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

Corso di Tecnologie per la sicurezza informatica

Digital Forensics

Metodologie e Simulazioni di Indagine

Vincenzo Calabrò

Agenda

- Introduzione
  - Definizioni
  - Metodologie
- 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.

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 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.

Digital Forensics
la gestione del reperto informatico

Identificazione

Raccolta

Acquisizione

Conservazione

Analisi e Interpretazione

Digital Forensics

Questa attività 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**

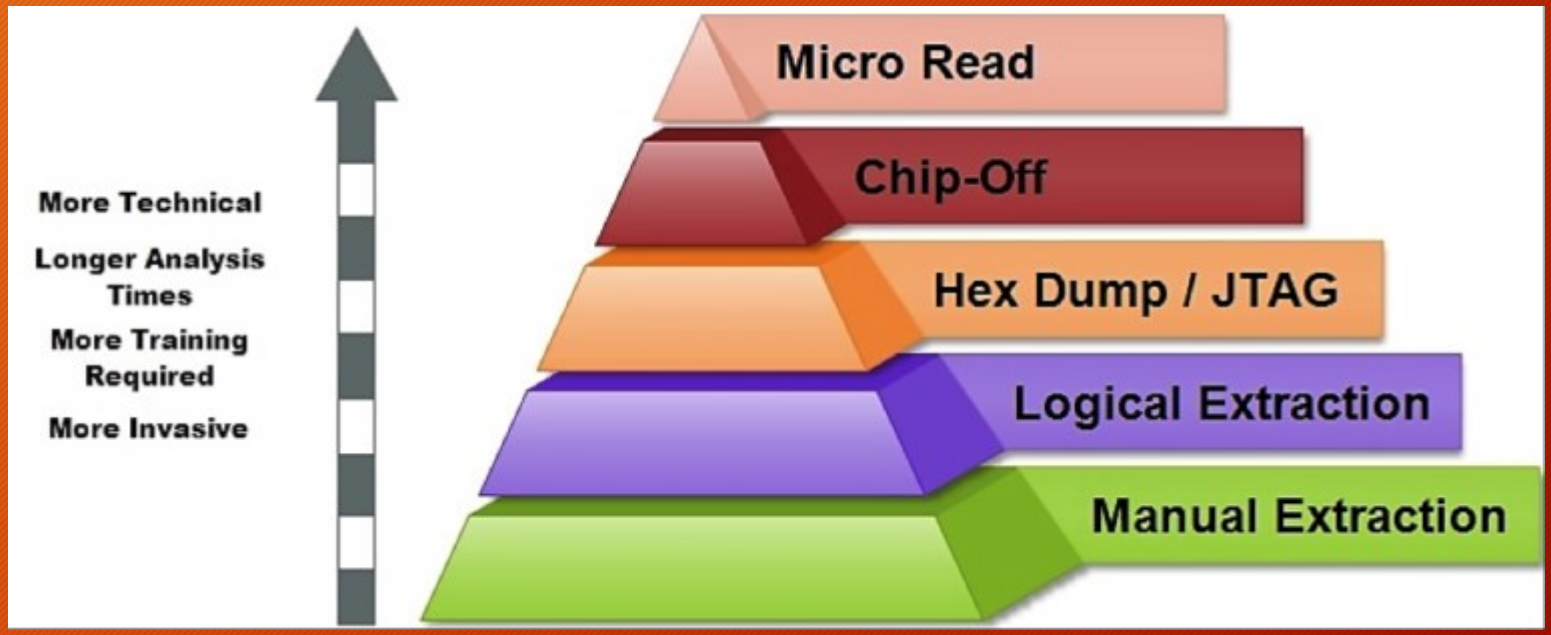
  Un caso particolare nella fase di acquisizione si ha quando ci si trova davanti ad un sistema critico, per cui per svariate ragioni non è possibile procedere all'acquisizione completa dei dati contenuti all'interno del sistema. Alcuni esempi di tali sistemi sono data center, sistemi di sorveglianza o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

