La computer forensics come strumento di supporto delle strutture di auditing nelle indagini interne aziendali

Studio Informatica Forense e sicurezza Informatica

Dott. Alessandro Fiorenzi
Consulente Sicurezza Informatica e Computer Forensics
Delegato Clusit in tema di Computer Forensics

alessandro@alessandrofiorenzi.it
www.alessandrofiorenzi.it www.studioinformaticaforense.it

Compiti Internal Auditing

Internal Auditing è :

- un'attività indipendente e obiettiva di "assurance" e consulenza, finalizzata al miglioramento dell'efficacia e dell'efficienza dell'organizzazione.
- Assiste l'organizzazione nel perseguimento dei propri obiettivi tramite un approccio professionale sistematico, che genera valore aggiunto in quanto finalizzato a valutare e migliorare i processi di controllo, di gestione dei rischi e di corporate governance.

Tipi di audit

Management audit o audit direzionale o audit strategico	• Analizza le attività di definizione e comunicazione degli obiettivi strategici di business e di rischio correlato, verificando nel tempo la coerenza dei comportamenti gestionali, tattici/operativi rispetto alle strategie/obiettivi dati dal CdA e DG (governance operativa), analizzando gli eventuali scostamenti di concerto con controllo di gestione e gestione del rischio; verifica l'adeguatezza e la coerenza dei supporti e delle informazioni disponibili. A questa categoria viene di fatto compreso l'audit sulle frodi, il quale rileva malversazioni/frodi perpetrate ai danni dell'azienda da parte di dipendenti e/o soggetti esterni.
Operational audit o audit tecnico-operativo	• Verifica o valuta l'adeguatezza, regolarità, affidabilità e funzionalità dei sistemi, processi e procedure, dei metodi (codificazione) e delle risorse in rapporto agli obiettivi, delle strutture organizzative.
Compliance audit o audit di conformità	• **Assicura l'effettiva attuazione del sistema di controllo (procedure previste e regolarità dei comportamenti) per la conformità dei processi alla regolamentazione interna (procedure) e esterna (leggi). L'IA interviene sulle cause che hanno portato scostamenti dal bilancio del consiglio di decisione e gestione.**
Financial audit o audit finanziario	• Audit contabile con esame dei sistemi informativi contabili e delle risultanze numeriche periodiche di bilancio; ricompreso nell'attività della società di revisione esterna ma senza sovrapposizioni.
IT audit o revisione dei sistemi informativi	• **Consiste in un processo di verifica sulla conformità dei sistemi informativi di un'organizzazione a quanto previsto da norme, regolamenti o pratiche interne.**
Audit sui progetti	• L'organizzazione deve disporre di strumenti e competenze per identificare i rischi dei propri progetti, strategie per ridurli o eliminarli; migliorare la capacità di effettuare analisi causa-effetto, per risalire alle motivazioni prime di eventi che determinano la gestione di progetto; migliorare la capacità di monitorare o gestire i progetti a tutti i livelli aziendali.

Processo di Audit

Il processo di auditing deve essere sistematico e ben documentato. Generalmente si compone dei seguenti passi:

- Analisi dei rischi
- Definizione degli obiettivi
- Pianificazione
- **Raccolta evidenze**
- Conclusioni e raccomandazioni
- Rapporto di Audit

Evidenze di audit

Metodi Raccolta Evidenze

- Esame documentale
- Registrazioni
- Interviste
- Riscontri ispettivi
- Campionamenti
- ecc

E’ sufficiente oggi?

Nuovi scenari dell'audit 1/2

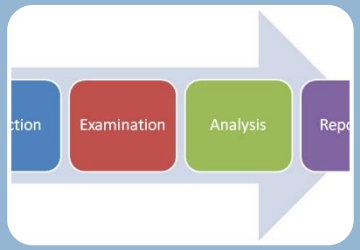
L'Internal Auditing è spesso il braccio armato a cui si rivolgono diversi uffici in azienda

- Compliance aziendale
- Affari legali
- HR

Si ricorre agli uffici di Auditing per cercare evidenze di inadempienze, illeciti o reati a cui dare seguito con azioni disciplinari o l'apertura di procedimenti civili o penali.

