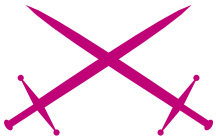

Analisi forense di un sistema informatico

dr. Stefano Fratepietro

Grado di difficoltà

Sentiamo spesso parlare di sequestri ed indagini, fatti dalla polizia giudiziaria, di materiale informatico perché tramite esso sono state eseguite operazioni atte a compiere un ipotetico illecito.

In pochi conoscono realmente quali sono le operazioni e le procedure da eseguire in casi di accertamenti tecnici, pochi conoscono realmente l'informatica forense (in inglese computer forensics), cioè la disciplina che concerne le attività di individuazione, conservazione, protezione, estrazione, documentazione e ogni altra forma di trattamento e interpretazione del dato memorizzato su supporto informatico, al fine di essere valutato come prova nei processi giudiziari. Nel dettaglio l'informatica forense studia a fini probatori i processi, le tecniche e gli strumenti per l'esame metodologico dei sistemi informatici, nonché l'analisi forense di ogni sistema informatico e telematico, l'esibizione della prova elettronica, l'esibizione del dato digitale, il recupero di dati e la loro esibizione, l'analisi ed esame del sistema informatico e telematico.

Premessa

Questo articolo tratterà solo due delle quattro fasi inerenti al trattamento del reperto informatico questo perché l'articolo è rivolto ad un target più informatico-pratico che giuridico-procedurale, pertanto salteremo le fasi di individuazione e valutazione per parlare solamente dei metodi e delle procedure utilizzate per l'acquisizione e l'analisi del reperto utilizzando strumenti open source.

Acquisizione

L'acquisizione di un reperto informatico, cioè l'estrapolazione dei dati dai loro supporti originari, è senza dubbio l'azione più delicata e complessa in assoluto, questo perché se l'acquisizione del reperto viene eseguita in modo non conforme, l'analisi fatta sul reperto potrebbe risultare non valida in ambito dibattimentale.

Dall'articolo imparerai...

- come vengono fatte le acquisizioni dei dati di un sistema posto sotto sequestro,
- metodi di analisi di un sistema informatico,
- software utilizzati per l'acquisizione e l'analisi analisi dei dati acquisiti.

Cosa dovresti sapere...

- nozioni basilari sulla Computer forensics,
- nozioni basilari sull'utilizzo di sistemi Linux,
- nozioni basilari sui filesystem.

Secondo le necessità investigative, l'acquisizione può essere effettuata o nell'immediatezza dell'intervento o in un secondo momento in laboratorio attraverso il sequestro giudiziario dei supporti. Trattandosi di attività molto critica e delicata, occorre svolgere le indagini adottando una precisa metodologia in modo da costruire delle prove attendibili e inattaccabili in sede dibattimentale. L'acquisizione dei dati contenuti all'interno del supporto comporta la creazione di una copia fedele mediante la procedura di bit streaming, che consiste nella riproduzione, non solo dei dati presenti nel supporto, ma anche delle tracce di dati cancellati, nascosti o crittografati; tale copia fedele servirà al soggetto investigatore per poter eseguire l'analisi senza correre il rischio di alterare il reperto originale.