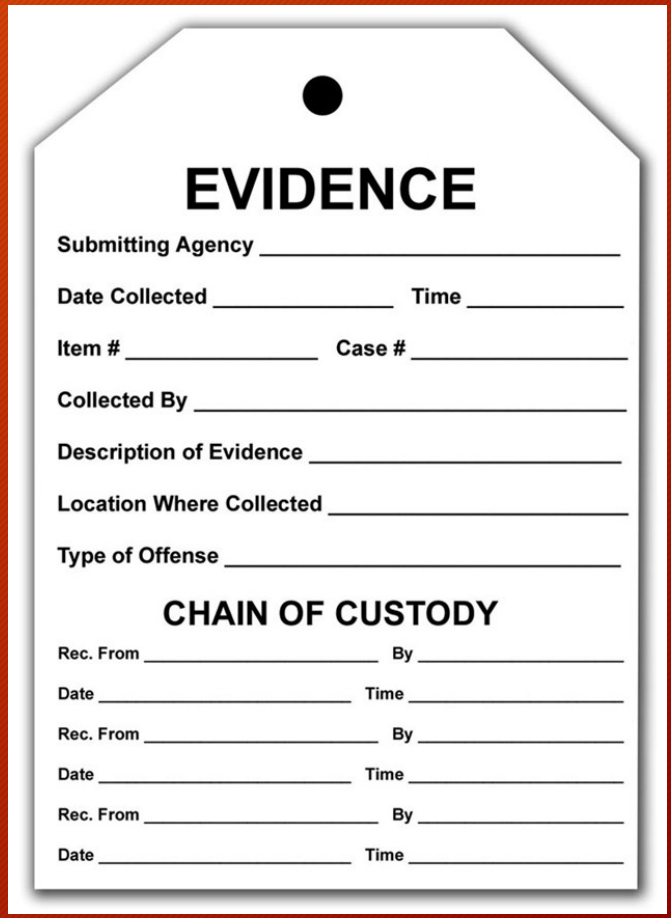
Per far ciò occorre:

- 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.

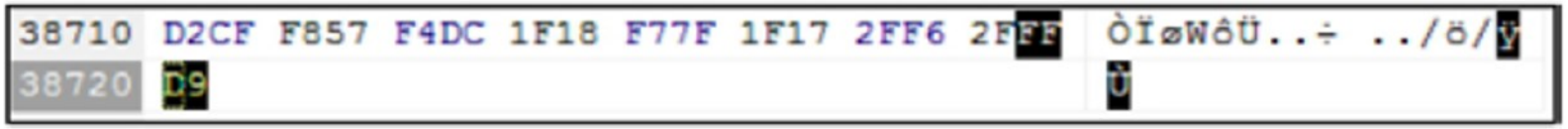


Figure 3. JPEG footer.

