DIIES Dipartimento di
INGEGNERIA
dell'INFORMAZIONE, delle INFRASTRUTTURE e dell'ENERGIA SOSTENIBILE

Corso di Tecnologie per la sicurezza informatica

Incident Response & Digital Forensics

Metodologie e Simulazioni di Indagine

19 aprile 2018

Agenda

- Definizioni e metodologie
- Incident Response: la risposta agli incidenti informatici
  - Definizione di un modello organizzativo per casi
  - Scoperta e notifica degli eventi
  - Valutazione degli eventi
- Digital Forensics: la gestione del reperto informatico
  - Identificazione
  - Raccolta
  - Acquisizione
  - Conservazione
  - Analisi e Interpretazione
- Considerazioni finali ed Aspetti giuridici

Introduzione

Definizioni

Metodologie

ISO/IEC 27000-series

- La serie ISO/IEC 27000 - **Information security management systems** raggruppa un insieme di norme che hanno lo scopo di proteggere le informazioni che vengono mantenute ed elaborate da un'organizzazione.
- Attraverso questa famiglia di standard, le organizzazioni possono sviluppare ed implementare un proprio framework per la gestione della sicurezza delle proprie risorse informative.
- Le informazioni vengono protette da possibili attacchi informatici, errori umani, calamità naturali o da qualsiasi altra vulnerabilità che si può presentare durante l'utilizzo di un sistema informatico.
- Data la natura dinamica del rischio e della sicurezza delle informazioni, il ISMS incorpora un feedback continuo e attività di miglioramento per rispondere ai cambiamenti delle minacce, delle vulnerabilità o degli impatti degli incidenti.

ISO/IEC 27000-guidelines

ISO/IEC 27035-1:2016 ISO/IEC 27035-2:2016

Information security incident management

Part 1: Principles of incident management - Part 2: Guidelines to plan and prepare for incident response

ISO/IEC 27041:2015

Guidance on assuring suitability and adequacy of incident investigative method

ISO/IEC 27043:2015

Incident investigation principles and processes

ISO/IEC 27037:2012

Guidelines for identification, collection, acquisition and preservation of digital evidence

ISO/IEC 27042:2015

Guidelines for the analysis and interpretation of digital evidence

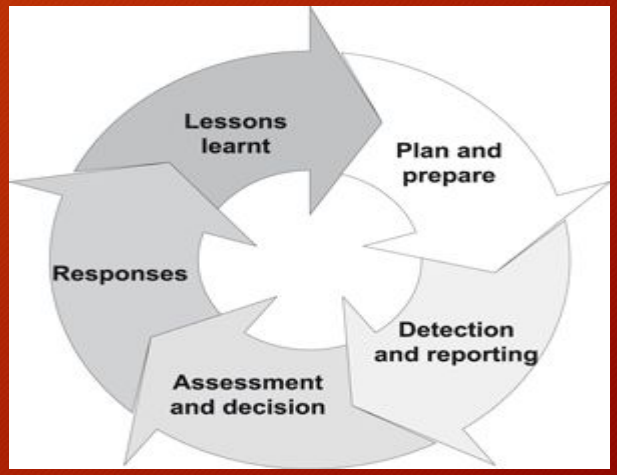
ISO/IEC 27050-1:2016 ISO/IEC 27050-2:dev ISO/IEC 27050-3:2017

Electronic discovery

ISO/IEC 27035

Lo standard 27035 fornisce delle linee guida per l'implementazione di procedure e controlli al fine di creare un approccio strutturato per la gestione degli incidenti informatici. Tale standard ha come obiettivo la minimizzazione degli impatti negativi che un incidente informatico può avere sul business aziendale, attraverso il contenimento dell'incidente, la rimozione della causa scatenante, l'analisi delle conseguenze e il successivo controllo di non occorrenza.

Per poter garantire il raggiungimento degli obiettivi appena descritti il processo di gestione degli incidenti viene suddiviso in cinque fasi, ciascuna contenente determinate attività, incluse in un ciclo che dall'ultima ritorna poi alla prima.



ISO/IEC 27035-key stages

1. **Prepare** (Pianificazione e preparazione)
   - (a) politiche di gestione degli incidenti di sicurezza
   - (b) politiche di gestione della sicurezza e dei rischi
   - (c) sistema di gestione degli incidenti di sicurezza
   - (d) formazione dell'ISIRT
   - (e) supporto (tecnico e di altro tipo)
   - (f) formazione sulla consapevolezza nella gestione degli incidenti di sicurezza
   - (g) test del sistema di gestione degli incidenti di sicurezza
2. **Identify** (Scoperta e notifica)
   - scoperta di un incidente e notifica alle appropriate funzioni aziendali
3. **Assess** (Valutazione e decisione)
   - valutazione dell'evento e decisione di classificarlo come evento di sicurezza

ISO/IEC 27035-key stages

4. **Respond of incident** (Risposta)
   - (a) risposte agli incidenti di sicurezza informatica, ivi incluse operazioni di analisi forense
   - (b) riprendersi da un incidente di sicurezza informatica
5. **Learn the lessons** (Lezioni apprese)
   - (a) analisi forensi più approfondite (se necessario)
   - (b) identificazione della lezione appresa
   - (c) identificazione e attuazione dei miglioramenti al sistema di sicurezza
   - (d) identificazione e attuazione dei miglioramenti alle valutazioni dei rischi di sicurezza
   - (e) identificazione e attuazione dei miglioramenti al sistema di gestione degli incidenti di sicurezza

ISO/IEC 27041

La ISO/IEC 27041 «Guidance on assuring suitability and adequacy of incident investigative method" fornisce una guida sui meccanismi per garantire che i metodi e i processi utilizzati nelle indagini sugli incidenti di sicurezza delle informazioni siano "adatti allo scopo".

Include le migliori metodologie per:

- la definizione dei requisiti,
- la descrizione dei metodi,
- la dimostrazione che le implementazioni dei metodi sono in grado di soddisfare i requisiti,
- la verifica dei test sui fornitori esterni utilizzabili per assistere il processo di validazione.

ISO/IEC 27043

La ISO/IEC 27043 «Incident investigation principles and processes» fornisce le linee guida basate sui modelli idealizzati per processi di investigazione su incidenti comuni che coinvolgono prove digitali.

Ciò include i processi che vanno dalla preparazione pre-incidente fino alla chiusura delle indagini, nonché qualsiasi altro suggerimento generale e alert su tali processi.

Le linee guida descrivono i processi e i principi applicabili a diversi tipi di indagini, inclusi, a titolo esemplificativo ma non esaustivo:

- Accesso non autorizzato
- Alterazione/perdita dei dati
- Arresti anomali del sistema
- Violazioni della sicurezza delle informazioni aziendali

ISO/IEC 27037

Lo standard 27037 dal titolo “Guidelines for identification, collection, acquisition, and preservation of digital evidence" fornisce delle linee guida relative alla gestione delle potenziali prove digitali, concentrandosi in particolar modo sulle fasi di identificazione, raccolta, acquisizione e preservazione.

Per ogni fase vengono indicate le best practices riconosciute per permettere che la potenziale prova possa essere utilizzata efficacemente in sede processuale, tenendo conto delle possibili (e più comuni) situazioni che l’investigatore può trovarsi a dover affrontare.

ISO/IEC 27037-key role

Vengono inoltre definite tre figure chiave, che si occupano e sono responsabili degli aspetti di gestione della prova digitale menzionati sopra:

1. **il DEFR o Digital Evidence First Responder** è un soggetto autorizzato, formato e qualificato ad agire per primo sulla scena di un incidente per eseguire attività di raccolta ed acquisizione delle prove avendone inoltre la responsabilità di corretta gestione
2. **il DES o Digital Evidence Specialist** è un soggetto che ha le capacità di eseguire le stesse attività eseguite da un DEFR ed in più possiede conoscenze specialistiche ed è in grado di gestire una moltitudine di problematiche tecniche, ad esempio è in grado di portare a termine attività quali acquisizione di rete, di memoria RAM ed ha ampia conoscenza di sistemi operativi e/o Mainframe
3. **l'Incident Response Specialist**, che normalmente è una figura professionale interna all'azienda che si occupa del primo intervento post incidente informatico.

ISO/IEC 27042

La ISO/IEC 27042 «Guidelines for the analysis and interpretation of digital evidence" fornisce una guida sull'analisi e l'interpretazione delle prove digitali in grado di affrontare le questioni di continuità, validità, riproducibilità e ripetibilità.

Include le migliori pratiche per la selezione, la progettazione e l'attuazione dei processi analitici e la registrazione delle informazioni per consentire a tali processi di essere sottoposti a controllo indipendente.

Fornisce indicazioni sui meccanismi appropriati per dimostrare le competenze del gruppo investigativo.

Fornisce un framework, per gli elementi analitici e interpretativi della gestione degli incidenti di sicurezza dei sistemi di informazione, che può essere utilizzato per assistere nell'implementazione di nuovi metodi e fornire uno standard minimo comune per le prove digitali prodotte da tali attività.

ISO/IEC 27050

L’Electronic discovery è il processo che consente di scoprire le informazioni memorizzate elettronicamente (ESI) pertinenti ad una o più parti coinvolte in un'indagine o in un contenzioso, o procedimento simile.