Nuovi scenari dell'Auditing 2/2

I metodi tradizionali della raccolta delle evidenze, in ambito Audit non sono sufficienti a garantire l'accettabilità della prova in giudizio.



E' necessario un nuovo approccio che per le evidenze raccolte garantisca

- Accettabilità
- Autenticità
- Completezza
- Attendibilità

La Computer Forensics è la risposta metodologica e scientifica per gestire le prove IT

Computer Forensics

La “Computer Forensic” è la disciplina scientifica che si occupa di, identificare, preservare e analizzare i dati dei sistemi informativi e informatici al fine di evidenziare l’esistenza di fonti di prova digitale, resistenti ad eventuali contestazioni circa la propria solidità e capacità probatoria sia in ambito civile che penale

Nasce nel 1984 dal CART (computer analysis and response team) internamente ad FBI

La CF giunge alla ribalta dei media solo recentemente in seguito all’incremento dei crimini informatici e dei crimini commessi con l’ausilio di strumenti informatici/digitali

Quando eseguire un accertamento tecnico informatico di computer forensics

Dopo l'illecito/reato

- E' eseguito dalle FFOO
- Permette di cristallizzare l'evidenza dell'illecito o reato
- Viene eseguito prevalentemente sul dispositivi del sospettato
- Non valuta le eventuali prove della parte lesa
- Alto rischio compromissione/alterazione delle prove

Indagini difensive preventive

- Permettono di valutare la tenuta dell'accusa prima della denuncia querela.
- Permettono di cristallizzare le prove
- Preservano le prove da atti di distruzione sottrazione
- Le prove si costituiscono su elementi della parte lesa
- Costituiscono un fascicolo di prove di accusa

Dove si può trovare una prova informatica?

Computer (desktop, portatili, server, appliance)

Stampanti (tutte hanno una busybox linux)

Memorie di massa (cd, dvd, pendrive, nastri, etc…)

Cellulari, smartpone, blackberry, tablet,

Servizi Internet e Intranet: siti web, forum, mail server, instant messaging, p2p, voip , social network etc…

In definitiva tutto ciò che implementa un software, quindi anche:

- Un navigatore satellitare
- Una xbox
- Un POS (terminali di pagamento)
- Il computer di bordo di un'auto

La prova informatica è una prova atipica e quindi deve essere trattata con metodi scientifici che siano di garanzia nelle fasi di acquisizione, custodia, analisi ed estrazione delle evidenze.

Prova digitale vs prova tradizionale

La prova tradizionale

- tipicamente presenta le caratteristiche di tangibilità, misurabilità ed è definita

La prova informatica /digitale

- INTANGIBILE: è costituita da file, trasmissioni, più in generale dati distribuiti sulla rete aziendale o addirittura in Internet
- VOLATILE le tracce informatiche in ragione del dispositivo in cui sono memorizzate possono essere più o meno persistenti nel tempo. In ordine di volatilità decrescente: registri di memoria, ram, stato della rete, processi (programmi) attivi, file temporanei, dischi, log, floppy, nastri, cd, dvd, stampe.
- ALTERABILE la prova informatica/digitale può essere facilmente alterata=compromessa o addirittura distrutta senza che ne rimanga traccia, o senza trovarsi in prossimità del dispositivo come nel caso di cancellazione contenuti su Internet , reset remoto iPad etc..

Principi della Computer Forensics

Limitare al minimo l'impatto

- Non nuocere, ovvero porre la massima attenzione nelle azioni che si intraprendono evitando di andare a compromettere sistemi e supporti che potrebbero contenere tracce
- Utilizzare procedure non invasive

Applicare la catena di custodia

Documentare ogni intervento

Operare le analisi su una copia dell'immagine acquisita

I passi della Computer Forensics

Identificazione

- Isolare e analizzare la scena del crimine o illecito
- identificare ciò che può costituire o contenere una prova,