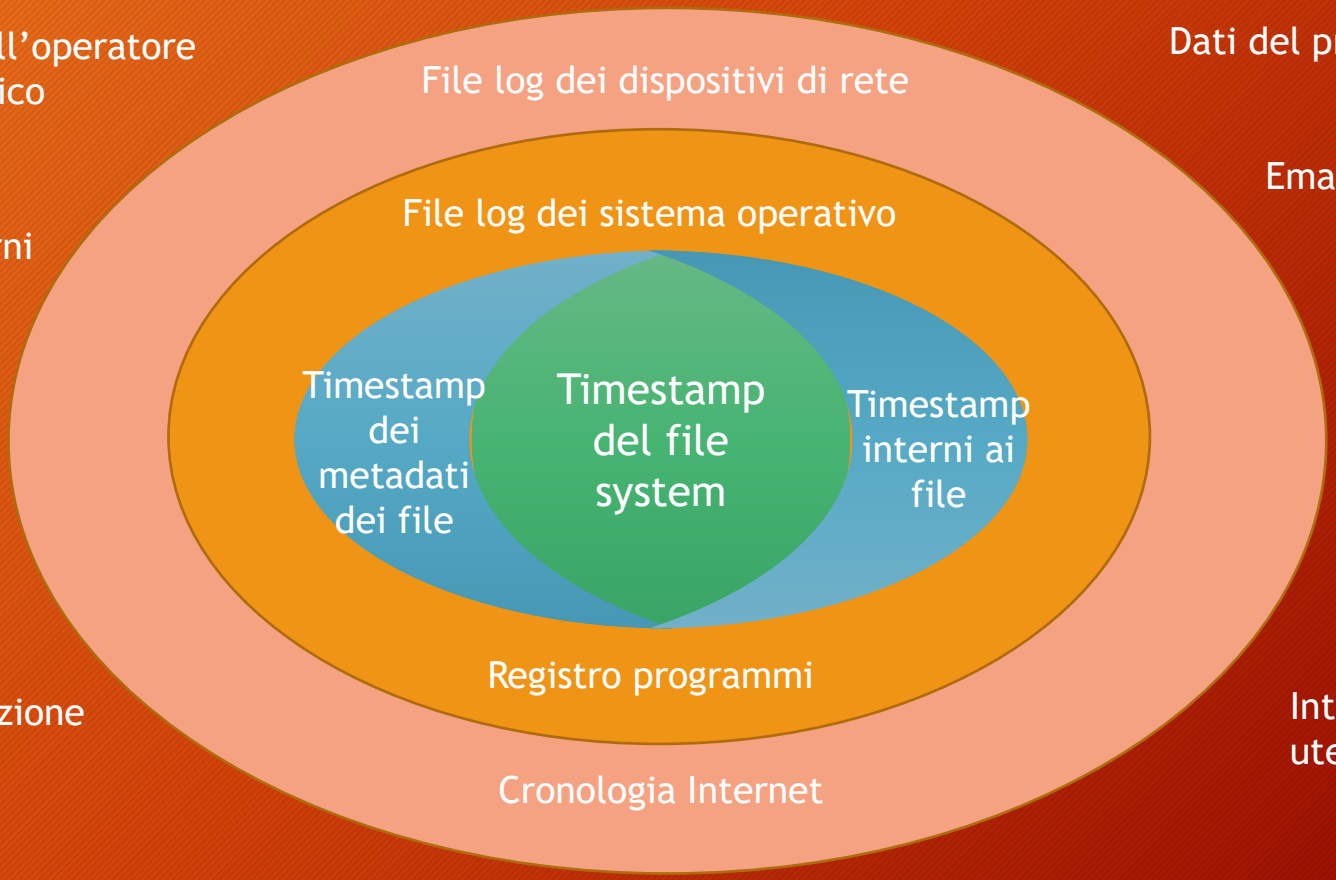
Analisi: timeline

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
   - 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

Captatori Informatici

L'utilizzo della crittografia per la memorizzazione dei dati (memorie di massa o mobile device) e la trasmissione delle informazioni rende complesso, se non impossibile, l'estrapolazione/cattura dei dati.

Una alternativa è quella di utilizzare i cosiddetti Captatori Informatici, ovvero dei RAT- Remote Access Trojan, un trojan per accesso remoto, che consente il controllo della apparecchiatura da remoto.

Installazione/inoculazione è effettuata con le tecniche di hacking.

Un RAT consente di gestire tutte le funzionalità offerte dal device con i permessi di root ed acquisire tutte le informazioni presenti, p.e.

Occorre fare attenzione ai limiti legali (non è consentito fare tutto) ed alle autorizzazioni.

Telefono	Rubrica
Microfono	Messaggi / Chat
Camera	Credenziali
GPS	Contenuti Multimediali
Apps	Posizionamento

Acquisizione a distanza

Nel caso in cui le evidenze si trovano su un server remoto raggiungibile è possibile effettuare un acquisizione da remoto. P.e.