La ISO/IEC 27050 fornisce una panoramica della Electronic discovery. Inoltre, definisce i termini correlati e descrive i concetti, inclusi, ma non limitati per l’identificazione, la conservazione, la raccolta, l’elaborazione, la revisione, l’analisi e la produzione di ESI.

La ISO/IEC 27050 è importante sia per il personale tecnico che non tecnico coinvolto in alcune o tutte le attività di electronic discovery. Le linee guida presenti non si contrappongono alle leggi e normative locali, pertanto l’utente deve prestare attenzione affinchè le previsioni siano conformi ai requisiti giurisdizionali prevalenti.

Incident Response

la risposta agli incidenti informatici

Definizione di un modello organizzativo per casi

Scoperta e notifica degli eventi

Valutazione degli eventi

Incidente informatico

- Nel momento in cui uno degli elementi di sicurezza previsti e in uso all'interno dell'azienda viene aggirato, ad esempio nel caso in cui un utente riesca ad avere accesso ad un sistema a cui non è autorizzato ad accedere, **accade ciò che viene definito incidente informatico** di sicurezza: *"un singolo od una serie di eventi di sicurezza informatica inaspettati o non voluti, che hanno significativa probabilità di compromettere le attività aziendali e minacciare la sicurezza delle informazioni"*.
- L'evento di sicurezza informatica appena menzionato viene definito come *"l'identificata occorrenza di uno stato di sistema, di servizio o di rete che indica una possibile violazione della sicurezza delle informazioni, delle policy o il fallimento dei controlli previsti, o di una situazione precedentemente sconosciuta che potrebbe essere rilevante ai fini della sicurezza"*

Incident response

- L'organizzazione, al verificarsi di eventi di sicurezza, deve essere in grado di verificare rapidamente se tale evento vada considerato un incidente informatico o meno ed eventualmente mettere in atto una serie di metodiche al fine di poter reagire efficacemente alla minaccia rilevata, **attraverso le cosiddette attività di incident response**.
- Tali attività hanno l'obiettivo di garantire la tempestiva identificazione dell'evento, la sua eventuale classificazione in "incidente informatico", le conseguenti operazioni da svolgere tempestivamente nel momento in cui l'evento viene segnalato e le successive attività di investigazione atte a reperire possibili fonti di prova.

Incident response: finalità

Lo scopo dell'Incident response non si limita alla gestione dell'evento, ma interagisce anche con le altre fasi del ciclo di security assessment.

A tal fine distinguiamo:

- **Fase Predittiva / Proattiva**: finalizzata all'analisi dei rischi che possono favorire gli incidenti informatici, le cause scatenanti e le soluzioni per mitigare gli effetti.
- **Fase Reattiva:** in cui vengono definite le modalità, i ruoli e le azioni che devono portare alla risoluzione degli incidenti informatici.
- **Fase Correttiva / Migliorativa**: in cui si esaminano gli incidenti subiti e si studiano le soluzioni idonee ad evitare che riaccadano.

Metodologia strutturata

La metodologia strutturata proposta prevede l'adozione di un modello organizzativo secondo un approccio per casi.

Per ogni caso viene effettuata una analisi di rischio collegata all'evento, viene proposto un metodo per permettere di documentare l'evento stesso ed infine vengono descritte le modalità di trattamento del reperto informatico, utili anche al fine di tracciare il fenomeno.

I casi che vengono presi in esame sono:

- accesso abusivo ad un sistema informatico
- violazione della casella di posta elettronica
- sottrazione di dati relativi a proprietà industriale
  - operata da dipendenti o collaboratori interni
- furto di sistemi informatici

Metodologia strutturata

Di seguito il dettaglio delle attività proposte:

1. Gestione dei rischi (predittiva/proattiva):
   - (a) evento - descrizione e riferimento normativo;
   - (b) identificazione delle possibili cause dell'evento;
   - (c) identificazione delle possibili conseguenze dell'evento;
   - (d) classificazione di rischio associato all'evento, secondo una scala di tipo qualitativo. **Verranno utilizzati i valori L (basso), M (medio), H(alto);**
   - (e) azioni atte a mitigare il livello di rischio rilevato.
   - (f) livello di rischio calcolato al termine del punto e).
2. Scoperta e notifica dell'evento (reattiva):
   - (a) modulo di segnalazione evento.
3. Valutazione e decisione (reattiva):
   - (a) valutazione dell'evento e sua classificazione.
4. Risposta (reattiva):
   - (a) modalità di trattamento del reperto informatico, utili a documentare il fenomeno.

Accesso abusivo:
Analisi del rischio

L'Accesso abusivo ad un sistema informatico o telematico è un reato e come tale è sanzionato ai sensi dell'Art. 615-ter c.p. secondo cui *"Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni[..]"*

Cause

1. SQL/Code injection
2. sistemi non protetti mediante tecnologie di protezione/controllo di accesso
3. insufficienza dei sistemi di protezione/controllo di accesso (es. nessuna limitazione minima sulla lunghezza e/o complessità della password, configurazione errata dei sistemi);
4. mancati aggiornamenti dei sistemi di protezione/controllo di accesso, utili alla risoluzione di vulnerabilità note (come sql injection), spesso sfruttate dagli attaccanti;
5. utilizzo di keylogger (si presuppone in questo caso la disponibilità di accesso fisico alla macchina).

Accesso abusivo:
Analisi del rischio

Conseguenze

Le principali conseguenze di tale evento riguardano la perdita di tutti i principali elementi portanti del concetto stesso di sicurezza informatica:

1. indisponibilità dei servizi
2. violazione dell'integrità dei dati (come la loro alterazione o cancellazione)
3. furto di dati
4. violazione della privatezza degli utilizzatori dei sistemi, che potrebbe sfociare in casi di furto di identità nel caso in cui le informazioni personali degli utenti a cui si riesce ad accedere siano molto dettagliate.

Livello di rischio calcolato

H: alto

M: medio

L: basso

Causa	Probabilitá di occorrenza	Conseguenze	Livello di rischio
1	H	1÷4:H	H
2	L	1÷2:M 3÷4:L	L
3	H	1÷3:H 4:M	H
4	H	1÷3:H 4:M	H
5	M-L	1÷3:H 4:M	M

Accesso abusivo:
Azioni per mitigare il livello di rischio

Per poter mitigare i livelli di rischio individuati occorre sostanzialmente ridurre la probabilità di occorrenza delle cause degli attacchi. In particolare è necessario:

- aggiornare costantemente i sistemi di controllo di accesso, così da ridurre la vulnerabilità agli attacchi noti;
- monitorare il funzionamento di tutti i sistemi, così da poter verificare preventivamente la presenza di errate configurazioni e apportare le dovute correzioni prima che si verifichi un attacco;
- imporre vincoli rigidi di protezione logica e fisica sui sistemi, come ad esempio password lunghe almeno 8 caratteri, da aggiornare periodicamente, sistemi antivirus abilitati e funzionanti, controllo di accesso fisico ai locali.

Livello di rischio mitigato

H: alto

M: medio

L: basso

Causa	Probabilitá di occorrenza	Conseguenze	Livello di rischio
1	L	1÷4:H	M
2	L	1÷2:M 3÷4:L	L
3	L	1÷3:H 4:M	M
4	L	1÷3:H 4:M	M
5	L	1÷3:H 4:M	L

Accesso abusivo:
Trattamento del reperto

In questo caso possiamo distinguere tre reperti informatici, presupponendo di aver già implementato le misure di mitigazione descritte:

1. copia forense del disco del personal computer del dipendente
2. file di log contenenti attività degli utenti sul server
3. filmato di videosorveglianza della stanza in cui risiede il sistema.

Nel primo caso, la costruzione di una timeline delle attività all'interno del personal computer, con particolare focus sul periodo di tempo indicato in fase di segnalazione, unito all'analisi del filmato di videosorveglianza può portare all'individuazione del soggetto che ha compiuto tali azioni e dei dati che sono stati visionati/prelevati abusivamente dal sistema. Tale timeline risulta utile anche nel caso di accesso da remoto.

Nel secondo caso, l'analisi dei file di log risulta molto utile per capire chi si è introdotto e a quali file ha avuto accesso.

Il terzo reperto normalmente serve ad identificare persone fisiche che hanno avuto accesso ai sistemi nella finestra temporale individuata, per cui risulterebbe ad esempio inutile nel caso di un accesso abusivo da remoto.

Violazione della casella di posta elettronica:
Analisi del rischio

Violazione della casella di posta elettronica, tale reato è sanzionato ai sensi dell'Art.616 c.p., secondo cui *"Chiunque prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta, ovvero sottrae o distrae, al fine di prenderne o di farne da altri prendere cognizione, una corrispondenza chiusa o aperta, a lui non diretta, ovvero, in tutto o in parte, la distrugge o sopprime, è punito, se il fatto non è preveduto come reato da altra disposizione di legge, con la reclusione fino a un anno o con la multa da euro 30 a euro 516.[..]*

Cause

1. utilizzo di account/pc condiviso
2. memorizzazione automatica delle credenziali di accesso alla casella di posta
3. mancata esecuzione del logout
4. password banale (es. parole prese da dizionario, nomi di persone/città)
5. utilizzo della postazione di lavoro del dipendente in sua assenza (es. malattia)
6. accesso abusivo

Violazione della casella di posta elettronica: Analisi del rischio

Conseguenze

Le principali conseguenze della violazione di una casella di posta elettronica si possono riassumere in:

1. violazione privacy dell'utilizzatore di tale casella;
2. possibile esposizione di informazioni riservate/critiche per il business aziendale o confidenziali.

