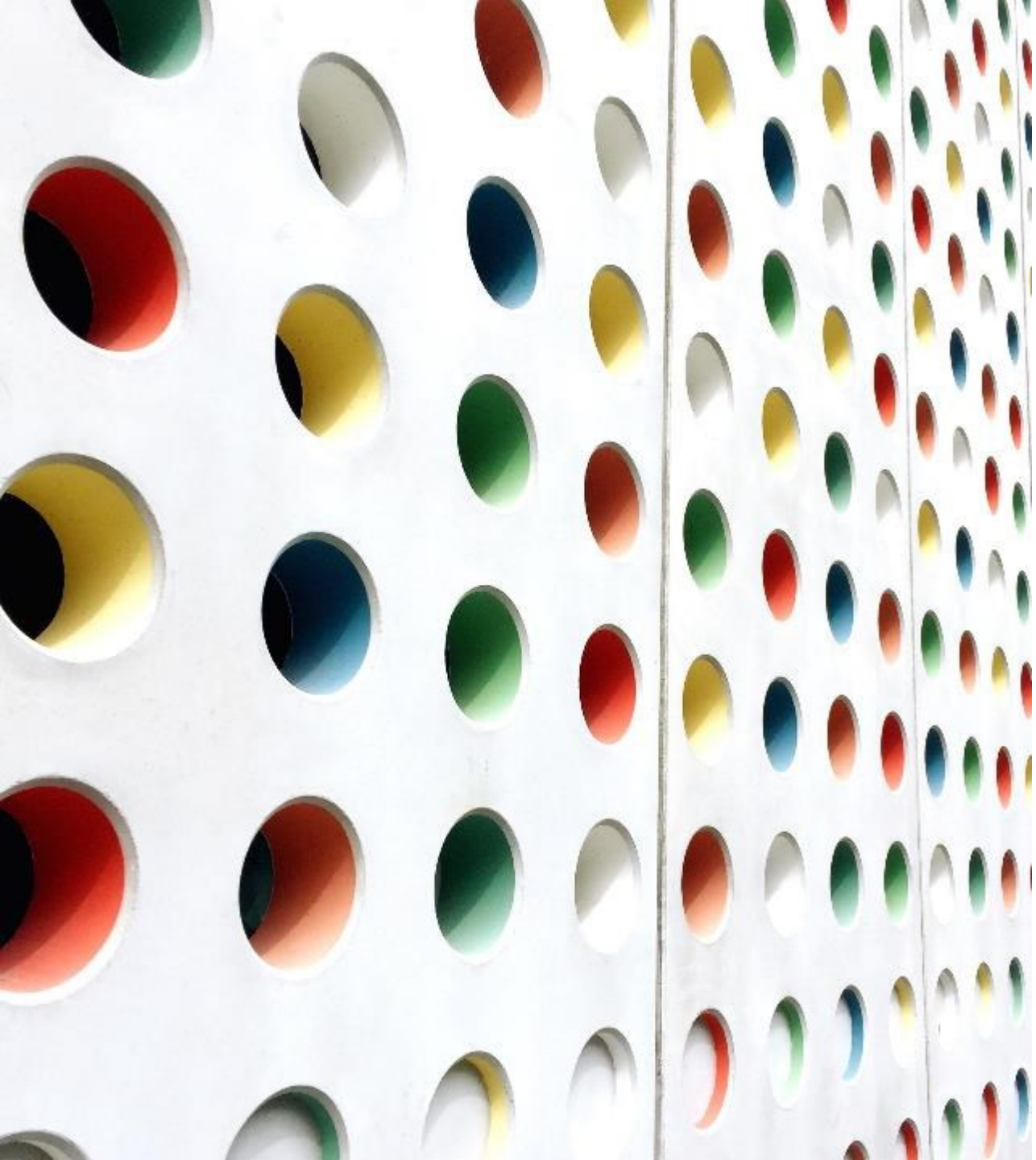


Tecnologie per la Sicurezza Informatica

Digital Forensics

VINCENZO CALABRÒ

Università degli Studi
Mediterranea
di Reggio Calabria

Agenda

1. Introduzione alla Digital Forensics
2. Ciclo di vita della Digital Forensics
   - Identification
   - Collection
   - Acquisition
   - Preservation
   - Transport
   - Examination
   - Analysis
   - Reporting
3. Applicazioni di Digital Forensics: memorie, smartphone, web, email, cloud, immagini, audio, video
4. Compliance normativa e regolatoria

Digital Forensics: perché?

La maggior parte delle azioni umane sono svolte interagendo, direttamente o indirettamente, con gli strumenti dell'ICT.

In particolare, gli incidenti informatici possono configurarsi come reati e, pertanto, occorre analizzare l'accaduto.

Distinguiamo:

- I reati tipicamente informatici
- I reati aventi ad oggetto gli strumenti dell'ICT
- I reati perpetrati attraverso l'uso di strumenti dell'ICT
- I reati che lasciano tracce sugli strumenti dell'ICT

E gli altri illeciti?

- Cause diritto civile
- Cause diritto del lavoro
- Cause diritto amministrativo
- Cause diritto tributario
- Cause diritto di famiglia
- Cause diritto commerciale
- Liti condominiali

Definizione: Digital Evidence

SWGDE *«qualsiasi informazione, con valore probatorio, che sia o meno memorizzata o trasmessa in un formato digitale»*

Eoghan Casey *«qualsiasi dato digitale che possa stabilire se un crimine è stato commesso o che può fornire un collegamento tra il crimine e chi l'ha commesso»*

Distinguiamo:

- La prova creata dall'uomo
- La prova creata autonomamente dal computer
- La prova creata sia dall'essere umano che dal computer

Definizione: Digital Evidence

A prescindere dalla definizione che vogliamo utilizzare, le peculiarità che contraddistinguono la fonte di prova digitale, che non possono essere ignorate, consistono in:

- **Immaterialità**: la prova digitale è il contenuto e non il supporto su cui è memorizzata;
- **Dispersione**: la prova digitale può essere dislocata su più dispositivi molto distanti tra loro,
- **Promiscuità**: la prova digitale può trovarsi all'interno di dispositivi che contengono altre informazioni non attinenti all'indagine,
- **Congenita modificabilità**: la prova digitale è estremamente alterabile.

Digital Evidence: valore probatorio

Il valore probatorio della prova informatica deve essere inteso come **la capacità di resistenza ad eventuali contestazioni e capacità di convincimento del giudice**, delle parti processuali o di altri soggetti in ordine alla **genuinità, non ripudiabilità, imputabilità e integrità** del dato stesso e dei fatti dallo stesso dimostrati.

Per tale motivo è fortemente consigliato impiegare tecniche e standard ispirati al **metodo scientifico**.

Scopo: Digital Forensics

Lo scopo dell'informatica forense si esplicita nelle seguenti prerogative:

identificare, conservare, acquisire, documentare e interpretare i dati presenti su una memoria digitale.