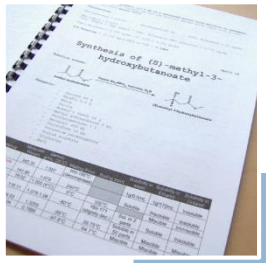
Acquisizione e conservazione

- Acquisizione
  - Copia Bit a Bit del supporto digitale verificando l'integrità della copia con funzioni di hash
  - Quando non può essere fatta una copia dei supporti, si deve provvedere ad adottare una soluzione che permetta di mantenere integri i dati e i metadati (NO Copia e Incolla di file: si perdono i metadati)
- Conservazione
  - Una volta in possesso della copia forense e dell'originale, occorre documentare come questi vengono conservati. Questa **è la catena di custodia, che fornisce la documentazione provante che l'integrità dei dati è stata preservata e non c'è stata alcuna modifica, seppur casuale**

Analsi e Presentazione

Analisi

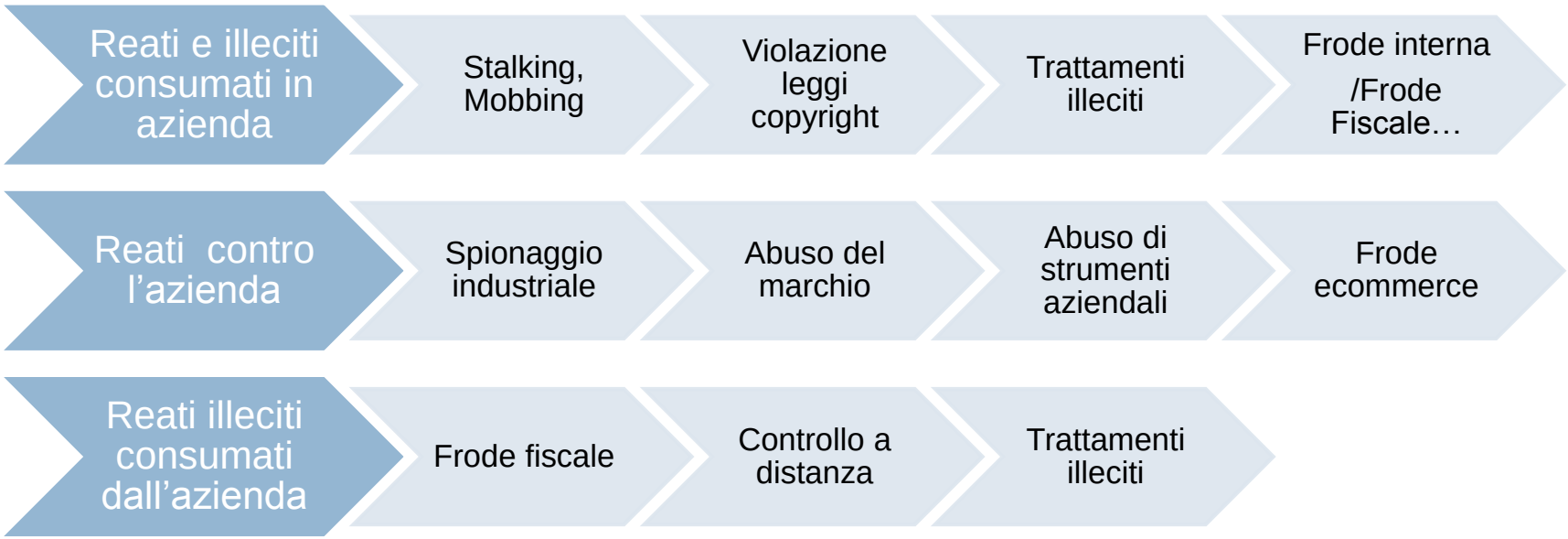
- E' la fase di indagini tecniche volte alla ricerca di specifiche evidenze. Può riguardare
- Documenti (DOC, XLS, PDF, …)
- Immagini
- Email , PEC, navigazione web, chat, skype
- P2P, Torrent, Emule
- Database
- File di Log
- Registri di sistema e ActiveData Stream
- File cancellati
- File nascosti
- SlackSpace
- Bad Blocks
- Steganografia
- File cifrati
- Partizioni nascoste
- Sms,
- Rubrica telefonica,
- Elenco chiamate in ingresso uscita,
- Dati GPS
- Contenuti
- Al termine dell'analisi deve essere fatta la verifica della



Presentazione:

- i risultati devono essere presentati in forma comprensibile sia a tecnici che non, documentando ogni passo eseguito per il rinvenimento delle evidenze al fine di rendere l'accertamento verificabile e non opponibile

Aziende: reati e illeciti legati all'uso delle tecnologie informatiche



E tutti quei reati e illeciti tradizionali consumati con l'ausilio di strumenti informatici o a danno di essi

Le specializzazione della Computer Forensics

Computer Forensics

- tratta l'acquisizione e la ricerca delle prove presenti su desktop, portatili, server o in programmi eseguiti all'interno di questi sistemi

Network Forensics

- Tratta l'acquisizione e la ricerca delle prove presenti in rete, che si tratti di lan aziendale piuttosto che di Internet

Mobile Forensics

- Tratta l'acquisizione e la ricerca delle prove presenti su dispositivi cellulari, palmari, smartphone, tablet

Computer Forenscis

Acquisizione legittima della prova da un computer

- Definizione della Catena di custodia per i reperti da acquisire
- Utilizzo di dispositivi di write blocker per la protezione del supporto
- Hashing del supporto originale
- Copia bit a bit indicata anche come bitstream
- Verifica hash della copia con hash originale
- Analisi con strumenti ad hoc Open Source o commerciali ma specifici per il tipo di ricerca

E quando non è possibile?

- Dischi troppo grandi
- Impossibilità di fermare un server per l'acquisizione forense
- Etc…
  - In tutti i casi in cui non è possibile procedere alla copia del disco, si devono adottare soluzioni che siano di garanzia rispetto al contenuto originale, adottando anche soluzioni di firma elettronica digitale con marca temporale per dare un riferimento temporale certo e valore legale

Evidence su Internet: altissima volatilità

Una prova che si trova su internet accentua, rispetto ad una che si trova su computer o cellulari, le caratteristiche di	Infatti può essere:	Il tutto in tempi estremamente rapidi, da un qualsiasi punto del globo collegato ad Internet
• Volatilità • Fragilità = facilmente alterabile	• Rimossa • Spostata su un altro sito • Sovrascritta	

Come procedere

- Acquisire tempestivamente la prova prima che venga alterata o rimossa
- Garantire la catena di custodia
- Assicurare che i dati originali non vengano alterati
- Usare tecniche e strumenti per garantire la ripetibilità degli accertamenti
- Garantire la conservazione e l'accesso nel tempo

Problematiche della prova Internet

La prova che si trova su internet presenta inoltre altri gravi problemi di identificazione e tutela

- Non è facile comprendere dove si trova. Il fatto che sia all'interno di una pagina web non significa che sia ospitata su quel sito ma potrebbe essere un contenuto proveniente da altri siti
- Transnazionalità: potrebbe trovarsi su sistemi in Italia o all'estero. Non sempre esistono accordi internazionali o bilaterali di collaborazione fra le polizie e taluni reati non sono considerati tali in altri paesi
- E' spesso impossibile procedere ad un sequestro tradizionale per motivi tecnici (grosse basi di dati, storage con TB di dischi, sistemi virtualizzati complessi etc..) o economici (blocco dell'attività aziendale e perdita di business)
- Difficoltà ad individuare l'owner del sito: la prova potrebbe trovarsi su server in housing o in hosting presso un service provider coinvolgendo soggetti diversi
- L'autore della prova può alterarla, nasconderla o addirittura distruggerla più facilmente su internet rispetto al caso in cui fosse sul suo computer o cellulare

Network Forensics Acquisizione 1/3

Quindi come possiamo acquisire una prova che è su un forum, un blog, un social network o su una pagina web, su un server nntp, o le evidenze degli SLA di un servizio di hosting ?

- Non con gli strumenti classici della CF
- Non facendo screenshot
- Non salvando la pagina in locale e stampandola

Non sono metodi validi

Network Forensics Acquisizione 2/3

Come è quindi possibile costituire una prova che sia una istantanea di un contenuto presente su intenet alla data corrente, e sia accettabile da un giudice?