Livello di rischio calcolato

H: alto

M: medio

L: basso

Causa	Probabilitá di occorrenza	Conseguenze	Livello di rischio
1	H	1:M 2:H	H
2	H	1:M 2:H	H
3	H	1:M 2:H	H
4	H	1:M 2:H	H
5	H	1:M 2:H	H

Violazione della casella di posta elettronica:
Azioni per mitigare il livello di rischio

Per poter mitigare i livelli di rischio occorre sostanzialmente ridurre la probabilità di occorrenza degli errori umani individuati. In particolare è necessario:

- inibire l'accesso alla casella di posta aziendale dall'esterno dell'azienda.
- nel caso in cui il punto precedente non fosse realizzabile, produrre e far rispettare un regolamento stretto per la consultazione della casella di posta all'esterno dell'ambiente lavorativo;
- non autorizzare la consultazione della casella email attraverso un pc utilizzato da più utenti
- divieto di memorizzare automaticamente le credenziali di accesso alla casella di posta
- imporre limitazioni sulla complessità minima per la password
- utilizzo di inoltro e/o riposta automatici
- utilizzo di meccanismo di logout automatico dall'account di posta se si riscontra inattività dell'utente
- utilizzo di meccanismo di autenticazione con verifica delle credenziali a doppia componente

Livello di rischio mitigato

H: alto

M: medio

L: basso

Causa	Probabilitá di occorrenza	Conseguenze	Livello di rischio
1	L	1:M 2:H	L
2	L	1:M 2:H	L
3	L	1:M 2:H	L
4	M	1:M 2:H	M
5	L	1:M 2:H	L

Violazione della casella di posta elettronica:
Trattamento del reperto

In questo caso possiamo distinguere due reperti informatici, presupponendo di aver già implementato le misure di mitigazione descritte:

1. copia forense del disco del personal computer del dipendente
2. file di log contenenti attività dell'utente sul server di posta

Nel primo caso, la costruzione di una timeline delle attività all'interno del personal computer, con particolare focus sulle attività compiute dall'utente sul client di posta o sul browser possono essere utili per risalire alla causa che ha permesso l'accesso abusivo alla casella di posta ed eventualmente (nel caso di utilizzo del client) comprendere le azioni dell'utente al fine di individuare, ad esempio, l'inoltro di informazioni riservate a persone esterne all'azienda.

Nel secondo caso, l'analisi dei file di log risulta molto utile per comprendere le attività effettuate dall'utente sul server di posta quando ad esempio non è stato possibile risalire alla postazione da cui si è collegato.

Sottrazione di proprietà industriale:
Analisi del rischio

Si applica il reato di furto perchè si considera che i dati prelevati siano contenuti all'interno di un supporto e quindi l'oggetto del furto è il supporto e non il dato.

Cause

1. mancanza di supervisione dei collaboratori interni
2. mancanza di sistemi di controllo di accesso (fisico e logico) ai sistemi e/o ai locali contenenti dati classificati come proprietari
3. possibilità di accesso alla rete aziendale e ai sistemi senza specifici livelli di autorizzazione definiti
4. mancato controllo in ingresso e in uscita dei sistemi in possesso dei dipendenti
5. mancato monitoraggio dell'utilizzo di supporti rimovibili per il trasferimento di informazioni
6. mancato divieto di accesso a piattaforme di file hosting/sharing (come ad esempio Drobpox, Google Drive)
7. recupero di dispositivi o informazioni impropriamente smaltiti
8. intercettazione delle comunicazioni all'interno della rete aziendale
9. errata configurazione dei livelli di autorizzazione (ad es. impiegato che accede ad informazioni confidenziali su accordi finanziari)
10. mansioni e/o aree di responsabilità non correttamente definite, che potrebbero indurre all'errata autorizzazione all'accesso ai dati
11. mancanza o insufficienza di procedure per mantenere in ordine la postazione di lavoro (scrivania e computer).

Sottrazione di proprietà industriale:
Analisi del rischio

Conseguenze

Le conseguenze di tali vulnerabilità riguardano principalmente l'accesso di tali dati da parte di persone non autorizzate che potrebbero utilizzarli per diversi scopi.

Di seguito le conseguenze di maggior rilievo:

1. furto di progetti in via di sviluppo, che potrebbero venir copiati e completati da una azienda concorrente, che otterrebbe quindi un vantaggio competitivo
2. esposizione dell'azienda a ricatti da parte del dipendente/collaboratore interno, che potrebbe esigere dei benefici personali o economici per la restituzione/distruzione dei dati di cui è in possesso
3. danno di immagine per l'azienda.

Causa	Probabilitá di occorrenza	Conseguenze	Livello di rischio
1	H	1÷3:H	H
2	L	1÷3:H	L
3	L	1÷3:H	L
4	M	1÷3:H	M
5	H	1÷3:H	H
6	H	1÷3:H	H
7	H	1÷3:H	H
8	L	1÷3:H	L
9	M	1÷3:H	M
10	M	1÷3:H	M
11	H	1÷3:H	H

Livello di rischio calcolato

H: alto M: medio L: basso

Sottrazione di proprietà industriale:
Azioni per mitigare il livello di rischio

Per poter mitigare i livelli di rischio individuati occorre ridurre la probabilità di occorrenza delle cause individuate. In particolare è necessario:

- definire la supervisione dei collaboratori interni
- tutti i locali e i sistemi devono essere dotati di un sistema di controllo di accesso
- l'accesso alla rete aziendale va vietato ai collaboratori interni, o può essere permesso mediante specifico sistema di livelli di autorizzazione. Per quanto concerne i dipendenti invece, l'accesso alle informazioni va regolato in modo tale che ogni dipendente sia autorizzato esclusivamente all'accesso a dati inerenti la sua mansione lavorativa
- controllo in ingresso ed in uscita, mediante addetti alla sicurezza, di eventuali dispositivi non autorizzati in possesso del dipendente (Es. Hard disk esterno, pen drive)
- monitoraggio continuo dell'avvenuta copia di informazioni su dispositivi rimovibili.
- utilizzo di sistema proxy aziendale per negare l'accesso a siti web che consentono la memorizzazione, anche temporanea, di file
- definire accuratamente lo smaltimento di dispositivi o informazioni non più utili (es. effettuare formattazione a più passate dei supporti rimovibili non più utili)
- definire correttamente ruoli e responsabilità per ogni dipendente/collaboratore, così da consentire l'accesso a quest'ultimo solo alle informazioni realmente necessarie per la sua mansione lavorativa
- istruire i dipendenti al mantenimento in ordine e in sicurezza della scrivania e della postazione pc (Es. Utilizzo della metodologia 6S, logout quando ci si allontana dalla postazione di lavoro, tenere il desktop in ordine)

Sottrazione di proprietà industriale:
Azioni per mitigare il livello di rischio

Livello di rischio mitigato

H: alto

M: medio

L: basso

Causa	Probabilitá di occorrenza	Conseguenze	Livello di rischio
1	L	1÷3:H	L
2	L	1÷3:H	L
3	L	1÷3:H	L
4	M	1÷3:H	M
5	L	1÷3:H	L
6	L	1÷3:H	L
7	L	1÷3:H	L
8	L	1÷3:H	L
9	L	1÷3:H	L
10	L	1÷3:H	L
11	M	1÷3:H	M

Sottrazione di proprietà industriale:
Trattamento del reperto

In questo caso possiamo distinguere quattro reperti informatici, presupponendo di aver già implementato le misure di mitigazione descritte:

1. copia forense del dispositivo (Es disco del dipendente o dispositivo smaltito)
2. file di log contenenti attività sul server (Es. accesso a cartelle condivise, copia dei file)
3. file di log degli accessi ottenuto dal sistema di lettore badge
4. filmato di videosorveglianza della stanza in cui risiede il sistema.

Nel primo caso, la costruzione di una timeline delle operazioni effettuate sul dispositivo, con particolare focus sul periodo di tempo indicato in fase di segnalazione, unito all'analisi del filmato di videosorveglianza può portare all'individuazione del soggetto che ha compiuto tali azioni e dei dati che sono stati visionati/prelevati dal sistema.

Nel secondo caso, l'analisi dei file di log risulta molto utile per capire chi ha visionato specifici insiemi di dati e se ne ha effettuato una copia, così da risalire all'utente ed operare in seguito sul suo personal computer alla ricerca di eventuali tracce.

Nel terzo caso, tale reperto è utile, insieme al quarto, per capire chi ha avuto accesso a quale stanza (Es. ufficio, stanza smaltimento) e in quale esatto momento.

Il quarto reperto servirà anche a dare un volto alla persona (poichè il badge potrebbe essere stato sottratto al proprietario, quindi da solo non fornisce prova certa)

Furto di sistemi informatici:
Analisi del rischio

In questo caso vengono considerati i dispositivi forniti dall'azienda al proprio dipendente al fine di permetterne l'esecuzione dell'attività lavorativa, come ad esempio notebook aziendale ed eventualmente anche il cellulare.
Tale reato rientra all'interno della definizione di furto, che è sanzionato ai sensi dell'Art.624 c.p., secondo cui *"Chiunque s'impossessa della cosa mobile altrui, sottraendola a chi la detiene, al fine di trarne profitto per sè o per altri, è punito con la reclusione[..].*

Cause

1. incuria del dipendente;
2. furto domestico o durante viaggio/trasferta del dipendente;
3. mancanza o insufficienza di adeguate procedure per il mantenimento in condizione sicura dei dispositivi assegnati.