Pertanto, occorre individuare le modalità e le tecnologie migliori per soddisfare i seguenti obiettivi:

- acquisire le prove senza alterare o modificare il sistema informatico su cui si trovano
- garantire che le prove acquisite siano identiche a quelle originarie
- analizzare i dati senza alterarli
- esplicitare il processo per renderlo ripetibile

Approccio: Digital Forensics

L'approccio, che consente di svolgere al meglio l'attività, riguarda quattro aspetti essenziali:

1. un aspetto TECNICO. Il primo problema da risolvere è quello dell'aggiornamento, in quanto la tecnologia muta rapidamente, aumentano le dimensioni dei sistemi di storage e i tools di analisi diventano spesso obsoleti o non sono in grado di gestire grandi quantità di dati.
2. un aspetto PROCEDURALE. L'analisi forense deve raccogliere tutto il materiale che potenzialmente possa contenere fonti di prova, e ciò vuol dire analizzare e vagliare tantissime informazioni a supporto delle investigazioni. Il problema, da un punto di vista squisitamente procedurale, è che sovente non esistono procedure, linee guida, protocolli standard o, se esistono, non vengono molto spesso applicati, conosciuti o standardizzati.
3. un aspetto SOCIALE. Le attività di forensics pongono seri problemi sociali, soprattutto con riferimento alla privacy dell'individuo e alla raccolta e all'analisi dei suoi dati.
4. un aspetto LEGALE, o giuridico che dir si voglia. Si possono utilizzare le tecnologie più avanzate esistenti, le tecniche più sofisticate, i sistemi più sperimentali sul mercato, ma se l'attività di indagine forense sui dati informatici non è conforme alle regole, soprattutto procedurali, dettate dalla legge, tutto ciò è assolutamente inutile.

Linee guida e normative

RFC 2350 (06/1998): *"Expectations for Computer Security Incident Response"*

Convenzione di Budapest (11/2001) del Consiglio d'Europa sulla *criminalità informatica*

RFC 3227 (02/2002): "*Guidelines for Evidence Collection and Archiving*"

Legge 48/2008 (03/2008): "*Ratifica la Convezione di Budapest e modifica il C.P, il C.P.P., il D.lgs. 231/2001 e il cd. Codice della Privacy*"

ISO 27035 (09/2011-11/2016): "*Information security incident management*"

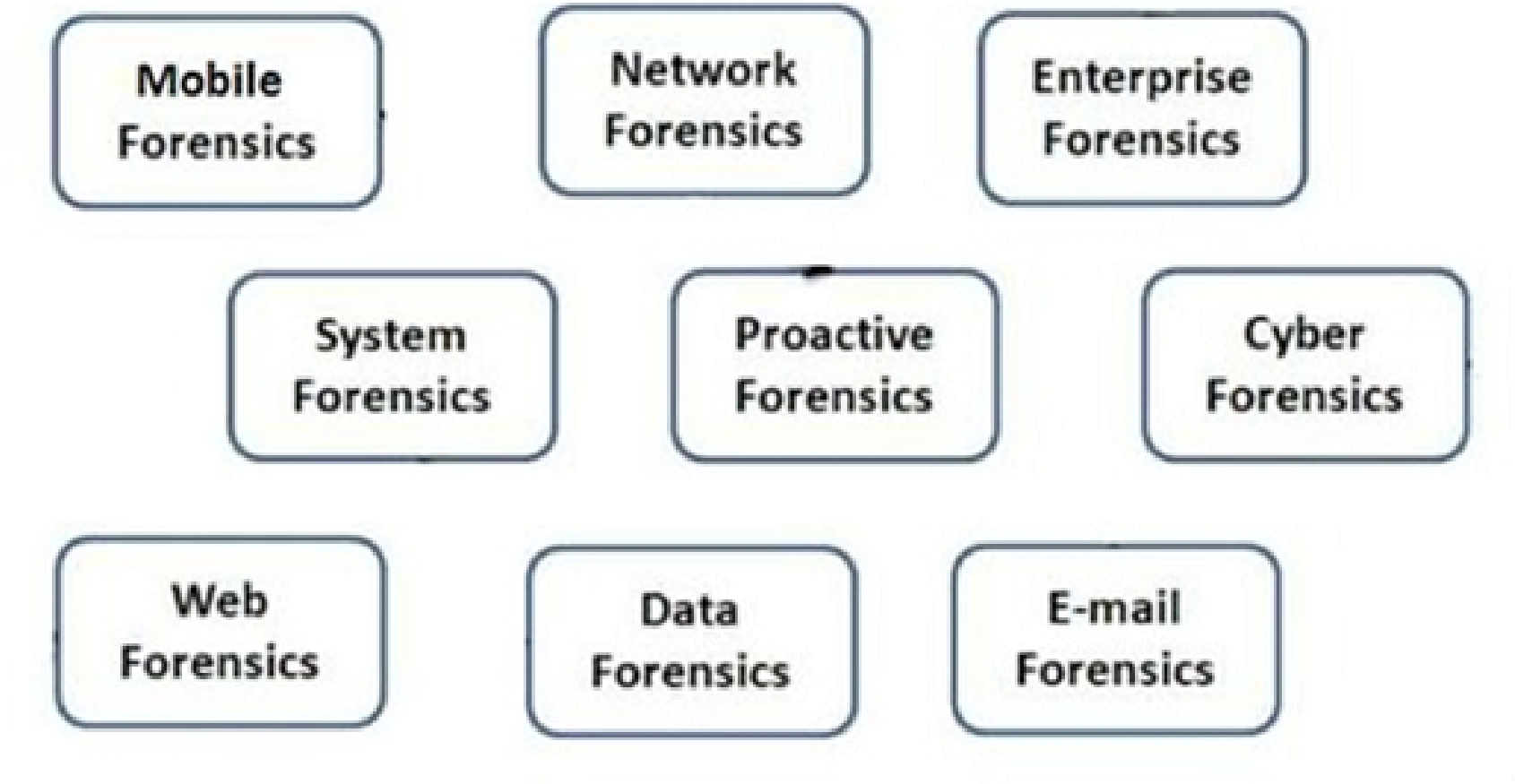
ISO 27037 (10/2012). "*Guidelines for identification, collection, acquisition and preservation of digital evidence*"

ISO 27041 (06/2015): "*Guidance on assuring suitability and adequacy of incident investigation methods*"

ISO 27042 (06/2015): "*Guidelines for analysis and interpretation of digital evidence*"

ISO 27043 (03/2015): "*Incident investigation principles and process*"

Digital Forensics: ambiti



Standard Internazionali

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. Tra queste troviamo:

- Lo standard ISO/IEC 27037:2012 "*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.
- Lo standard ISO/IEC 27042:2015 «*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.

Standard Internazionali

La norma ISO stabilisce i requisiti della prova in formato digitale
che sono di seguito riepilogati:

- **Pertinenza**: occorre dimostrare che il materiale è rilevante, cioè che contiene dati utili e che pertanto esiste una buona ragione per acquisirli
- **Affidabilità**: tutti i processi eseguiti devono essere ben documentati producendo un risultato riproducibile
- **Sufficienza**: occorre raccogliere tutto il materiale informatico necessario, valutando in base al caso e alle limitazioni di carattere giuridico
- **Verificabilità**: documentando tutte le attività svolte, un consulente tecnico informatico terzo deve essere in grado di verificare le attività svolte, valutando metodo scientifico, le tecniche e le procedure seguite
- **Giustificabilità**: bisogna essere in grado di dimostrare che le scelte adoperate erano le migliori possibili o le uniche possibili

Fasi della Digital Forensics

- Identification
- Collection
- Acquisition
- Preservation
- Transport
- Examination
- Analysis
- Reporting

IDENTIFICATION

Il processo di identificazione implica la ricerca, l'individuazione e la documentazione delle potenziali prove digitali.

