Introduzione

Negli ultimi anni il campo della Digital Forensics è cresciuto e si è diversificato enormemente, per numerosi motivi. La diffusione di dispositivi IoT, di tecnologie indossabili (wearable) e di altre nuove tecnologie, come il 5G, è trattata in dettaglio nel Capitolo 13, perché l'incidenza sulla Digital Forensics sarà profonda. Quel capitolo inoltre esamina come le nuove tecnologie siano contribuendo a modificare le regole di comportamento e la sicurezza delle forze dell'ordine. Il capitolo analizza anche il campo, in rapida crescita, dell'analisi forense dei veicoli (*Vehicle Forensics*).

Non c'è stata una riduzione, a livello globale, nel numero delle intrusioni nelle reti, perciò il bisogno di esperti di Digital Forensics per la risposta agli incidenti è più grande che mai. Di conseguenza il Capitolo 7 si concentra sullo sviluppo delle competenze per chi deve rispondere agli incidenti e sugli indicatori di compromissione.

La Mobile Forensics è in continua evoluzione; i cambiamenti sono trattati in vari capitoli: il Capitolo 9 offre un'introduzione, ma spiega anche come sono cambiati i dispositivi Android e i metodi di esame. Il Capitolo 11 spiega come siano cambiate drasticamente le tecniche di analisi degli iPhone e mostra come un exploit, recentemente scoperto, consenta ora l'estrazione dell'intero file system. Le applicazioni (app) per il mobile salvano una quantità enorme di informazioni personali e praticamente ogni indagine oggi include almeno un dispositivo mobile. Perciò il Capitolo 10 presenta agli investigatori le tecniche forensi per eseguire un esame sia statico sia dinamico delle app per mobile. Quello stesso capitolo spiega anche come da molte app di grande diffusione si possano ricavare informazioni in tempo reale.

Tutti i capitoli sono stati ampiamente aggiornati per incorporare i molti cambiamenti nella tecnologia e le tecniche più recenti scoperte per ottenere prove digitali.

Il libro non presuppone una conoscenza pregressa dell'argomento; l'ho scritto pensando sia agli studenti universitari sia agli investigatori forensi. Inoltre, anche altri professionisti possono trarre giovamento dalla lettura del libro: può essere utile per avvocati, contabili forensi, professionisti della sicurezza e altri, che hanno bisogno di comprendere come si raccolgano, si gestiscano e si presentino in tribunale le prove digitali. Il libro pone l'accento in particolare sui processi e la conformità alla legge, che sono parimenti importanti per le prove che possono essere raccolte.

Il lettore deve anche sapere che un'ampia conoscenza della Computer Forensics può aprire vari tipi di carriera. Esaminatori ed esperti forensi lavorano per società di revisione dei conti, società di software, banche, forze dell'ordine, agenzie di intelligence e società

di consulenza. Ogni grande azienda ha un team di risposta agli incidenti e molte hanno un team o un reparto di intelligence delle minacce. Questo libro sarà certamente utile a chi ha già intrapreso questa professione e anche a chi sta pensando di cambiare lavoro. La crescita dei social media e di dati e strumenti open source crea una grande quantità di informazioni per gli investigatori, e di questo si parlerà nel libro. Alcuni sono esperti di Mobile Forensics, altri di Network Forensics, altri ancora si specializzano nei personal computer, altri sono specializzati in Mac Forensics o nella retroingegnerizzazione di malware. Chi si laurea con un'esperienza di Computer Forensics ha davanti a sé buone prespettive e molti ambiti fra cui scegliere: il mercato del lavoro per loro rimarrà robusto e per il futuro prevedibile saranno disponibili più posti di lavoro di quanti siano i laureati che possono aspirarvi.
Questo libro è una guida pratica, non solo per le attività che presenta, ma anche per i numerosi casi di studio e le applicazioni pratiche di tecniche di Computer Forensics. I casi sono un modo molto efficace per dimostrare come siano stati utilizzati con successo, in indagini differenti, particolari tipi di prove digitali.
Infine, questo libro fa spesso riferimento a strumenti professionali che possono essere costosi. Le istituzioni accademiche possono godere di sconti significativi, se acquistano questi prodotti. In queste pagine citeremo regolarmente molti strumenti gratuiti o a basso costo che possono essere efficaci quanto alcuni degli strumenti più costosi. Potete sicuramente creare un vostro programma o un vostro laboratorio mantenendo contenuti i costi.

Ringraziamenti

Devo innanzitutto ringraziare mia moglie, Nalini, la mia migliore amica, per il suo sostegno e la sua pazienza. Le molte ore che si devono dedicare alla scrittura di un libro significano sacrifici per tutti in famiglia e i miei figli, Nicolai, Aine, Fiona e Shay, sono stati stupendi. I miei genitori, Annette e Ted, sono stati la mia guida per tutta la vita e sarò sempre in debito con loro.