Furto di sistemi informatici:
Analisi del rischio

Conseguenze

Le principali conseguenze del furto di dispositivi aziendali si possono riassumere in:

1. esposizione di segreti aziendali/industriali: si pensi a documentazione contenuta all'interno del dispositivo e classificata come Business only o Confidential
2. impossibilità o difficoltà nell'esecuzione delle attività lavorative da parte del dipendente
3. possibile danno economico per l'azienda, che deve fornire al dipendente un dispositivo in sostituzione di quello sottratto.

Livello di rischio calcolato

H: alto

M: medio

L: basso

Causa	Probabilitá di occorrenza	Conseguenze	Livello di rischio
1	H	1:H 2÷3:M	H
2	H	1:H 2÷3:M	H
3	M	1:H 2÷3:M	M

Furto di sistemi informatici:
Azioni per mitigare il livello di rischio

Per poter mitigare i livelli di rischio individuati occorre sostanzialmente incrementare il livello di attenzione del dipendente nei confronti dei dispositivi ad esso affidati, mediante l'utilizzo di adeguate procedure e misure di sicurezza. In particolare è necessario:

- protezione fisica dei dispositivi (es. messa in sicurezza all'interno di cassaforte del dispositivo quando ci si allontana dalla stanza d'albergo, utilizzo del cavo antifurto di tipo Kensington)
- utilizzo di sistema di controllo di accesso, che nel caso di controllo di accesso alla rete aziendale deve essere notevolmente complesso, come ad esempio autenticazione alla VPN con utilizzo di certificato al posto della (meno sicura) password
- utilizzo di tecniche di cifratura (come ad esempio BitLocker)
- utilizzo di sistema di backup centralizzato, così da permettere la disponibilità dei documenti utili al lavoro del dipendente anche in seguito al furto
- predisposizione di meccanismo di blocco/disabilitazione del dispositivo con relativa eliminazione dei dati contenuti all'interno utilizzabile da remoto.

Livello di rischio mitigato

H: alto

M: medio

L: basso

Causa	Probabilitá di occorrenza	Conseguenze	Livello di rischio
1	L	1:H 2÷3:M	L
2	L	1:H 2÷3:M	L
3	M	1:H 2÷3:M	M

Furto di sistemi informatici:
Trattamento del reperto

In questo caso possiamo distinguere tre reperti informatici:

1. analisi di eventuali file di log contenenti attività degli utenti sul server, nel caso in cui ci si renda conto che siano riusciti ad accedere alla rete aziendale utilizzando i dispositivi oggetto di furto
2. tracciato degli spostamenti del cellulare ed elenco delle chiamate effettuate/ricevute successivamente al furto (mediante collaborazione con il provider telefonico). Nel caso in cui anche il notebook fosse dotato di connessione GSM le considerazioni fatte valgono anche per il notebook
3. copia forense del dispositivo recuperato (sia esso il personal computer o il cellulare) ed ulteriori investigazioni secondo necessità.

Nel primo caso, l'analisi dei file di log risulta molto utile per capire chi si è introdotto (tracciare la connessione) e a quali file ha avuto accesso.

Nel secondo caso, l'analisi di tali tracciati può essere utile a rintracciare chi ha perpetrato il furto e recuperare il dispositivo.

Nel terzo caso, la costruzione di una timeline delle operazioni effettuate con il personal computer o il cellulare può essere utile per capire se sono stati letti/copiati file critici per il business aziendale, o ricostruire le operazioni effettuate da chi deteneva i dispositivi.

Scoperta e notifica degli eventi

All'interno di un sistema di gestione degli incidenti di sicurezza, si entra nella fase di scoperta e notifica di un evento di sicurezza informatica nel momento in cui viene riscontrata e comunicata l'occorrenza di un evento di sicurezza o la scoperta di una vulnerabilità all'interno dei sistemi in uso.

Tale scoperta può avvenire mediante il supporto di sistemi di monitoraggio o da personale direttamente o indirettamente coinvolto nell'utilizzo dei sistemi, come ad esempio:

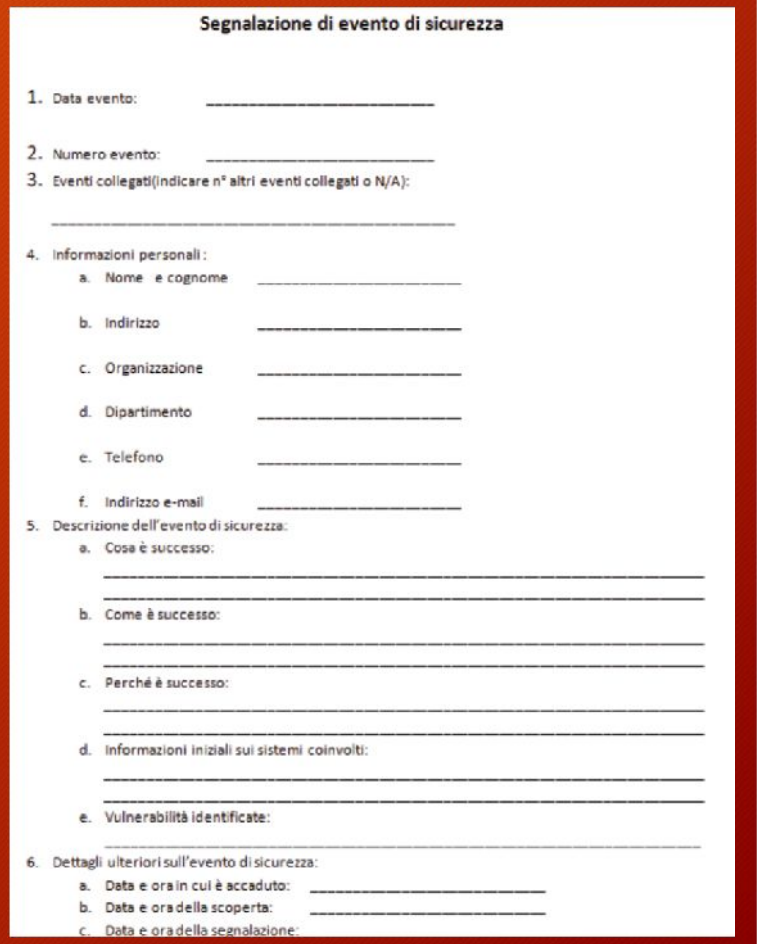
- notifiche provenienti da sistemi di monitoraggio (Es. antivirus, sistema di monitoraggio della rete, analisi di file di log di sistemi o server)
- notifiche da parte degli utilizzatori dei sistemi
- informative provenienti da enti esterni, come ISP5, fornitori o servizi che forniscono consulenza di sicurezza informatica
- responsabili della sicurezza
- dipartimento IT interno all'azienda
- clienti
- siti web di pubblica informazione (es. blog sulla sicurezza)
- mezzi di informazione di massa (tv, giornali).

Modulo di segnalazione evento

La persona (aiutata o meno dagli strumenti automatici) che nota un evento di sicurezza informatica è tenuto a segnalarlo tempestivamente al PoC (Point of Contact) oppure al ISIRT che procederà con la valutazione dell'evento.

Il modulo utilizzato per segnalare l'evento dovrebbe contenere come minimo le seguenti informazioni, indispensabili per poter effettuare l'analisi:

- data e ora della scoperta
- osservazioni
- informazioni di contatto



Segnalazione di evento di sicurezza

1. Data evento: _____
2. Numero evento: _____
3. Eventi collegati(indicare n° altri eventi collegati o N/A):

   _____
4. Informazioni personali:
   a. Nome e cognome _____
   b. Indirizzo _____
   c. Organizzazione _____
   d. Dipartimento _____
   e. Telefono _____
   f. Indirizzo e-mail _____
5. Descrizione dell'evento di sicurezza:
   a. Cosa è successo:
      _____
      _____
   b. Come è successo:
      _____
      _____
   c. Perché è successo:
      _____
      _____
   d. Informazioni iniziali sui sistemi coinvolti:
      _____
      _____
   e. Vulnerabilità identificate:
      _____
6. Dettagli ulteriori sull'evento di sicurezza:
   a. Data e ora in cui è accaduto: _____
   b. Data e ora della scoperta: _____
   c. Data e ora della segnalazione:

Valutazione degli eventi

Non appena il PoC riceve il modulo di segnalazione di evento di sicurezza, deve effettuare la sua valutazione per decidere se l'evento segnalato sia da considerare come un possibile (o già concluso) evento di sicurezza o un falso allarme.

Se viene identificato come un falso allarme, deve comunque completare il modulo ed inviarne una copia al l'ISIRT e alla persona che ha effettuato la segnalazione.

Se, invece, valuta che l'evento è un incidente di sicurezza e possiede delle competenze adeguate, lui stesso potrebbe svolgere ulteriori azioni di analisi e approfondimento per individuare, ad esempio, ulteriori misure di controllo immediate.