Ci viene in aiuto il provvedimento della Corte di Cassazione Sezione Lavoro n. 2912 del 18 febbraio 2004, Pres. Mattone, Rel. Spanò secondo la quale:

"AltaLex(http://www.altalex.com/index.php?idnot=6991 ***): La copia di una "pagina web" su supporto cartaceo ha valore probatorio solo se raccolta con le dovute garanzie****.*

Per la rispondenza all'originale e la riferibilità ad un momento ben individuato - Le informazioni tratte da una rete telematica sono per loro natura volatili e suscettibili di continua trasformazione.

Va escluso che costituisca documento utile ai fini probatori una copia di "pagina web" su supporto cartaceo che non risulti essere stata raccolta con garanzia di rispondenza all'originale e di riferibilità a un ben individuato momento *(Cassazione Sezione Lavoro n. 2912 del 18 febbraio 2004, Pres. Mattone, Rel. Spanò).*

Network Forensics Acquisizione 3/3

Il procedimento di acquisizione può variare in ragione della tipologia di prova che cerchiamo di cristallizzare ma in linea di massima è riconducibile ai seguenti passi

Registrazione traffico di rete. Questa operazione ci permette di registrare tutte le interazioni che si svilupperanno nel mirror o nella copia del sito. Così facendo si catturerà il traffico comprensivo di

- Richieste client
- Header dei server
- Risposte dei server

Effettuare una sincronizzazione ntp del proprio sistema con un server ntp riconosciuto a livello internazonale (p.e. Tempo universale Galileo Ferraris; anche questa operazione viene registrata sul traffico di rete)

Identificare il proprio indirizzo IP statico: è quello che dovrà essere riportato nel verbale di acquisizione e sarà presente nei log del webserver o del servizio che acquisiamo.

Navigare o copiare le pagine web interessate, la loro navigazione, o le operazioni che ci conducano alla prova che cerchiamo

Firmare digitalmente e con marca temporale il file del traffico di rete

Estrazione della prova

Lavorando **su una copia dei dati acquisti** si può procedere a:

Se si è effettuato un mirror (copia di un sito): aprire le pagine interessate e fornirne una copia in formato pdf/a firmato digitalmente con marca temporale	Estrarre, dal dump del traffico di rete, con soluzioni come xplico il dato di interesse, foto, immagini, documenti, chat, voce etc.… E firmarla digitalmente con marca temporale.	Documentare dettagliatamente tutto quello che è stato fatto spiegando perché sono stati utilizzati certi strumenti e quale è l'output di ogni strumento utilizzato, ricordandosi che Avvocati e Giudici non sono Tecnici

Mobile Forensics

Cellulari, smartphone tablet uniscono le funzionalità tipiche del telefono a quelle tipiche dei computer

Sono privi di standard

- Hw non standardizzato
- Sistemi Operativi (Linux, Android, iOs, Windows Mobile, RIM OS,Pal OS, Symbian, Bada etc.)
- Android: molte customizzazioni
- Filesystem proprietari

Alcuni modelli non sono supportati totalmente dai software di acquisizione forense