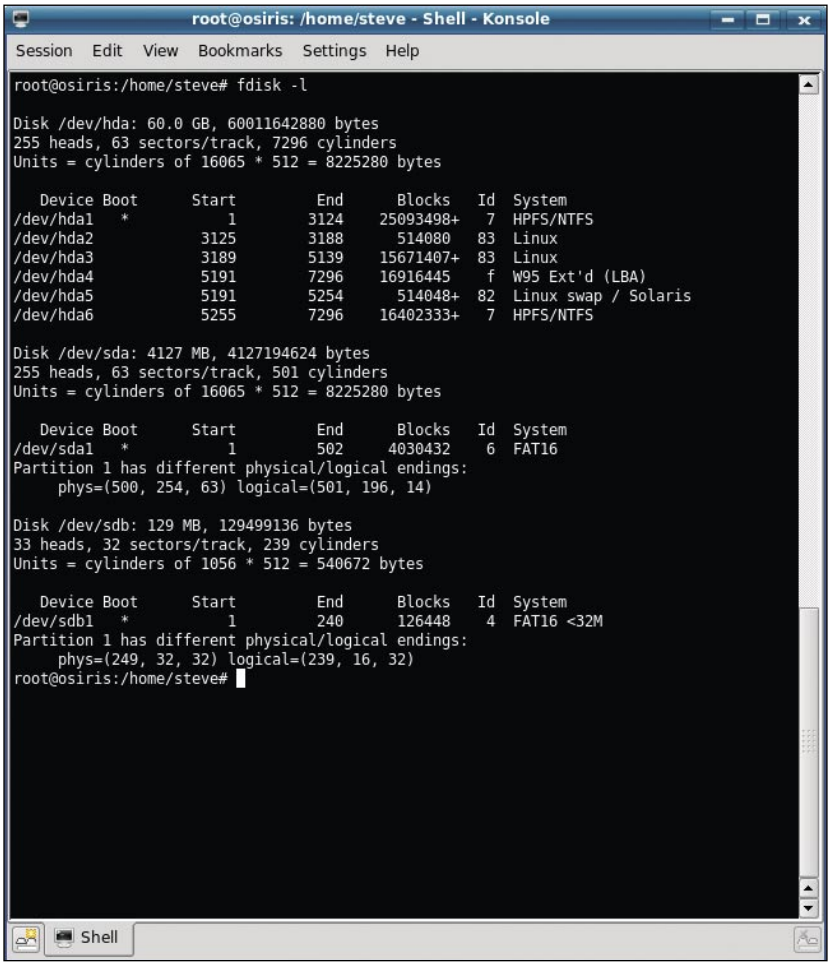

Fig. 1: *Fdisk -l in funzione*

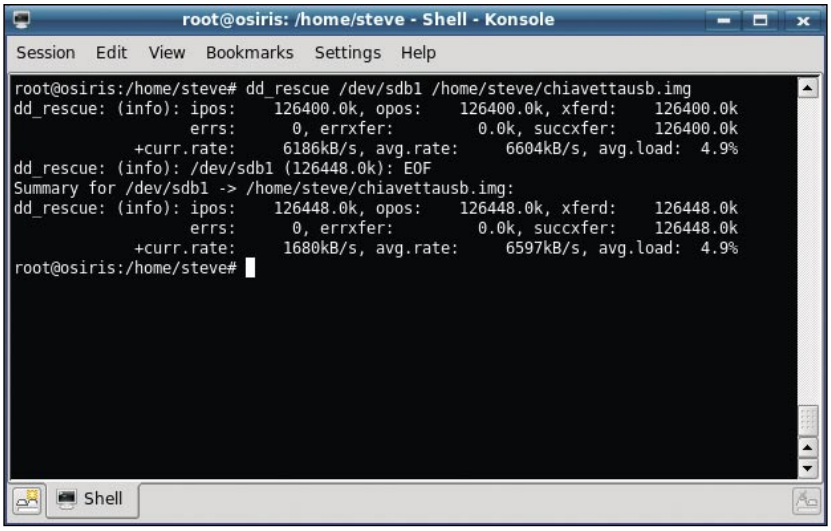

Fig. 2: *Output di ddrescue al termine dell'acquisizione*

Software open source per l'acquisizione forense

Tra i software disponibili per l'acquisizione di dispositivi di memoria troviamo molte soluzioni a codice aperto come dd, ddrescue e aimage. Supponiamo di dover utilizzare ddrescue per l'acquisizione del device /dev/sda1 (dove nel nostro caso corrisponde ad una penna usb da 128Mb) riscontrato mediante il comando `fdisk -l` (vedi Fig. 1) che da come output la lista dei device attualmente collegati al sistema; la sintassi che ci permette di creare una bitstream del device sarà `ddrescue /dev/sdb1 /home/utente/analisi/chiavettausb.img` dove `/dev/sdb1` è il device che vogliamo acquisire e `/home/utente/analisi/chiavettausb.img` è il path dove vogliamo salvare l'output dell'acquisizione.

Il programma terminerà senza dare alcun messaggio di avvenuta acquisizione pertanto bisogna riscontrare a mano l'esistenza del file chiavettausb.img (vedi Fig. 2).

In questa fase ha molta importanza la procedura di autenticazione dell'integrità dei dati originali e dei dati acquisiti.