In ogni caso, l'incidente va segnalato all'ISIRT così che si possa procedere ad ulteriori valutazioni e decisioni da parte del team preposto allo svolgimento di tali attività.

Durante la valutazione il PoC deve reperire il maggior numero di informazioni possibile. In particolare, dovrebbe essere in grado di fornire le seguenti informazioni:

- informazioni generali sull'incidente: che tipo di incidente è, da chi o da che cosa è stato causato, su cosa potrebbe influire e cosa è stato fatto fin'ora per gestire tale incidente;
- conseguenze dell'incidente: bisogna valutare quale dei pilastri della sicurezza informatica è stato violato, quindi identificare se come conseguenza si sia ottenuto il rilascio o la modifica di informazioni senza autorizzazione, il ripudio di informazioni, la non disponibilità di informazioni o servizi o la distruzione di informazioni o servizi.

Valutazione degli eventi

Se l'incidente di sicurezza informatica venisse risolto in questa fase, il PoC dovrebbe completare il modulo inserendo tutte le azioni effettuate ed eventuali "lesson learned" ed inviare il modulo all'ISIRT per la revisione e l'archiviazione.

Sebbene, in generale, la maggior parte delle situazioni normalmente implichi il passaggio di testimone all'ISIRT per la valutazione finale, vi possono essere dei casi in cui il PoC ritenga l'incidente particolarmente grave, per cui debba contattare direttamente la persona a capo dell'ISIRT e scalare la segnalazione all'unità di crisi, che si occuperà del caso.

L'ISIRT ha la responsabilità di prendere la decisione finale in merito all'occorrenza o meno di un possibile incidente di sicurezza. Una volta ricevuto da parte del PoC il modulo, compilato in modo più o meno dettagliato, la persona contattata deve rivederne il contenuto e raccogliere più informazioni utili a valutare l'incidente, che può essere ridotto a falso allarme o essere confermato.

Risoluzione degli eventi

Una volta effettuata l'analisi dell'evento, la gestione dell'incidente, inclusa la risposta immediata ed eventuali azioni aggiuntive, va prioritizzata a seconda della criticità e degli impatti sull'azienda.

L'unità di crisi, che prende in carico la gestione dell'evento, deve conoscere e applicare le modalità operative codificate e idonee a mitigare i danni e rimuovere il problema, in caso contrario, in collaborazione con il responsabile dell'ISIRT dovrà individuare le soluzioni più opportune.

Quest'ultima opzione presuppone che:

- Non è stata eseguita una corretta valutazione dei rischi
- Non sono state previste adeguate misure di contenimento/risoluzione
- Non è stata sviluppata un'idonea fase di formazione/informazione

Digital Forensics

la gestione del reperto informatico

Identificazione

Raccolta

Acquisizione

Conservazione

Analisi e Interpretazione

Digital Forensics

Questa attività è trasversale alle precedenti (“Scoperta e notifica”, “Valutazione”) e consiste nella raccolta ed analisi dei reperti che possono essere utilizzati al fine di documentare il fenomeno verificatosi e poter perseguire i responsabili.

Affinchè le prove estrapolate dai reperti possano essere utilizzabili in sede processuale è bene adottare una serie di linee guida.

Queste hanno il compito di:

- Definire i requisiti del reperto digitale
- Stabilire le fasi da seguire e l’obiettivo che si vuole raggiungere
- Individuare le figure professionali che gestiranno le evidenze digitali

Requisiti del reperto digitale

- Prova digitale
  - Informazione o dato, memorizzato o trasmesso in formato binario, che può essere utilizzato come prova
- Copia di prova digitale
  - Copia di prova digitale che può essere prodotta per mantenere l'affidabilità della prova, includendo sia la prova digitale che la procedura di verifica
- Dato volatile
  - Dato facilmente soggetto a modifica. Una variazione può essere dovuta ad assenza di corrente o ad interventi di campi magnetici, a cambi di stato del sistema
- Alterazione
  - Modifica del valore di potenziali evidenze digitali e riduzione del valore probatorio
- Distruzione di prova
  - Modifica volontaria del valore di potenziali evidenze digitali

Requisiti del metodo forense

- Pertinenza
  - Serve per incolpare (o discolpare)
  - Dimostrare che il materiale è rilevante, cioè che contiene dati utili e che pertanto esiste una buona ragione per acquisirli
- Affidabilità
  - Assicurarsi che la prova digitale sia genuina
  - Tutti i processi eseguiti devono essere ben documentati e, se possibile, ripetibili. Il risultato dovrebbe essere riproducibile
- Sufficienza
  - Il DEFR deve valutare quale materiale deve essere raccolto e le procedure idonee
  - Il materiale può essere copiato o acquisito (sequestrato)
  - Non è detto che sia sempre necessario acquisire una copia completa
  - Valutare in base al caso (interessa la figura del DEFR)
  - Può dipende dalla legislazione nazionale

Requisiti del metodo forense

- Verificabilità
  - Un terzo deve essere in grado di valutare le attività svolte dal DEFR e dal DES
    - Attuabile se esiste la documentazione delle azioni svolte
    - Valutare il metodo scientifico, le tecniche e le procedure seguite
  - DEFR e DES devono essere in grado di giustificare le azioni svolte
- Ripetibilità
  - Le operazioni devono sempre essere ripetibili utilizzando le stesse procedure, lo stesso metodo, gli stessi strumenti, sotto le stesse condizioni
- Riproducibilità
  - Le operazioni possono essere ripetibili anche usando lo stesso metodo, gli strumenti diversi, sotto condizioni diverse
- Giustificabilità
  - Dimostrare che le scelte adoperate erano le migliori possibili

Fasi

La ISO/IEC 27037 indica le fasi che consento la raccolta delle evidenze:

- **Identificazione**
- **Raccolta**
- **Acquisizione**
- **Conservazione**

Mentre la ISO/IEC 27042 si concentra sull'analisi delle evidenze:

- **Analisi**
- **Interpretazione**

L'obiettivo finale consiste nella **Presentazione** dei risultati raggiunti.

Identificazione

- La prova informatica si presenta in forma fisica e logica
  - Device
  - Rappresentazione dei dati
- Ricerca dei device che possono contenere dati rilevanti
  - Priorità ai dati volatili
  - Considerare dispositivi di difficile identificazione
    - Geografica: Es.: Cloud computing, SAN
    - Dimensioni Es.: miniSD
- Si considera computer un dispositivo digitale standalone che riceve, processa e memorizza dati e produce risultati
    - Non connesso in rete
    - Ci possono essere periferiche connesse
- Se il computer ha un'interfaccia di rete, anche se non è connesso in rete al momento dell'intervento, bisogna individuare gli eventuali sistemi con cui può aver comunicato

Identificazione

La scena del crimine può contenere diversi tipi di dispositivi di memorizzazione

- Hard disk, hard disk esterni, floppy disk
- Memorie flash, memory card, CD, DVD, Blu-ray

In fase di identificazione il DEFR deve:

- Documentare marca, tipo e numero di serie di ogni supporto individuato. Inoltre, se i supporti risultano danneggiati esternamente, deve documentare lo stato con l'ausilio di foto
- Identificare tutti i computer e il loro stato (acceso/spento), che deve rimanere inalterato:
  - stato acceso: documentare cosa è visibile sullo schermo (effettuando foto) e inserirlo a verbale
  - stato spento: non effettuare alcuna operazione sul dispositivo.
- Reperire i caricabatterie dei dispositivi alimentati a batteria, per evitare che possano scaricarsi
- Utilizzare un rilevatore di segnali wireless per verificare la presenza di dispositivi nascosti
- In determinate situazioni può essere molto utile prendere in considerazione anche evidenze non digitali, come ad esempio informazioni sui dispositivi fornite da personale impiegato in azienda (ad esempio: scopo di utilizzo del dispositivo, password per l'accesso, ecc. . .)

Raccolta (sequestro) o acquisizione?

Una volta terminata la fase di identificazione il DEFR, con gli strumenti in suo possesso, deve decidere se procedere con la raccolta o l'acquisizione.

Per prendere tale decisione vanno presi in considerazione alcuni fattori:

- volatilità della possibile evidenza
- esistenza di cifratura completa o parziale dei supporti (nel qual caso può essere utile effettuare l'acquisizione dei dati volatili in RAM)
- criticità del sistema (es. server che non può essere spento poiché critico per il business aziendale)
- requisiti legali
- carenza delle risorse necessarie (ad es. quantitativo di spazio necessario o disponibilità del personale).

Raccolta

Nel caso in cui si opti per il sequestro dei dispositivi, la modalità di esecuzione della stessa dipende dallo stato in cui si trova il sistema.

- **Sistema trovato spento**

  Nel caso in cui il sistema venga trovato spento, vanno prese in considerazione le seguenti attività:

  - assicurarsi che il dispositivo sia effettivamente spento e non in standby
  - rimuovere il cavo di alimentazione, staccando prima l'estremità connessa al dispositivo e poi quella a muro
  - disconnettere e assicurare tutti i cavi connessi al dispositivo ed etichettare le relative porte a cui sono connessi, così da ricostruire le connessioni in seguito
  - proteggere il tasto di accensione, onde evitare accensione casuale del dispositivo
  - mettere in sicurezza eventuali alloggiamenti per floppy disk, cd/dvd con del nastro per evitare apertura/espulsione del contenuto.