Il processo di identificazione dovrà individuare gli strumenti di archiviazione digitale e i device di elaborazione che possono contenere potenziali prove digitali.

Questo processo comprende anche un'attività di attribuzione della priorità nella raccolta delle prove basata sulla loro volatilità.

Inoltre, il processo dovrà accertare l’eventualità di potenziali prove digitali nascoste.

Fasi della Digital Forensics

- Identification
- Collection
- Acquisition
- Preservation
- Transport
- Examination
- Analysis
- Reporting

COLLECTION

Una volta identificati i digital device che possono contenere potenziali prove digitali, si dovrà decidere se procedere alla raccolta/sequestro o all'acquisizione nel processo che segue.

La raccolta è un processo in cui i device che possono contenere potenziali prove digitali sono trasferiti dalla loro posizione originale ad un laboratorio.

Questo processo include la documentazione dell'intero metodo, compreso l'imballaggio di questi device prioritario al trasporto.

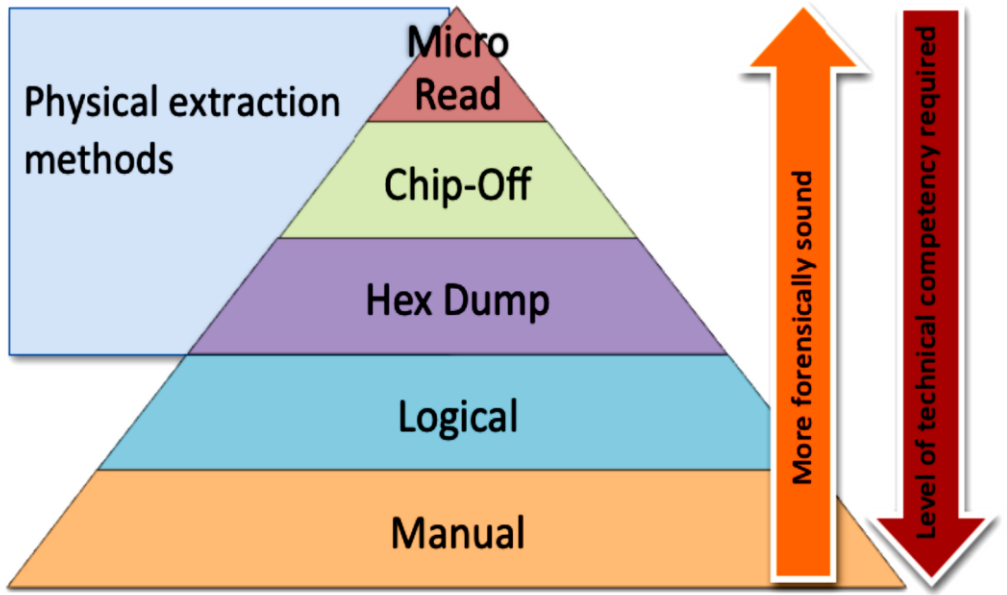
Fasi della Digital Forensics

- Identification
- Collection
- Acquisition
- Preservation
- Transport
- Examination
- Analysis
- Reporting

ACQUISITION

Il processo d'acquisizione implica la produzione di una copia forense delle prove digitali e la documentazione dei metodi utilizzati e delle attività svolte.

Occorre rispettare l'ordine di volatilità. Tipi di acquisizione:



Fasi della Digital Forensics

- Identification
- Collection
- Acquisition
- Preservation
- Transport
- Examination
- Analysis
- Reporting

PRESERVATION

La fase nella quale occorre proteggere la riservatezza e l'integrità dei supporti informatici e dei dati digitali raccolti e acquisiti.

Le potenziali prove digitali dovranno essere conservate per assicurare la loro utilità nelle indagini. È importante proteggere l'integrità delle prove. Il processo di conservazione implica la salvaguardia delle potenziali prove digitali e dei digital device che possono contenere potenziali prove digitali da manomissioni e alterazioni.

Fasi della Digital Forensics

- Identification
- Collection
- Acquisition
- Preservation
- Transport
- Examination
- Analysis
- Reporting

TRANSPORT

La fase nella quale occorre adottare gli opportuni accorgimenti per la protezione di riservatezza e integrità del supporto informatico e del dato digitale.

È importante utilizzare la catena di custodia per documentare la storia degli accessi e degli spostamenti dei reperti originali e delle copie.

Fasi della Digital Forensics

- Identification
- Collection
- Acquisition
- Preservation
- Transport
- Examination
- Analysis
- Reporting

EXAMINATION

In questa fase sono esaminate le evidenze digitali per identificare ed estrarre tutto il contenuto digitale utile alla fase successiva di analisi.

Possono essere adoperate tecniche di data carving per tentare di recuperare le evidenze cancellate.

E' possibile che il dato sia cifrato o protetto, pertanto è necessario utilizzare tecniche di hacking per ottenere il dato in chiaro.

Fasi della Digital Forensics

- Identification
- Collection
- Acquisition
- Preservation
- Transport
- Examination
- Analysis
- Reporting

ANALYSIS

Solitamente è la fase più laboriosa.

Vengono analizzate tutte le evidenze digitali estratte per tentare di rispondere al quesito.

Le evidenze possono essere messe in correlazione tra loro per ricostruire un determinato evento.

In presenza di molti dati possono essere utilizzate metodologie di big data analysis.

Fasi della Digital Forensics

- Identification
- Collection
- Acquisition
- Preservation
- Transport
- Examination
- Analysis
- Reporting

REPORTING

L'obiettivo finale è quello di redigere un elaborato in cui descrivere:

- L'origine delle evidenze
- La metodologie utilizzata
- La tecnologie adoperata
- La procedura eseguita
- I risultati ottenuti oppure la risposta al quesito

In sintesi

Il Consulente Tecnico, durante il suo operato, deve assicurare che siano rispettate cinque tipi di garanzie fondamentali:

1. il dovere di conservare inalterato il dato informatico originale nella sua genuinità
2. il dovere di impedire l'alterazione successiva del dato originale
3. il dovere di formare una copia che assicuri la conformità del dato informatico acquisito rispetto a quello originale
4. il dovere di assicurare l'immodificabilità della copia del documento informatico
5. la garanzia delle installazioni di sigilli informatici sui documenti acquisiti

Memory Forensics

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 (sequestro) o acquisizione?

Dopo aver identificato i reperti e scelto se sequestrarli o acquisirli in loco occorre:

- Valutare cosa è pertinente e cosa è trascurabile
- Acquisire tutto quello che è necessario
- Assegnare un identificativo ad ogni reperto ed etichettarlo
- Compilare una scheda con le informazioni visibili (marca, modello, seriale, ubicazione, stato, condizioni, collegamenti)
- Stabilire un piano di acquisizione efficace e conforme agli obiettivi dell'indagine

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 cifratura 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.