Integrità del dato acquisito

La prova dell'integrità e dell'autenticità può essere fornita tramite l'uso di sistemi crittografici e di firma digitale; per ogni singolo file o per l'intero dispositivo viene calcolato un valore numerico, che ha le funzionalità dell'impronta digitale. Confrontando il valore ottenuto prima e dopo l'analisi, si può dimostrare che non sono state introdotte modifiche e che la prova è autentica. Nel nostro caso sarà necessario calcolare l'impronta del file e confrontarla con l'impronta del device; se le due impronte corrisponde-

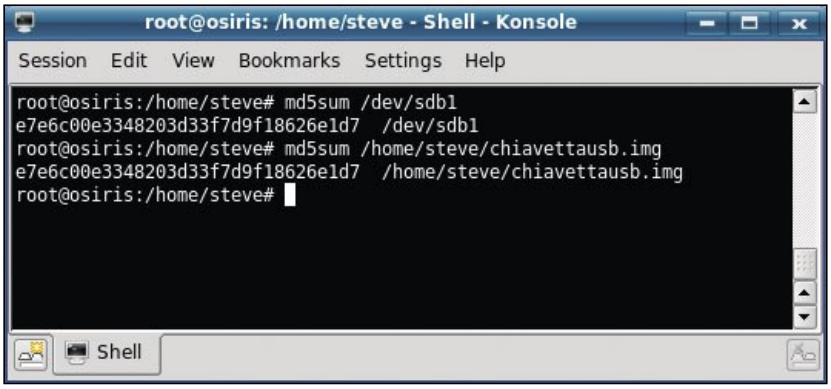

Fig. 3: *Confronto dello hash md5 del device e dell'immagine acquisita*

ranno, l'acquisizione è stata eseguita senza alcun errore, pertanto la prova sarà considerata valida, in caso contrario sarà necessario rieseguire nuovamente l'acquisizione e al controllo degli output delle funzioni di hashing. I metodi più utilizzati per garantire l'integrità del dato digitale sono il calcolo mediante md5sum e sha1sum; nel nostro caso il calcolo dell'impronta sarà eseguito con md5sum con il comando `md5sum /dev/sdb1` per il device e `md5sum /home/utente/analisi/chiavettausb.img` (vedi Fig. 3) per l'immagine acquisita o sha1sum con il comando `sha1sum /dev/sdb1` per il device e `sha1sum /home/utente/analisi/chiavettausb.img` per l'immagine acquisita se decidiamo di utilizzare sha1sum (vedi Fig. 3).

Advanced Forensics Format

Advanced Forensic Format (AFF) è una recente implementazione open source ed estensibile distribuita sotto licenza BSD modificata di un formato che analogamente alla normale bitstream image memorizza l'immagine in maniera compressa e indirizzabile consentendo la memorizzare di meta informazioni sia all'interno del file che in un file esterno collegato a quello di riferimento; attualmente AFF è un formato ancora giovane ma ha tutte le carte in regola per poter diventare uno degli standard più utilizzati nel campo delle acquisizioni informatico forensi questo perché:

- a prodotti simili, AFF mentre esegue l'acquisizione del reperto calcola anche lo hash SHA1 e MD5 dell'immagine grezza consentendo un sostanzioso risparmio di tempo rispetto alle procedure a più passi;
- a prodotti simili, AFF consente di creare l'immagine dei dati grezzi compressa permettendo l'apertura e la lettura del file senza dover decomprimere in un secondo momento l'immagine;
- a prodotti simili, AFF consente una visualizzazione a elevata usabilità di informazioni dettagliate riguardanti i segment, meta informazioni, dati sullo hash dei singoli file;

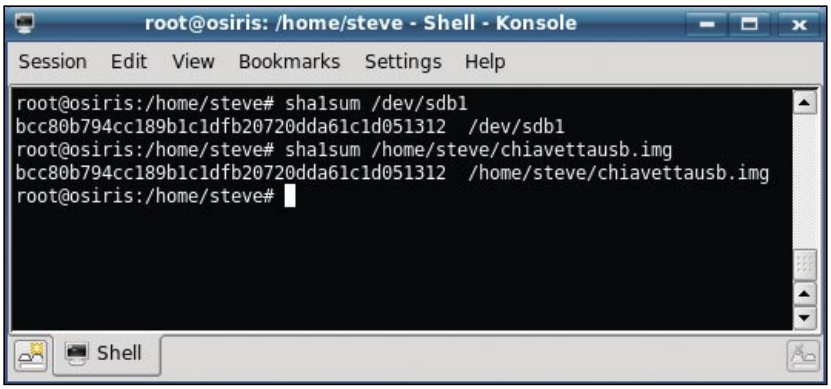

Fig. 4: *Confronto dello hash sha1 del device e dell'immagine acquisita*

- a prodotti simili, AFF produce file compressi più piccoli;

AFF è composto da una serie di tool che permettono di acquisire e di mantenere la bitstream del device che abbiamo acquisito. Nel nostro caso se avessimo voluto acquisire in formato AFF la chiavetta usb avremmo dovuto utilizzare aimage con la seguente sintassi: `aimage /dev/sdb1 /home/utente/analisi/chiavettausb.aff` (vedi Fig. 5).