Raccolta

- **Sistema trovato acceso**

  Nel caso in cui il sistema venga trovato accesso, vanno prese in considerazione le seguenti attività:

  - acquisire i dati volatili del dispositivo prima di spegnerlo, così da poter avere a disposizione eventuali chiavi di crifratura residenti in memoria. Nel caso in cui si sospetti la presenza di meccanismi di cifratura conviene procedere in seguito con acquisizione logica
  - nel caso in cui si voglia lasciare il dispositivo acceso (ad esempio per presenza confermata di meccanismi di cifratura), bisogna prestare particolare cura durante il trasporto (raffreddamento, protezione da shock)
  - nel caso in cui si decida di spegnere il dispositivo, valutare se sia il caso di effettuarlo mediante regolare procedura di spegnimento o staccando il cavo di alimentazione (rimuovendo prima l'estremità attaccata al dispositivo e poi quella attaccata alla presa). Normalmente tale decisione dipende dalla configurazione del sistema
  - etichettare e staccare tutti i cavi dal sistema. Etichettare tutte le porte cosi che lo stato del sistema possa essere ricostruito in laboratorio
  - proteggere il tasto di accensione, onde evitare una accensione casuale del dispositivo
  - infine, nel caso tale dispositivo sia un notebook, acquisire i dati volatili prima di rimuovere batteria e successivamente il cavo di alimentazione. Mettere in sicurezza anche eventuali alloggiamenti per floppy disk, cd/dvd utilizzando del nastro.

Acquisizione

Nel caso in cui si opti per l'acquisizione dei dispositivi, sia on-site che in laboratorio, la modalità di esecuzione della stessa dipende, allo stesso modo della raccolta dallo stato in cui si trova il sistema.

- **Sistema trovato acceso**

  Nel caso in cui il sistema venga trovato accesso, vanno prese in considerazione le seguenti attività:

  - acquisire tutti i dati volatili che verrebbero persi se il dispositivo venisse spento (es. RAM, processi in esecuzione, connessioni di rete, impostazioni di data ed ora). Per effettuare l'acquisizione è consigliabile riversare i dati copiati in un contenitore logico, calcolarne l'hash e documentarne il valore. Ove ciò non sia fattibile è possibile utilizzare un contenitore di tipo ZIP, calcolarne l'hash e documentarlo
  - iniziare il processo di copia forense dei dati non volatili utilizzando strumenti validati. La copia forense ottenuta va memorizzata in un dispositivo preparato per tale scopo (es. Formattato). Se la copia viene invece memorizzata in un contenitore logico bisogna assicurarsi che questa non possa essere corrotta o danneggiata. Al termine del processo di copia calcolare e annotare il valore di hash
  - utilizzare una sorgente affidabile per documentare data e ora e documentare accuratamente inizio e fine di oggi attività

Acquisizione

- **Sistema trovato spento**

  Nel caso in cui il sistema venga trovato spento, vanno prese in considerazione le seguenti attività:
  • assicurarsi che il sistema sia davvero spento
  • rimuovere il supporto di memoria dal dispositivo spento (se non già fatto), ed etichettarlo accuratamente (es. Produttore, modello, numero di serie)
  • eseguire la copia forense del supporto di memoria utilizzando un tool validato. Calcolarne il valore di hash al termine.

- **Sistemi critici**

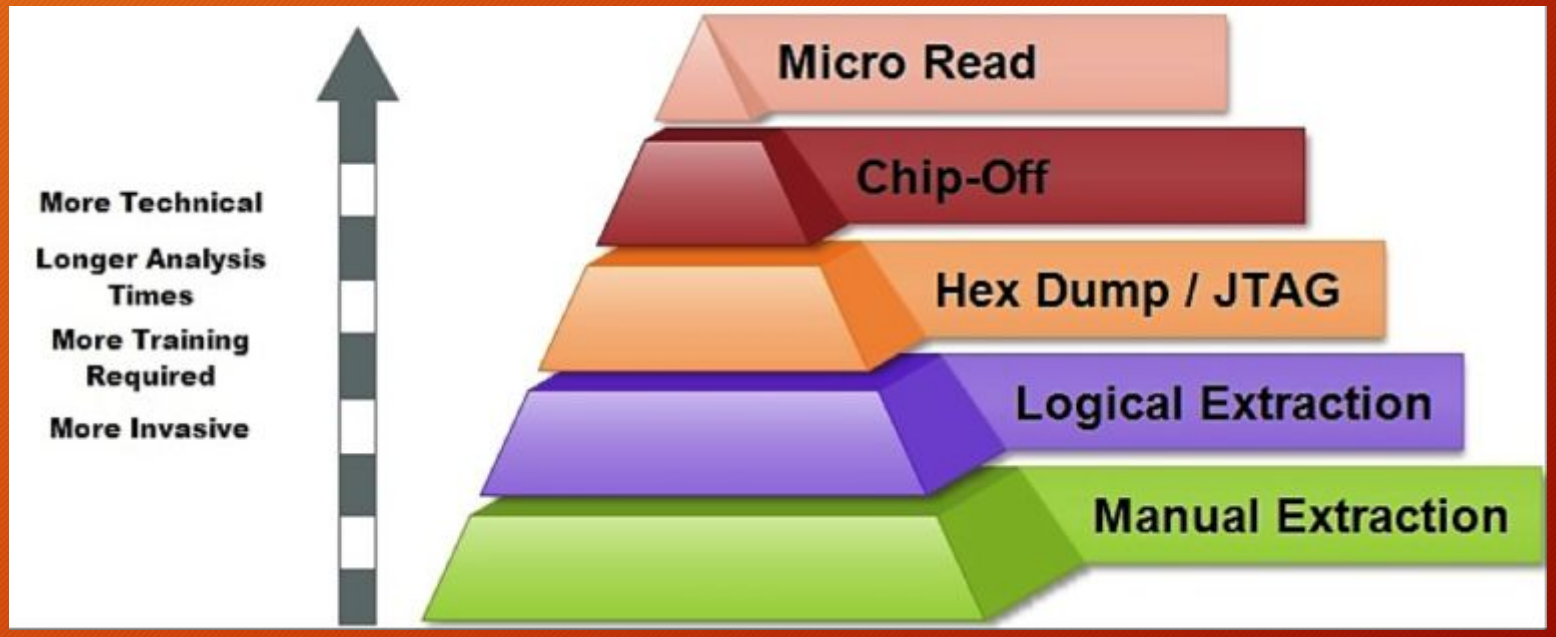
  Un caso particolare nella fase di acquisizione si ha quando ci si trova davanti ad un sistema critico, per cui per svariate ragioni non è possibile procedere all'acquisizione completa dei dati contenuti all'interno del sistema. Alcuni esempi di tali sistemi sono data center, sistemi di sorveglianza o sistemi medici. In tali situazioni vi sono due sole possibili alternative di acquisizione:

  • acquisizione live (acquisizione totale della memoria RAM e di massa)

  • acquisizione parziale (solo determinate porzioni di memoria di interesse investigativo):
    - il sistema di cui si vogliono acquisire i dati ha una capacità di memoria notevolmente grande, contenendo quindi una mole notevole di dati (si pensi ai database server)
    - il sistema, a causa della sua criticità, non può essere spento
    - solo alcuni dati sono rilevanti all'interno del sistema
    - vi sono dei vincoli legali che consentono solo l'acquisizione di alcuni dati.

Acquisizione: classificazione

Per acquisizione forense del supporto di memorizzazione si intende l'estrazione del contenuto memorizzato sotto forma di sequenza di bit memorizzati al suo interno.



La copia forense ideale è una copia bit a bit del supporto originale perché include:

- Tutti i file, quelli cancellati, lo slack space, lo spazio libero

Acquisizione: write blocker

Per dare garanzia del rispetto dei principi enunciati, tutte le operazioni eseguite in fase di acquisizione devono essere accuratamente documentate, meglio se si utilizzando dei dispositivi che registrano automaticamente quanto viene eseguito.

Se possibile è conveniente utilizzare anche dei dispositivi che impediscono l'alterazione del supporto di origine: c.d. write-blocker

Acquisizione: impronta hash

Al termine della fase di acquisizione bisogna “sigillare” i dati acquisiti attraverso un sigillo digitale (solitamente un impronta hash con l’eventuale aggiunta dell’utilizzo di una firma digitale per associare l’operazione al DEFR) per dimostrare che la copia ottenuta sia identica all’originale.

L'algoritmo di hash elabora una qualunque mole di bit e restituisce in output una stringa di bit di dimensione fissa. L'output è detto digest.

- La stringa di output è univoca per ogni documento e ne è un identificatore
- L'algoritmo non è invertibile, ossia non è possibile ricostruire il documento originale a partire dalla stringa che viene restituita in output (anche se in realtà per ogni digest esistono infiniti input che lo generano – cd. collisioni)

DPCM 8 febbraio 1999: “l'impronta di una sequenza di simboli binari è una sequenza di simboli binari di lunghezza predefinita generata mediante l'applicazione alla prima di un'opportuna funzione di hash“

Conservazione

Inoltre, occorre garantire che sia preservata, con i dovuti accorgimenti, la confidenzialità, l'integrità e la disponibilità della potenziale prova.