Preservazione

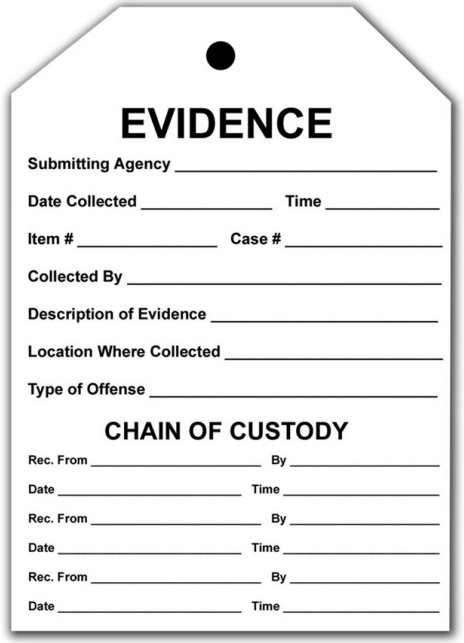
Occorre garantire che sia preservata, con i dovuti accorgimenti, la confidenzialità, l'integrità e la disponibilità della potenziale prova.
L'evidenza, infatti, va preservata sia durante il trasporto che lo stoccaggio, che potrebbe superare il suo tempo di vita a seconda dei tempi di giustizia.
In caso di modifica accidentale o incidentale, deve essere giustificata e documentata con apposito verbale.
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

Data la fragilità dei dati e dei supporti che li contengono, questi ultimi devono essere protetti e sigillati per evitare modifiche o guasti e deve essere creata la Catena di Custodia.

- Documentare movimenti e interazioni con la fonte di 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



Acquisizione forense

La copia forense è un duplicato fedele della memoria originale in ogni sua parte.

Le copie eseguite a basso livello sono dette bit stream image.

Possiamo distinguere alcuni tipi di acquisizioni:

- **Post mortem**: (dopo lo spegnimento) si scollega il dispositivo dal sistema di origine e lo si collega ad un postazione forense dotata di write blocker.
- **Live**: (direttamente sul sistema di origine) nel caso in cui non è possibile o è complicato scollegare i supporti di massa (dischi RAID o memoria saldate) la copia è effettuata sulla stessa macchina
- **Tramite rete**: è possibile trasferire la copia attraverso la rete

Acquisizione

Occorre stabilire e rispettare l'ordine di volatilità:

- Registri, Memoria Cache
- Memoria RAM
- Stato della rete (connessioni, socket in ascolto, applicazioni coinvolte, arp cache, routing table, dns cache, ecc.)
- Processi attivi
- Supporti di massa collegati (memorie interne: hd, pendrive)
- Log remoti
- Dispositivi rimovibili (memorie esterne: floppi, nastri)
- Supporti di backup (ottici e magnetici)

Acquisizione

- Le copie eseguite devono essere identiche o il più possibile simili all'originale (in tal caso occorre giustificare la scelta)
- Durante la copia dell'origine, quest'ultima non deve essere modificata (integrità)
- Nel caso in cui non ci sia un metodo che consenta di evitare di alterare l'originale, la scelta va giustificata e documentata
- Le procedure devono essere attuate e documentate secondo metodologie e tecnologie riconosciute, in modo da poter essere verificabili dagli altri attori (verificabilità)
- Potrebbe essere necessario eseguire copie parziali della memoria del dispositivo, anche in questo caso la scelta deve essere motivata e documentata

Acquisizione forense

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 forense

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.

Algoritmi di hashing

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 inalterata ed identica all'originale.

L'algoritmo di hash (MD5, SHA-1) 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)

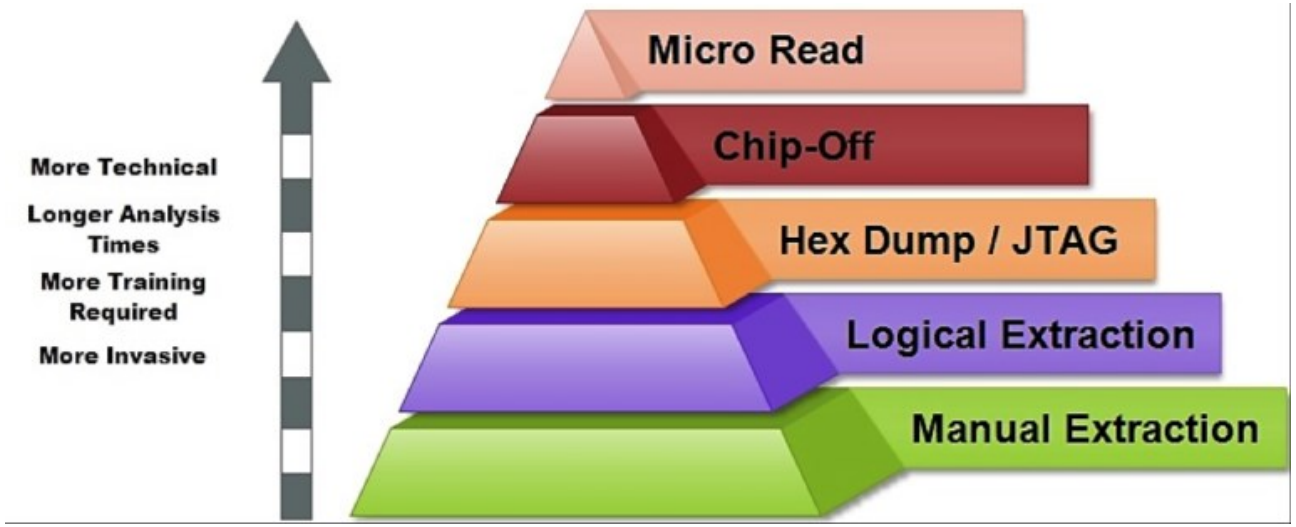
DPCM 8 febbraio 1999: «l'impronta di una sequenza di simboli binari è una sequenza di simboli binari di lunghezza predefinita generata mediante l'applicazione alla prima di un'opportuna funzione di hash»

Algoritmi di hashing

- L'algoritmo restituisce una stringa di numeri e lettere (detto digest) a partire da un qualsiasi flusso di bit di qualsiasi dimensione finita.
- La stringa di output dell'algoritmo è univoca per ogni documento identificato. Pertanto, l'algoritmo di hashing è utilizzato per la firma digitale.
- La lunghezza del digest varia a seconda degli algoritmo utilizzato
- L'algoritmo non è invertibile, cioè non si può ricavare la sequenza di bit in ingresso a partire dal digest.

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 perché include:

tutti i file, anche quelli cancellati, lo slack space e lo spazio libero.