Acquisizione di device in sistemi raid

Tutte queste operazioni possono essere eseguite in scenari diversi, a seconda delle caratteristiche dell'hardware dei device che dobbiamo acquisire. Questa premessa è d'obbligo perché nel caso dovessimo acquisire un sistema con ad esempio hard disk in raid 5, la singola acquisizione dei dispositivi sarà totalmente inutile perché non avendo a disposizione gli algoritmi utilizzati dal controller raid, non saremo mai in grado di leggere in modo corretto i dati pertanto il reperto in questione sarà inutilizzabile; in questi casi è d'obbligo attuare l'acquisizione localmente sulla macchina avviando il computer in modo tale che il controller renda disponibile la corretta lettura del sistema raid per poi poter utilizzare un live cd Linux per la Computer Forensics, come ad esempio DEFT Linux, acquisendo il contenuto del raid come se fosse un normale hard disk stand alone.

Analisi

Una volta acquisiti i dati, è necessario procedere all'analisi degli stessi mediante procedure eseguite esclusivamente sulle copie fedeli dei device acquisiti. l'analisi deve essere in grado di rintracciare tutte le possibili prove informatiche utili ai fini probatori, e a tal fine, i dispositivi di memoria offrono una considerevole quantità di informazioni, spesso però non sempre facili da visualizzare come ad esempio il recupero, anche se parziale, di dati cancellati risultanti spesso fondamentali per

l'analisi. La valutazione delle informazioni contenute all'interno dei dati è un'operazione generalmente molto semplice salvo quando abbiamo a che fare con il trattamento di dati ove vi è una necessità di conoscenze aggiunte come file codificati con sistemi crittografici. Nell'ambito dei software open source il programma leader per l'analisi forense di reperti è lo Sleuth Kit utilizzato mediante Autopsy.

Autopsy

Sleuth Kit ed Autopsy costituiscono un ottimo framework open source per l'analisi di immagini e device con supporto ad alcuni (manca purtroppo il supporto per i file system hfs e hfs+) dei più diffusi file system come:

- FAT 12, 16 e 32,
- NTFS,
- EXT 2 e 3,
- UFS,
- ISO 9660,
- File System per sistemi Solaris,
- File System per sistemi Bsd e Free Bsd,
- Raw,
- Swap.

Diversamente dalla maggior parte delle piattaforme di computer forensics, la struttura è completamente modulare questo perché Sleuth Kit non è un programma ma un insieme di tool a linea di comando, ognuno dei quali esegue operazioni specifiche; Autopsy invece fornisce l'interfaccia grafica e l'ambiente di collegamento dei vari programmi. La caratteristica che lo rende un software per la computer forensics è la garanzia di inalterabilità dei dati analizzati questo perché l'accesso ad essi viene effettuato in sola lettura con controlli che impongono agli applicativi, che compongono lo sleuthkit, una inalterabilità dei file posti ad analisi. Le principali funzioni di Autopsy sono:

- calcolo di hash md5,
- analisi di device,
- recupero ed esportazione di file cancellati,
- ricerche con parole chiave su file, settori allocati e non allocati,
- analizzare ogni singolo inode del device acquisito,
- creazione di timeline,
- aggiungere note di contorno al caso,
- creazione di report automatici riassuntivi del caso.

Una semplice analisi del reperto utilizzando Autopsy

Autopsy supporta nativamente sia bitstreame grezze, come quelle acquisite mediante ddrescue, sia bitstreame avanzate, come quelle acquisite in formato AFF o EnCase. Obiettivamente la fase di analisi è la parte che meno si può standardizzare questo perché a seconda dell'esigenze la persona che deve eseguire l'analisi può approcciare il caso con diverse metodologie; ad esempio, se nel nostro caso dobbiamo trovare dei file che sappiamo per certi cancellati dall'utente utilizzatore della nostra chiavetta, Autopsy ci permette di lavorare solo e solamente sui file cancellati