L'evidenza, infatti, va preservata sia durante il trasporto che lo stoccaggio, che potrebbe superare il suo tempo di vita a seconda dei tempi di giustizia.

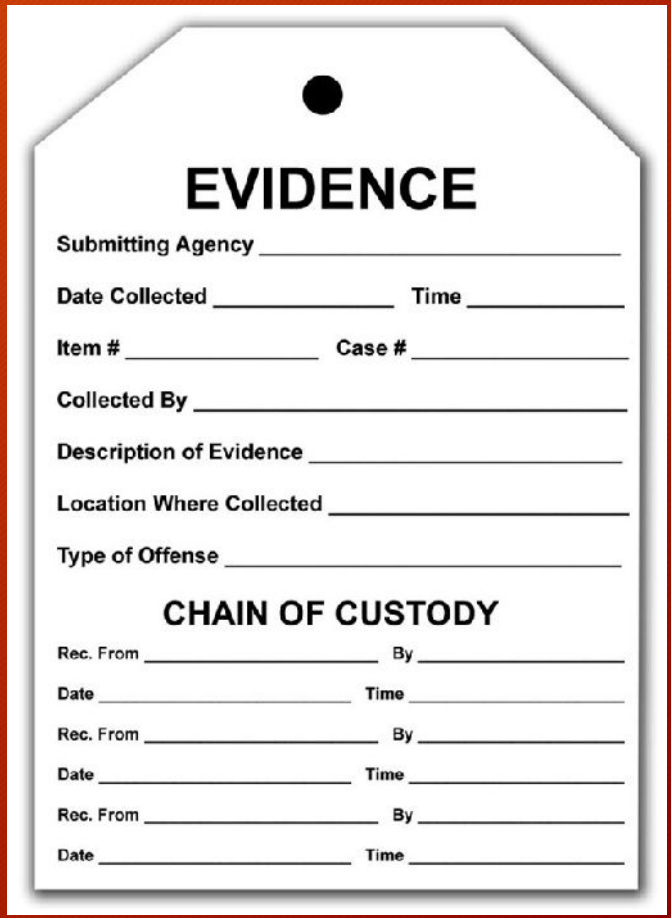
Per far ciò occorre:

- Etichettare tutto
- Verificare che le batterie siano opportunamente caricate (e ricaricare)
- Bloccare parti mobili
- Ridurre rischi in base alla natura del supporto
- Ridurre rischi dovuti al trasporto
- Preservare eventuali altri tracce
  - Es.: tracce biologiche
  - Utilizzare guanti puliti

Conservazione: catena di custodia

Catena di custodia

- Documentare movimenti e interazioni con la potenziale prova digitale
- Storia del supporto a partire dalla fase di raccolta
- Formato cartaceo o digitale
- Deve contenere
  - Identificativo unico dell'evidenza
  - Quando, dove, chi e perché ha avuto accesso all'evidenza
  - Documentare e giustificare ogni alterazione inevitabile, con il nome del responsabile



Analisi

L’analisi deve consentire la ricostruzione degli eventi passati attraverso la lettura dei dati rinvenuti.

Poiché ogni copia coincide con l’originale, l’analisi va eseguita su una copia dei dati acquisiti e non sull’originale

Caratteristiche dell’analisi

- Riproducibilità: Ogni singola operazione deve produrre sempre lo stesso risultato (si intende risultato oggettivo, cioè i dati e non la loro valutazione)
- Metodologie: si può applicare la Regola delle 5W
  - WHO? («Chi?»)
  - WHAT? («Che cosa?»)
  - WHEN? («Quando?»)
  - WHERE? («Dove?»)
  - WHY? («Perché?»)

Analisi: metodologia

- Che cosa è successo e come si è svolto?
  - Individuare i dati utili a ricostruire I fatti
  - Comunicazioni
  - Documenti
  - Log
  - Metadati (date, luoghi, coordinate…)
- Chi è coinvolto?
  - Comunicazioni
  - Metadati (date, utenti)
- Quando è accaduto?
  - Comunicazioni
  - Metadati (date, utenti)
- Da dove a dove?
  - Comunicazioni
  - Documenti
  - Log
  - Metadati (date, luoghi, coordinate…)
  - Tabulati telefonici
- Quante volte si è verificato?
  - Comunicazioni
  - Documenti
  - Log
  - Metadati (date…)
- C'era consapevolezza?
  - Comunicazioni
  - Cancellazione dati
  - Documenti
  - Log
  - Metadati (date…)
  - Navigazione web
  - Competenze utente

Analisi: strategie operative

- Ricerche
  - Autore
  - Intervallo di date
  - Tipo di file
  - Parola chiave
  - Per hash
  - Per thread (email)
- Recupero dati
  - Recupero dati cancellati, carving…
- Interpretazione dati
- Conversione tra formati
- Crack password
  - File tipicamente protetti
  - Tipologie di attacco
- Artefatti del sistema operativo

Analisi: carving

Il data carving è un processo di estrazione di un set di dati da un insieme di dati molto più ampio.

La tecnica del data carving è utilizzata solitamente durante le indagini di analisi forense per analizzare lo spazio non allocato.

Durante questo procedimento è ignorata la struttura del file system.

I file sono individuati e catalogati in base all'header e al footer trovato.

Distinguiamo

- Data carving base
  - L'header e footer dei file non sono sovrascritti
  - Il file non è frammentato
  - Il file non è compresso
  - Il file estratto è l'insieme di bit contenuti tra header e footer
- Data carving avanzato
  - I frammenti non sono sequenziali
  - I frammenti non sono ordinati
  - Mancano dei frammenti

Data Carving di un immagine JPEG

Short Name	Bytes	Payload	Name
SOI	0x FF D8	none	Start of Image
SOF0	0x FF C0	variable size	Start of Frame (Baseline DCT)
SOF2	0x FF C2	variable size	Start of Frame (Progressive DCT)
DHT	0x FF C4	variable size	Define Huffman Table(s)
DQT	0x FF DB	variable size	Define Quantization Table(s)
DRI	0x FF DD	2 bytes	Define Restart Interval
SOS	0x FF DA	variable size	Start of Stream
RST*n*	0x FF D0…0x FF D7	none	Restart
App*n*	0x FF E*n*	variable size	Application-Specific
COM	0x FF FE	variable size	Comment (text)
EOI	0x FF D9	none	End of Image

Figure 1. File structure of a JPEG file.

Figure 2. JPEG header.

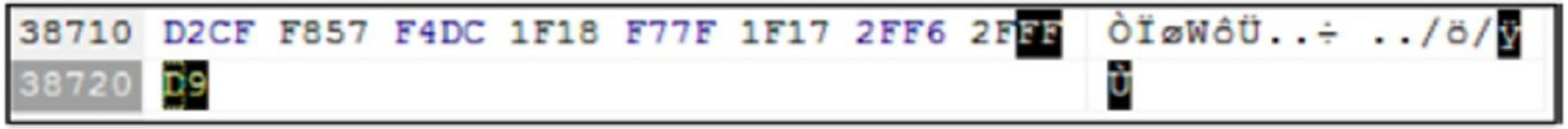


Figure 3. JPEG footer.

