi di Informatica Forense tenuti soprattutto da case produttrici di software o corsi per il personale interno nell'ambito delle organizzazioni statali di polizia o di intelligence. Sono previsti anche corsi di formazione per operatori giuridici e avvocati nell'ambito delle associazioni professionali.

Nel nostro paese cominciano a svilupparsi corsi a livello accademico correlati a quelli relativi alla sicurezza dei sistemi. In una prospettiva di influenza della tecnologia sul diritto, iniziano a prendere piede, in campo giuridico, studi sull'evoluzione del concetto di documento e corsi sui crimini informatici legati al campo del diritto penale, del diritto privato dell'informatica e dell'informatica giuridica.

- *Ingegneria Forense:*

Cenni storici:

L'Ingegneria Forense costituisce tema noto e diffuso nei Paesi anglosassoni, soprattutto negli Stati Uniti d'America, da oltre vent'anni. In Italia tale argomento è stato sviluppato grazie alla Facoltà di Ingegneria dell'Università Federico II di Napoli ove di recente è stato attivato il primo corso universitario nel quale vengono trattate queste problematiche. L'obiettivo è quello di conferire alla materia il lignaggio di scienza.

Definizione:

L'Ingegneria Forense applica i principi e i metodi specifici dell'Ingegneria alla soluzione dei problemi tecnici in ambito giudiziario. Il settore tradizionale della disciplina, nei Paesi anglosassoni, è quello strutturale che analizza i crolli e i grandi dissesti. In senso stretto la materia indaga sulle cause e sulle responsabilità di un evento dannoso. In senso lato opera nei procedimenti giudiziari civili e penali.

L'Ingegnere Forense:

È quella figura professionale che indaga sulle cause più probabili per cui si è verificata una prestazione diversa da quella attesa e sulle responsabilità. L' Ingegnere Forense individua i problemi quali dissesto, difetto, danno o guasto che si verificano per ogni tipo di costruzione. È un Ingegnere "inverso" poiché parte dagli effetti (es. disastro) per individuare le cause (danno, guasto ecc...).L'Ingegneria Forense dunque opera sia nel settore civile (disastri edilizi e quant'altro) sia nel settore industriale denso di attività forensi come quelle riguardanti il campo meccanico, chimico, navale, aeronautico ed elettrico. Questa figura dunque non è utile solo ad individuare cause e responsabilità di un dissesto, ma anche ad evitare il ripetersi degli errori.

Metodi di analisi:

Come la Scienza Forense, anche l'Ingegneria Forense utilizza il microscopio ottico, lo "scanning Electron microscope (SEM)", la spettroscopia a raggi infrarossi, ultravioletti e la risonanza magnetica nucleare per esaminare le prove. Anche la radiografia a raggi-X o a neutroni è molto importante nell'individuazione di possibili difetti, utili nella ricostruzione di un incidente. Inoltre l'Ingegneria Forense si concentra molto sull'analisi chimica dei materiali presenti sulla scena del crimine o di un incidente per determinarne la natura.

La casistica dell'Ingegneria Forense riguarda:

- Incidenti automobilistici
- Catastrofi ambientali o edili
- Incendi
- Supporto sulla scena del crimini