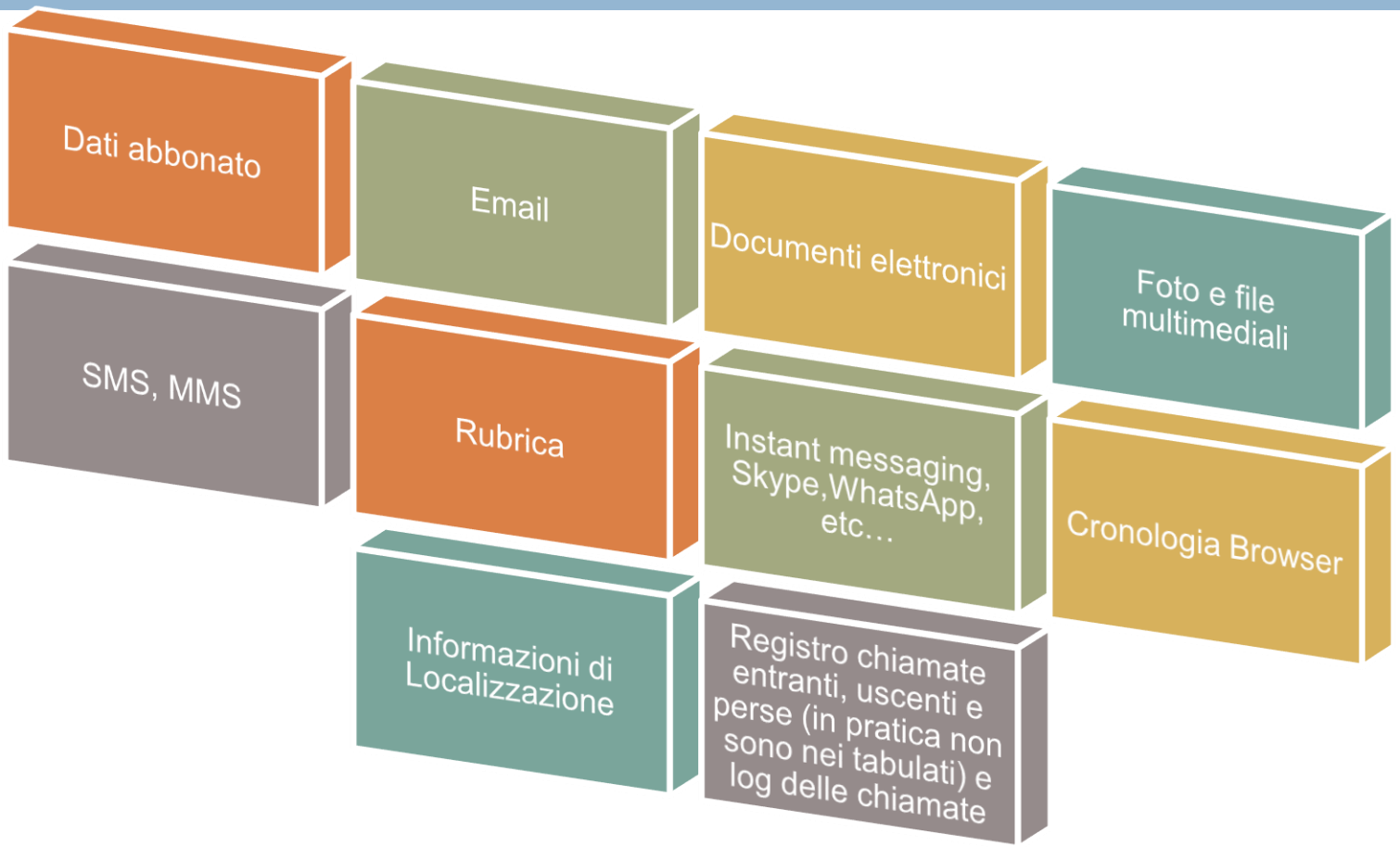
Spesso si tratta di accertamenti non ripetibli.

Mobile Forensics - Acquisizione

Telefono rinvenuto Acceso/spento:	• PIN, script di pulizia, etc..
Isolamento radio del telefono	• Alterazione dati presenti collegamenti con reti Wi-Fi, GSM, UMTS, Bluetooth • Accesso e manipolazione remota (iPad p.e)
Alimentazione e collegamenti	• Telefono isolato aumenta i consumi • Cavi di collegamento

Acquisizione	• Fisica:copia bit a bit della memoria fisica del dispositivo
	  • pochi software, richiede molto tempo, fornisce molte informazioni
	• Logica; copia bit a bit degli oggetti di memoria logici
	  • Ampiamente supportata, richiede meno tempo, fornisce meno informazioni,

Le prove in un cellulare



In conclusione

L'Auditing IT oggi cambia faccia rispetto al passato

- E' diventato il braccio armato dell'ufficio legale, compliance e dell'HR
- Ha il compito di raccogliere le evidenze informatiche con metodi forensi
- Ha il compito di monitorare, e tutelare il sistema informativo IT
- Ha bisogno di maggiori skill tecnici rispetto al passato

ISO 27001, PCI-DSS etc… già contemplano nella funzioni di controllo, tipiche dell'Auditing, le competenze di computer forensics sa tutela dell'azienda e della prova.

Grazie

Studio Informatica Forense

Dott. Alessandro Fiorenzi

Consulente Sicurezza Informatica e Computer Forensic

www.alessandrofiorenzi.it
www.studioinformaticaforense.it
alessandro@alessandrofiorenzi.it
Mobile: 348/7920172