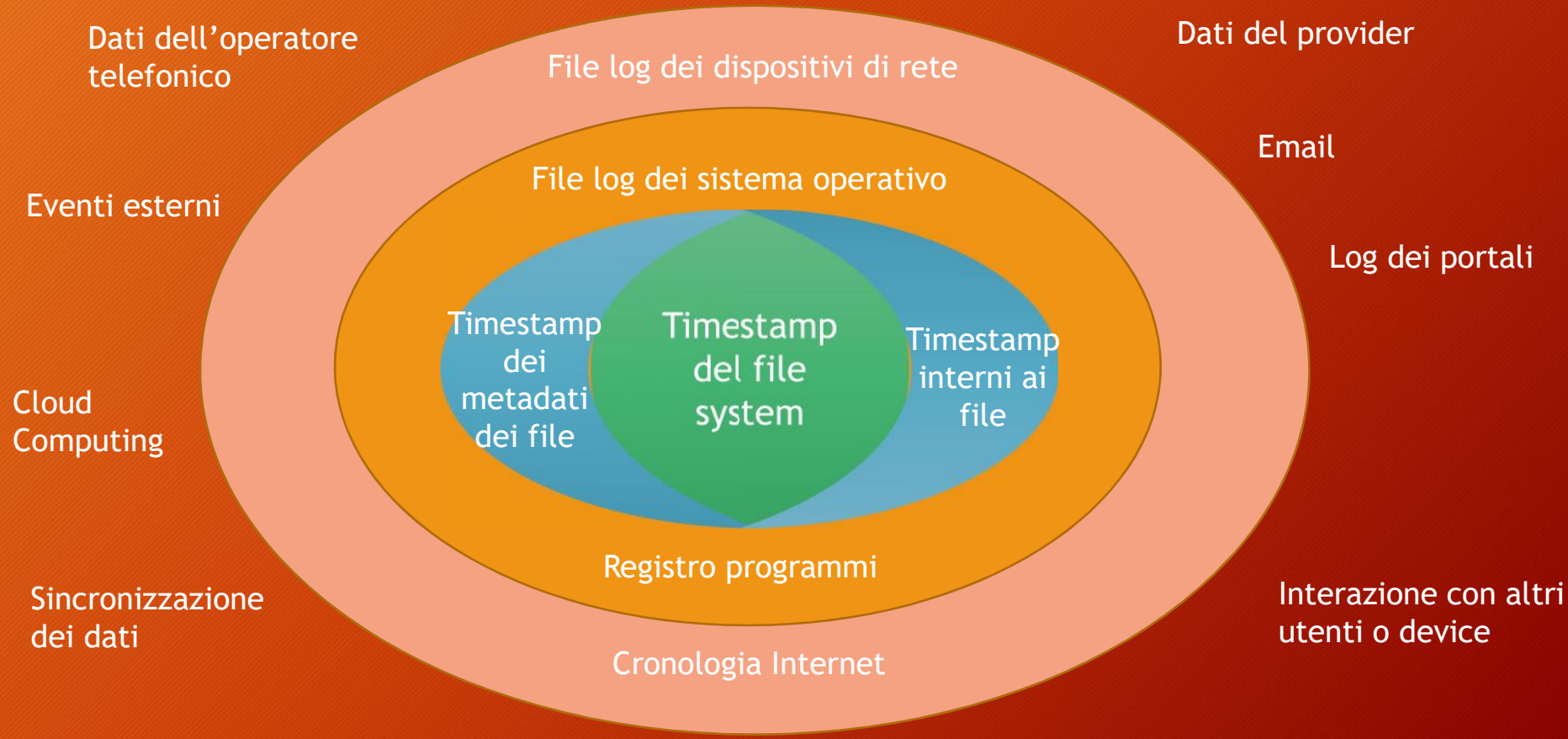
Analisi: timeline

Spesso è necessario ricostruire la cronologia delle attività che hanno determinato lo stato del dispositivo con l'obiettivo di individuare gli elementi di prova che concorreranno a dimostrare o confutare dei fatti.

Occorre creare una linea temporale relativa agli eventi verificatesi e richiede l'integrazione delle varie informazioni temporali (timestamp) create dal sistema operativo, dal file system e dalle applicazioni utente.

- Metadata dei file (timestamp della creazione, ultimo accesso ed ultima modifica dei file)
- Esecuzione dei programmi (S.O. registra informazioni sull'esecuzione dei programmi)
  - File prefetch su Windows
  - Registro di Windows
  - File log di sistema ….
- Artefatti generati dai programmi ad ogni esecuzione
  - Elenco file aperti o salvati
  - File di cronologia di navigazione
  - File di log ….

Analisi: supertimeline



Valutazione

La valutazione è una fase necessaria per stabilire:

- Se il reperto informatico è stato
  - alterato
  - inquinato
  - contraffatto
- Se le procedure di acquisizione sono state legittime
- Se il reperto è
  - attendibile
  - integro
  - Autentico
- Il significato dei dati presenti sul supporto

Presentazione

La presentazione è l'elemento con cui si valuta tutta l'attività svolta.

Essa deve comprendere in maniera dettagliata:

- Le fasi dell'analisi
- Le metodologie applicate
- Gli strumenti utilizzati
- I risultati ottenuti
  - Integrando con gli allegati
  - Foto dei reperti
- La risposta al quesito

Esercitazione

Creazione di una copia forense
Analisi della copia forense
Recupero dei file cancellati
Ricostruzione di una timeline
Esecuzione del data carving

Creazione di una copia forense

Su Kali Linux

1. Identificare il device
   - lsblk (vedere dischi e partizioni)
   - lsusb (vedere periferiche USB)
   - fdisk -l (vedere tutte le partizioni)
   - file -s /dev/sdx
   - df -h (spazio libero)
   - hdparm -I /dev/sdx (info device)
2. Clonare il device
   - dcfldd if=/dev/sdx hash=md5,sha256 md5log=md5.txt sha256log=sha256.txt of=driveimage.dd
   - file driveimage.dd

Su Windows (FTK Imager Lite)

1. Identificare il device
   - Selezionare File>Add Evidence Item
   - Navigare l'albero proposto
2. Clonare il device
   - Selezionare File>Create Disk Image
   - Scegliere Physical Drive
   - Selezionare il drive da clonare
   - Aggiungere la destinazione:
     1. Raw(dd) oppure E01
     2. Cartella di destinazione
     3. Nome file dell'immagine
     4. Livello di frammentazione
3. Dump Memoria
   1. Selezionare File>Capture Memory

Analisi della copia forense

Su Kali Linux

1. Autopsy Forensic Browser
   - http://localhost:9999/autopsy
   - New Case
   - Add Host
   - Add Image (driveimage.dd)
   - Analyze
   - File Deleted
   - File Activity TimeLines

Su Windows

1. Ftk Imager Lite
2. Identificare il device
   - Selezionare File>Add Evidence Item
   - Navigare l'albero proposto
3. Autopsy 4.6.0
   - New Case
   - Add Data Source (driveimage.dd)
   - Run Module
   - Navigare l'albero
   - Timeline

Esecuzione del data carving

Su Kali Linux

1. Foremost -i driveimage.dd
2. Si può scegliere i tipi di file con il parametro -t (es. -t doc,xls,pdf)
3. I risultati sono riversati in /Output

Su Windows

1. Aprire qphotorec_win.exe
2. Aggiungere un immagine raw
3. Selezionare il disco/partizione
4. Scegliere se leggere solo lo spazio libero oppure tutta la partizione
5. Scegliere la cartella dove registrare i file recuperati

Altre evidenze

Tools per trovare altri artefatti di interesse investigativo:

- DEFT - Digital Evidence & Forensics Toolkit (www.deftlinux.net)
  - Distribuzione Linux con tools per la Digital Forensics e l'Incident Response
- DART - Digital Advanced Response Toolkit (www.deftlinux.net)
  - Tools per Windows per la Digital Forensics e l'Incident Response
- NIRSOFT Package (www.nirsoft.net)
  - Password Recovery Utilities
  - Network Monitoring Tools
  - Web Browser Tools
  - Video/Audio Related Utilities
  - Internet Related Utilities
  - Desktop Utilities
  - Outlook/Office Utilities
  - Disk Utilities
  - System Utilities

Conclusioni

Considerazioni finali

Aspetti legali

Criticità

1. Continuo sviluppo tecnologico
2. Crittografia
3. Virtualizzazione
4. Giurisdizione
5. BYOD (Bring your own device)
6. Network Forensics
7. Web Forensics
8. Cloud Computing Forensics
9. Mobile Device Forensics
10. IoT Forensics

Conclusioni

Il reperto informatico è molto delicato e i dati in esso contenuti sono estremamente volatili.

Pertanto le attività esposte:

- Necessitano di rigore scientifico nel trattamento di dati informatici
- In determinati contesti portano inevitabilmente all'alterazione del dato
    - per esempio le date di accesso
        - Si perdono alibi
        - Si perde consapevolezza
        - Si perdono prove!

Infine, occorre ricordarsi che tutte le attività ed i risultati ottenuti andranno a far parte di un procedimento giudiziario, per cui è necessario conoscere le procedure legali ed i vincoli imposti dalla normativa vigente.

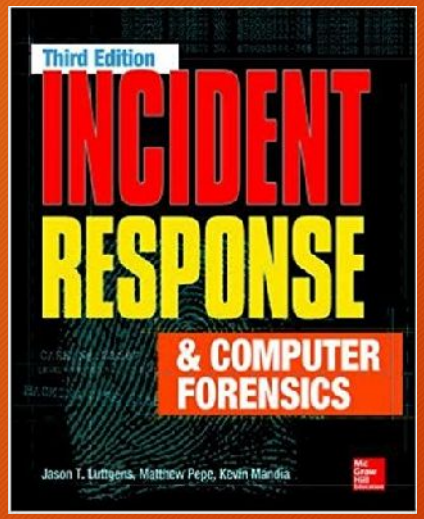
Aspetti legali

Spesso l'attività di digital forensics è svolta nell'ambito di un procedimento giudiziale e può essere finalizzato a:

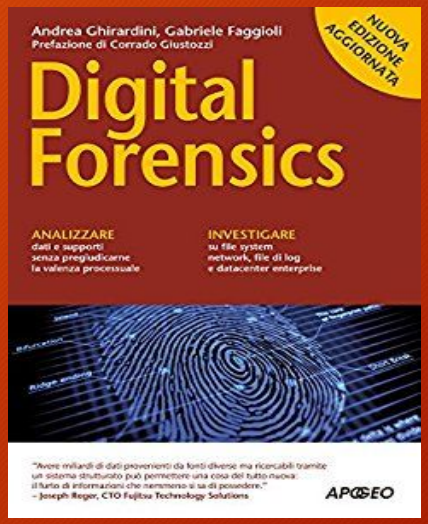
- Effettuare accertamenti tecnici durante le indagini preliminari
  - Ripetibili
  - Non ripetibili
- Rispondere ad un quesito tecnico nelle altre fasi del processo

L'incarico può essere assegnato da un qualsiasi attore del procedimento:

- Giudice -> Consulente Tecnico d'Ufficio (CTU)
- Pubblico Ministero -> Perito del Pubblico Ministero
- Parte Privata -> Consulente Tecnico di Parte (CTP)
- Polizia Giudiziaria -> Ausiliario della Polizia Giudiziaria



Riferimenti



Fine

vincenzocalabro.it