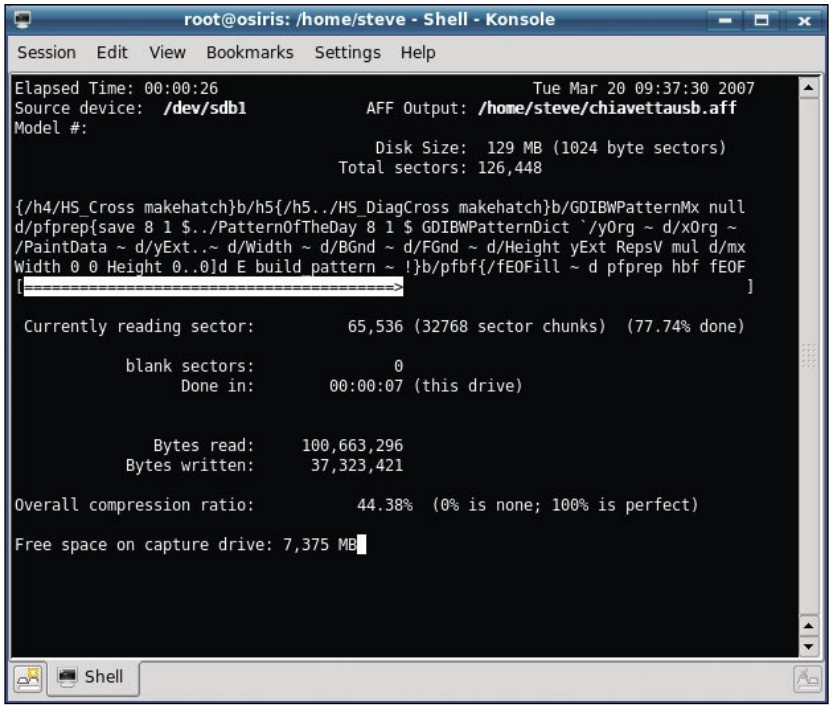

Fig. 5: *Acquisizione utilizzando aimage*

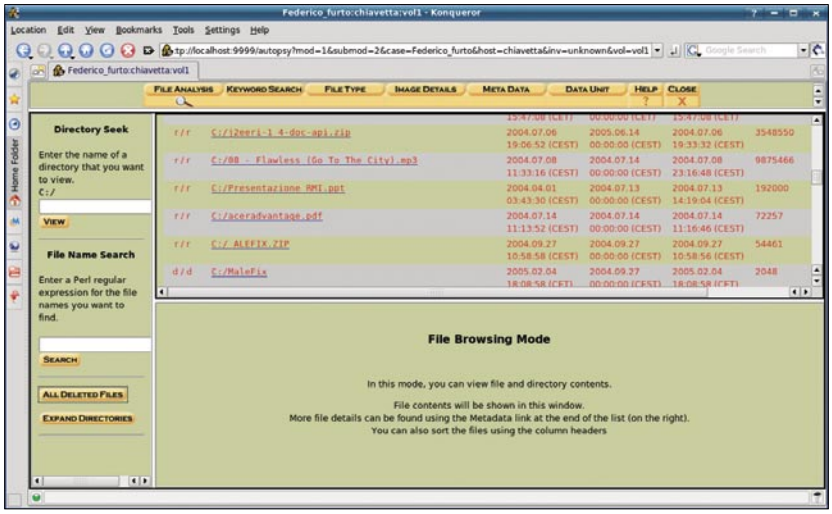

Fig. 6: *Autopsy in modalità All deleted files*

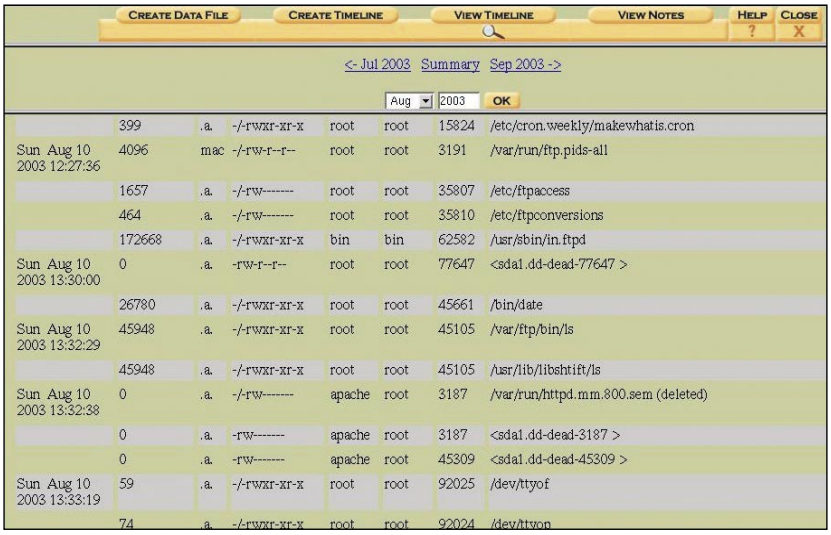

Fig. 7: *Timeline con Autopsy*

nel device da noi selezionato, al contrario, sempre secondo nostre esigenze, possiamo decidere di lavorare in modalità standard quindi attuare la visualizzazione completa del contenuto del file system acquisito (Fig. 5).

Timeline

Un elemento fondamentale nella scenda del crimine è il tempo. Esso è uno dei punti di riferimento principali quando dobbiamo effettuare una qualsiasi azione all'interno dei dati posti ad analisi; per esempio nel caso tipico in cui le forze dell'ordine hanno a che fare con un cadavere, la prima cosa che viene chiesta al medico legale è per l'appunto stabilire data ed ora del decesso. Nel nostro caso avere dei punti di riferimento temporali può aiutare la ricerca e l'analisi dei dati, al contrario senza aver un riferimento temporale, la ricerca di evidenze sarebbe effettuata senza nessuna metodologia, andando letteralmente a caso, correndo il rischio di perdere dati fondamentali per il caso in anlisi. Nell'informatica forense per timeline si intende una fotografia di tutti gli eventi storici avvenuti in un determinato sistema. Essa viene creata mettendo in ordine cronologico tutti gli eventi successi in un determinato tempo di vita del sistema posto ad analisi. Possiamo quindi affermare che, metaforicamente parlando, una timeline ci permette di viaggiare nel tempo potendo cosi risalire ad ogni singola azione avvenuta in un arco di tempo definito dall'esaminatore, creatore della timeline. C'è però da precisare che la timeline viene creata a seconda della data del sistema, pertanto se ad esempio il proprietario del pc che stiamo analizzando non si è mai posto il problema di impostare correttamente la data del sistema operativo, i riferimenti temporali potrebbero essere completamente inattendibili, pertanto prima di dare per attendibile una Timeline bisognerebbe assicurarsi che il sistema, sin dalla sua prima accenzione, abbia sempre avuto i riferimenti temporali corretti. In Autopsy è possibile creare Timeline.