Tipi di copia forense

Un dispositivo di memoria può essere copia in due modalità:

- Device to device
- Device to file

Nel secondo caso, quello più utilizzato, si può scegliere:

- Il formato: RAW (dd), EWF o AFF (compressi)
- Lo split su più file
- Livello di compressione
- La cifratura
- I metadati
- Calcolo degli hash
- È possibile memorizzare più copie sullo stesso device

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 dispositivi che impediscono l'alterazione del supporto di origine: c.d. write-blocker

Acquisizione live

Nel caso in cui ci dovesse capitare di trovare le apparecchiature in funzione oppure non è possibile spegnerle (macchine critiche), occorre effettuare l'acquisizione della ram e delle altre informazioni presenti all'interno della macchina.

In questo caso sono utilizzate le distribuzioni che consento di eseguire programmi presenti su altri dispositivi (DVD o Pendrive) senza intaccare la memoria di massa.

Lo stesso tipo di acquisizione può essere sfruttata su quelle macchine dove è complicato raggiungere la memoria, in questo caso il sistema può essere avviato direttamente dalla distribuzione in modalità Live.

Attività di preview o triage

Potrebbe essere necessario effettuare una preview del contenuto del sistema (per esempio durante un'ispezione) oppure acquisire solo alcune informazioni (perquisizione)

Oppure semplicemente occorre valutare se quel dispositivo è pertinente con l'obiettivo dell'attività oppure no.

È importante che qualsiasi attività posta in essere, anche se non comporta alcuna modifica dei dati, sia documentata in un apposito verbale di ispezione o perquisizione.

Acquisizione logica

In determinate condizioni, potrebbe essere necessario effettuare la copia logica, ovvero una copia parziale del contenuto del dispositivo.

Questa ipotesi si verifica principalmente nei dispositivi:

- Cifrati
- Server
- Mobile
- Condivisi o multifunzione

In pratica in quei dispositivi dove è necessario operare con il sistema operativo acceso oppure dove le informazioni di interesse sono circoscritte a determinati file.

Acquisizione della RAM

La RAM (Random Access Memory) è una memoria di tipo volatile, che permette l'accesso diretto a qualunque indirizzo di memoria con lo stesso tempo di accesso.

Dopo lo spegnimento del dispositivo i dati vengono persi.

L'acquisizione della RAM si effettua a sistema acceso.

È utile acquisire la RAM quando:

- Si vuole recuperare le password o le informazioni presenti in memoria
- Per tenere traccia dei processi attivi ed analizzarli successivamente
- Per recuperare informazioni dai software che non lasciano tracce
- Nel caso di analisi di malware, rootkit o trojan

Acquisizione della RAM

- Eseguire il tool di acquisizione da dispositivo esterno (pendrive, DVD)
- Salvare il contenuto su dispositivo esterno per non intaccare i dischi locali
- Se la macchina da clonare è virtuale basta usare il comando «snapshot»

Software per acquisire e analizzare la RAM

- Volatility
- AccessData FTK Imager
- Windows Memory Reader
- Magnet RAM Capture

Verifica e apertura di un immagine forense

- È possibile verificare l'integrità di una copia forense ricalcolando l'hash sulla stessa immagine e confrontandolo con quello calcolato al momento della realizzazione della copia
- In base alla modalità con cui è stata eseguita la copia forense, (raw, split, ewf, aff, clone) ci sono diverse alternative per l'accesso in fase di analisi
- Il fine è quello di poter accedere al contenuto (filesystem, aree allocate e non) dell'immagine acquisita per poter eseguire le verifiche richieste
- Alcuni formati prevedono solo l'acceso in sola lettura

Problematiche

- Dischi cifrati
- Memorie SSD
- Sistemi di sicurezza logica
- Sistemi embedded

Esempio: Memory Forensics

Analisi

L'analisi deve consentire:

- la ricostruzione degli eventi passati attraverso la lettura dei dati rinvenuti.
- L'estrazione dei dati e l'elaborazione per ricostruire le informazioni
- L'interpretazione delle informazioni per individuare gli elementi utili all'indagine
- La comprensione e correlazione dei dati, in modo da affinare le ricerche e poterne trarre le conclusioni

È sicuramente la fase più laboriosa di tutto il processo e richiede conoscenze multidisciplinari.

Analisi: caratteristiche

Poiché ogni copia coincide con l'originale, l'analisi va eseguita sulla 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: correlazione dei dati

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)

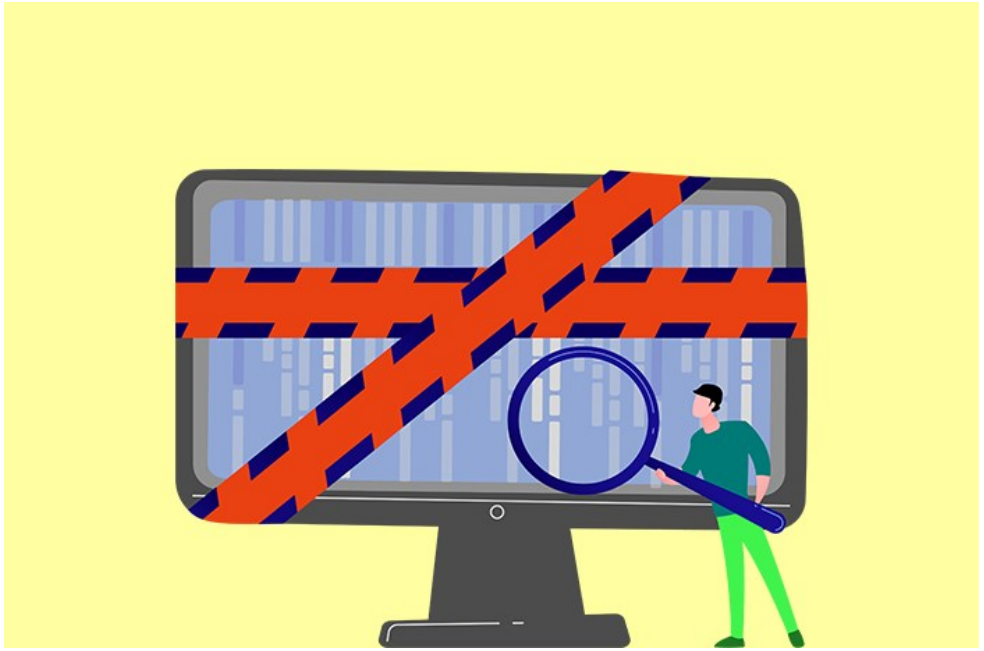
Recupero dati
- Recupero dati cancellati, carving…

Interpretazione dati

Conversione tra formati

Crack password
- File tipicamente protetti
- Tipologie di attacco

Artefatti del sistema operativo



Recupero dei dati cancellati

Quando si cancella un file, i dati non sono immediatamente azzerati, ma soltanto derefenziati, ovvero viene cancellata la voce sul registro del file system che consente di richiamarlo.