- Una pagina web
- Un post su un Social Network
- Un'email
- Un contenuto su cloud storage (Dropbox, Google Drive, ecc.)
- Un contenuto multimediale (Youtube, ecc.)

Occorre fare molta attenzione a:

- Permessi di accesso
- Proprietà dei dati

Big Data & Artificial Intelligence

La crescente mole di dati acquisiti e da analizzare può richiedere l'uso di tecniche di gestione dei Big Data e dell'Intelligenza Artificiale.
Le prime aiutano a filtrare le informazioni pertinenti all'indagine.
Le seconde facilitano le ricerche, riducono il tempo dell'indagine ed evidenziano le connessioni tra i vari dati.

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

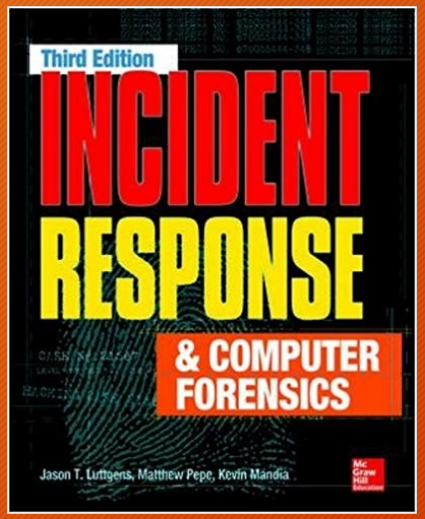
L'incarico può essere assegnato da un qualsiasi attore del procedimento:

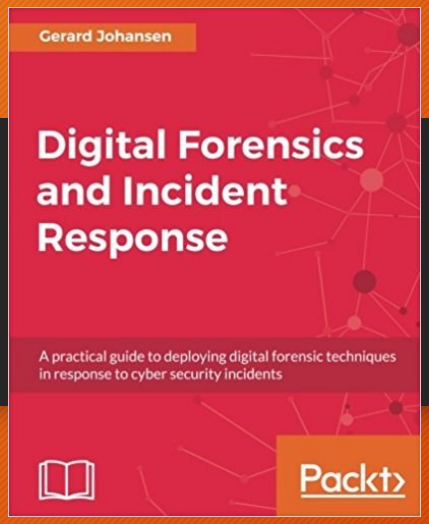
- Giudice -> Consulente Tecnico d'Ufficio (CTU)
- Pubblico Ministero -> Perito del Pubblico Ministero
- Parte Privata -> Consulente Tecnico di Parte (CTP)
- Polizia Giudiziaria -> Ausiliario della Polizia Giudiziaria

Esercitazione

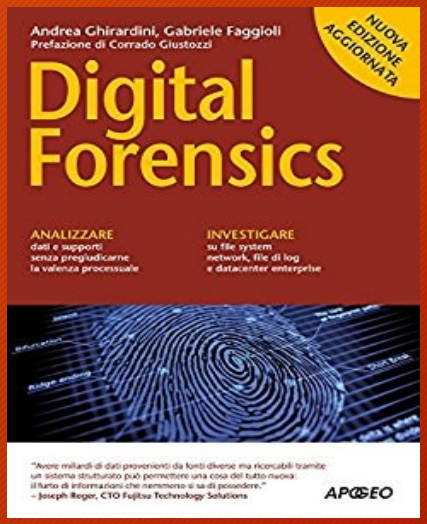
Effettuare la copia forense di una pagina web o email:

- Acquisire il codice html della pagina o email
- Acquisire tutto il traffico di rete generato (Winpcap o Wireshark)
- Realizzare un filmato di tutta l'operazione (OBS Studio)
- Applicare in sigillo digitale
- Realizzare un Report





Riferimenti



UNIVERSITÀ DEGLI STUDI DI REGGIO CALABRIA
Mediterranea

Fine

vincenzo.calabro@unirc.it

linkedin.com/in/vincenzocalabro