Riassunto

L'articolo introduce l'informatica forense trattando due (acquisizione ed analisi) delle quattro fasi inerenti al trattamento del reperto informatico mostrando le potenzialità dei tool open source, ormai entrati negli standard dei software per la computer forensics, introducendo la libreria advanced forensics format, Autopsy e il concetto di Timeline, questultimo fondamentale per gli inquadramenti temporali delle azioni avvenute all'interno del sistema posto in analisi. ●

Terminologia

- Bitstream image: copia grezza dal primo fino all'utimo bit di un dispositivo di memoria
- EnCase: software closed source leader nella Computer Forensics

In Rete

- *http://www.sleuthkit.org* – sito ufficiale dello Sleuth Kit,
- *http://www.stevelab.net/deft* – sito ufficiale di DEFT Linux
- *http://www.forensikswiki.org* – un wiki dedicato alla Computer Forensics.
- *http://www.afflib.org* – sito ufficiale dell'Advanced Forensics Format

Cenni sull'autore

Stefano Fratepietro è dottore in Information Technology & Management (Università di Bologna, dipartimento di Informatica) con tesi di laurea in Informatica forense. Lavora da molti anni nel settore dell'informatica come sistemista di reti miste (Linux, Mac, Solaris e Windows), attualmente è sistemista presso il CIRSFID (Centro di Ricerca in Storia del Diritto, Filosofia e Sociologia del Diritto e Informatica Giuridica) Università di Bologna, ed è a capo di Yourside.it attività che fornisce soluzioni informatiche nel campo della sicurezza e della computer forensics; collabora con il prof. Cesare Maioli per il corso di informatica forense presso la facoltà di Giurisprudenza dell' Università di Bologna; creatore e sviluppatore di DEFT Linux, si occupa di ricerca in campo informatico forense e pratica attività peritali per tribunali e privati.