I dati, di conseguenza, sono ancora sul supporto di memoria, ma lo spazio precedentemente occupato risulta deallocato (libero)

Anche i metadati potrebbero essere ancora presenti in maniera analoga sul File system (MFT)

Per il recupero dei file cancellati possono essere percorse due soluzioni alternative:

- Analisi dei metadati del file system
- File carving

Recupero dei dati cancellati

Recupero tramite analisi dei Metadati:

- Strettamente dipendente del File system
- Consente di ricostruire anche i file frammentati
- È possibile recuperare altre informazioni tra cui:
  - il nome del file
  - la data di creazione
  - la data di modifica
  - la data di ultimo accesso
  - il proprietario (dipende dal File system)
  - Permessi scrittura e lettura

Recupero dei dati cancellati

Recupero tramite File Carving:

- Se il dato è completamente dereferenziato, l'unico recupero possibile è tramite la scansione del Binary Large Object
- Vengono ricercate le intestazioni (header o magic number) identificative di specifici formati di file
- Si cerca di interpretare quello che segue come parte integrante del file (se esiste viene cercato anche il footer)
- Funziona bene nel caso in cui i file siano allocati su cluster contigui, ma non in caso di frammentazione
- Non recupera le informazioni come il nome originario del file e gli altri metadati del file system

Data 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 la struttura del file system viene ignorata.

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

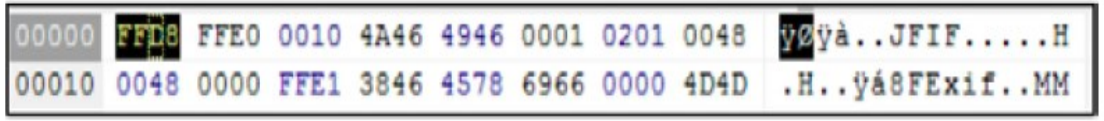


Figure 2. JPEG header.

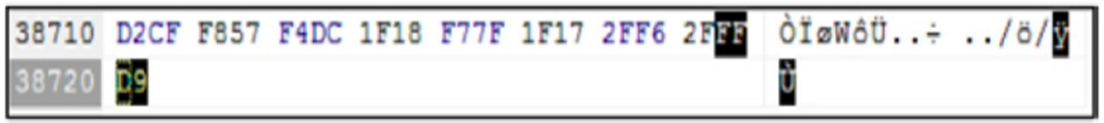


Figure 3. JPEG footer.

Analisi dei metadati

I metadati sono dati riguardanti altri dati. Spesso hanno un ruolo fondamentale nelle indagini digitali.

- Possono fornire informazioni importanti riguardanti il documento stesso, l'autore e la data e ora di creazione e modifica.
- Possono rilevare informazioni che si è tentato di oscurare, nascondere o cancellare
- Possono essere utilizzati per correlare i documenti allo loro fonte

Esempi di metadati:

- File system
- Documenti (office, pdf, ecc.)
- Immagini (dati exif)
- Audio / Video
- Email
- Applicazioni

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)

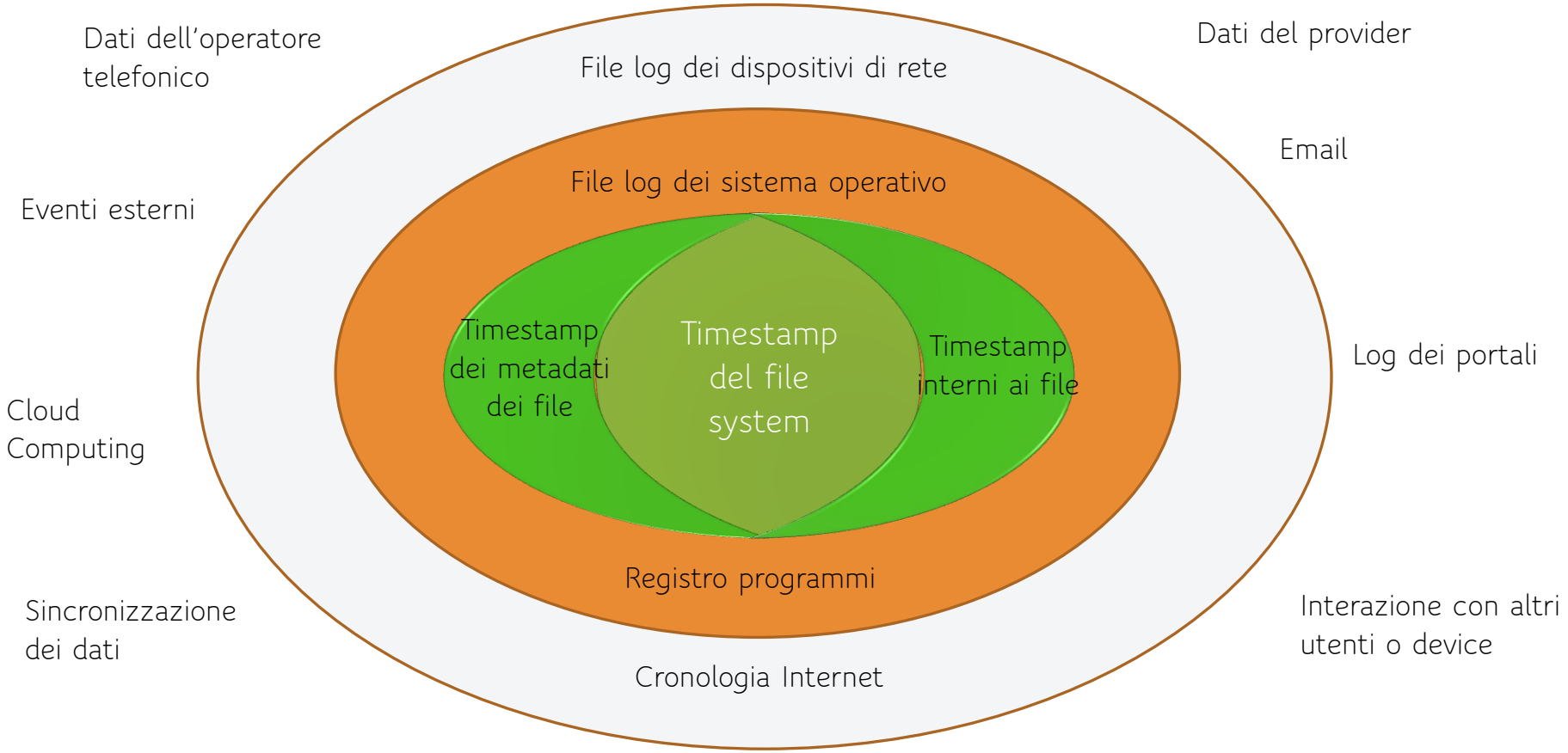
Esecuzione dei programmi (S.O. registra informazioni sull'esecuzione dei programmi)

- 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



Esempio: Memory Analysis

Virtualizzazione delle immagini forensi

- Potrebbe essere necessario effettuare accertamenti direttamente sulla macchina accesa (p.e. per verificare il funzionamento di un programma o interrogare un database)
- La soluzione che consente di effettuare questo tipo di analisi, consiste nel creare una macchina virtuale a partire dalla copia forense, che deve essere obbligatoriamente bit a bit, e successivamente si esegue
- La macchina virtuale deve avere le schede di rete **disabilitate**
- Possono essere eseguiti programmi, in formato portable, per estrarre informazioni utili alle indagini
- Il vantaggio della macchina virtuale è legato soprattutto alla ripetibilità delle operazioni eseguite

Valutazione

La valutazione è una fase necessaria per stabilire:

Se il reperto informatico è stato

- alterato
- inquinato
- contraffatto

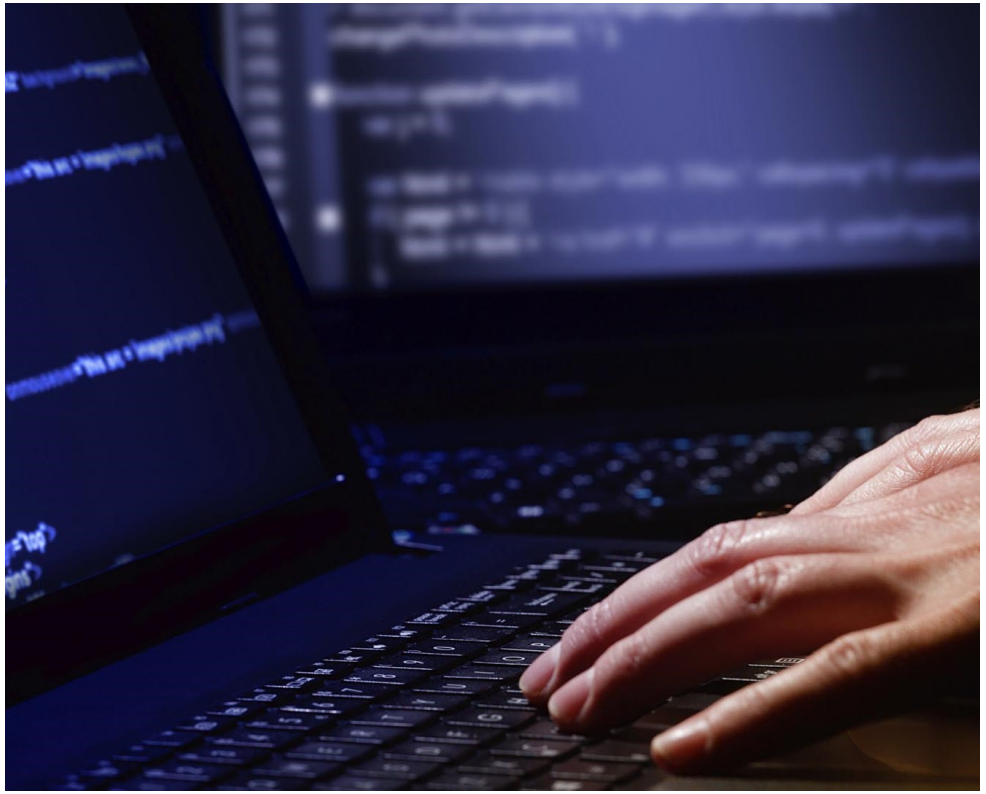
Se le procedure di acquisizione sono state legittime

Se il reperto è

- attendibile
- integro
- Autentico

Il significato dei dati presenti sul supporto

Esempi di ricerche



- Ricerca per parole chiave
- Utilizzo delle periferiche usb
- Analisi dei documenti aperti e utilizzati
- Ricostruzione della navigazione in internet
- Manomissione delle prove
- Cronologia dei programmi
- Conferma di un alibi
- Verifica dell'autore

Presentazione

Dopo aver completato le fasi tecniche, occorre predisporre una sintesi dell'intero processo tramite l'esposizione, entro i limiti concordati, delle informazioni fattuali ricavate dalle prove e dall'insieme di esami ed analisi che hanno costituito l'indagine. Questo obiettivo si concretizza attraverso la redazione di un elaborato o report da cui sia possibile ricavare:

- l'origine delle fonti di prova digitale,
- la metodologia utilizzata per la gestione delle fonti di prova,
- la tecnologia adoperata per il trattamento delle fonti di prova,
- la procedura eseguita per giungere ai risultati conseguiti,
- i risultati ottenuti (anche sottoforma di allegati multimediali),
- la risposta al quesito.

Presentazione

Un metodo suggerito per la stesura della relazione finale consiste nello sviluppare e strutturare la presentazione seguendo lo stesso ordine delle fasi ISO descritte nei paragrafi precedenti.

La presentazione dei risultati è l'elemento con cui si valuta tutta l'attività svolta. Per cui, durante la stesura, è fortemente consigliato tener conto delle seguenti indicazioni:

- occorre essere semplici e chiari,
- i risultati devono essere esposti in una forma facilmente comprensibile a tutti,
- i destinatari non hanno di solito competenze informatiche,
- molto probabilmente la relazione sarà esaminata da un tecnico della controparte,
- non bisogna essere approssimativi o esprimere giudizi che non siano corroborati dai dati.

Report

Tipologia: La Perizia e la Consulenza tecnica

La perizia e la consulenza tecnica sono i due mezzi di prova attraverso i quali fa ingresso nel processo penale il sapere tecnico, scientifico e artistico.

Entrambe si sostanziano, alternativamente o cumulativamente, nello svolgimento di indagini, nell'acquisizione di dati o nell'effettuazione di valutazioni che richiedono per la loro natura particolari competenze tecniche, scientifiche o artistiche.

- La perizia (artt. 220 e ss.c.p.p.) costituisce mezzo di prova "neutro" (essendone affidato l'espletamento ad un soggetto terzo, quindi imparziale, nominato dal giudice) ed essenzialmente discrezionale (essendo rimessa al giudice la valutazione sul requisito della sua "occorrenza"). Oltre che a richiesta di parte, può essere disposta anche d'ufficio.
- La consulenza tecnica, invece, può esperirsi: nell'ambito di una perizia già disposta, concedendo alle parti facoltà di nominare propri consulenti che possono partecipare alle operazioni peritali al fine di realizzare il contraddittorio nella formazione della prova (art. 225 c.p.p.).

Report/Relazione

Parti essenziali:

Premessa

- *Curriculum del consulente*
- Oggetto dell'Incarico
- Quesiti formulati
- *Breve descrizioni dei Fatti*

Fasi dell'Attività

- *Documenti e/o Evidenze forniti ed analizzati*
- *Metodologia applicata*
- Strumenti (hardware e software) utilizzati
- Descrizione dettagliata delle operazioni eseguite (anche foto e video)

Risultati

- Risposte ai quesiti
- Conclusioni
- *Elenco Allegati*

Internet Forensics

Acquisizione a distanza

La nascita del c.d. Web 2.0 e la crescente pervasività delle tecnologie ha favorito la proliferazione di diversi servizi Internet (**Newsgroup, Blog, Chat, Social network**), utilizzati per la diffusione delle informazioni, spesso non regolamentati e coperti dall'anonimato.

Ciò ha incrementato il numero di determinati reati quali:

la diffamazione, lo stalking (cyber-stalking), l'hate-speech, l'adescamento telematico (grooming), la pedopornografia, il reverge porn, il sextortion, il furto d'identità digitale, la sostituzione di persona, la violazione di copyright e l'utilizzo illecito di marchi, il furto dei dati, il phishing, le truffe online, l'accesso abusivo ad una banca dati, la violazione della privacy, il controllo a distanza illecito, l'assenza di tutela legale, l'intercettazione abusiva, gli attacchi denial of service, il danneggiamento degli apparati di telecomunicazione, ecc.

Problema

In base alle caratteristiche di alcuni dei predetti servizi, le informazioni oggetto di reato possono essere volatili e, quindi, facilmente manipolabili o rimovibili.

Quindi abbiamo la necessità di acquisire in maniera certa e sicura le evidenze presenti online da diversi fonti e servizi diversi.

La soluzione consiste nel realizzare una acquisizione forense e certificata del contenuto che si contesta così come è consultabile, che diventerà evidenza, prima che possa scomparire.

Tipologie di dati online

- siti web, forum, gruppi di discussione
- posta elettronica e mailing list
- Dati di geolocalizzazione
- profili, pagine, gruppi su social network
- file sharing
- streaming audio/video
- servizi o app web per dispositivi desktop e mobile
- chat, gruppi, supergruppi, canali e bot
- messaggi delle piattaforme di messagistica
- informazioni sui conti delle cripto valute

Acquisizione di una pagina web

La stampa in PDF o su carta può essere utilizzata come prova?

Le stampe o gli screenshot difficilmente sono ammessi in un procedimento giudiziario come prova perchè non godono dell'integrità delle evidenze informatiche raccolte con strumentazione adeguata e metodi scientifici.

Anche la fotografia dello schermo del PC non ha pienamente valore probatorio, o meglio, può essere facilmente essere contestata dalla controparte, poiché per quanto possa avere una storicità temporale (l'ora esatta potrebbe essere contenuta nell'immagine, ovvero il sistema che l'ha generata si sincronizza automaticamente con l'ora esatta e salva le immagini in modo incrementale) ritrae qualcosa che può facilmente essere artefatto (lo schermo).

Identificazione dei contenuti web

Iniziare a raccogliere le informazioni a latere:

- l'indirizzo del sito/servizio (whois)
- il proprietario del sito/servizio
- la tecnologia utilizzata per creare il sito/servizio
- l'autore dell'informazione (ID user)
- i dati identificativi dell'informazione (ID del post, l'ora e la data)
- Creare la storyboard dei contenuti che occorre acquisire per
  - rappresentare l'informazione d'interesse
  - dimostrare l'autore della pubblicazione (profiling)
    e delle altre informazioni a latere
    che aiutano a rafforzare l'autenticità del dato

Identificazione tools

Per individuare le informazioni sul Target si suggerisce l'utilizzo di alcuni servizi web quali:

- DOMAINTOOLS (https://whois.domaintools.com/): un portale che ci consente di ottenere le informazioni sul nome di dominio, il proprietario, l'indirizzo del server, la localizzazione, ISP ed i suoi DNS di riferimento;
- IPINFO.IO (https://ipinfo.io/): consente di ottenere informazioni dettagliate sull'indirizzo IP;
- WAPPALYZER (https://www.wappalyzer.com/): rileva le tecnologie in uso sul server;
- SHODAN (https://www.shodan.io/): un motore di ricerca dedicato alla ricerca dei dispositivi collegati ad Internet e ci consente di scoprirne anche le tecnologie impiegate.

Per reperire le informazioni concernenti la Connettività e la postazione Client è sufficiente eseguire interrogare il sito:

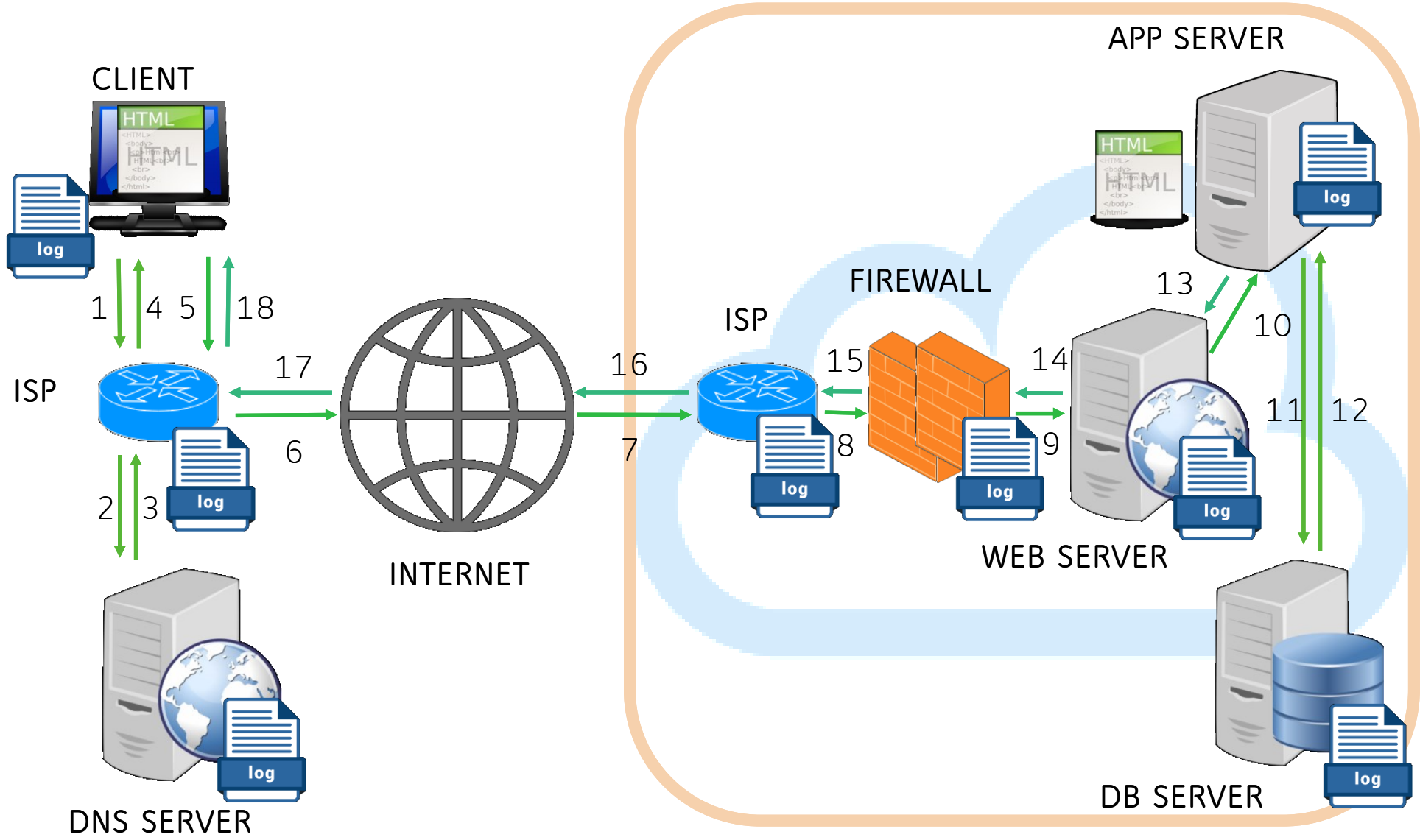
- IP Analyzer (https://ipalyzer.com/) (inserendo il proprio indirizzo ip visibile in homepage)
- Data e ora esatta
- ipconfig /all

Collection

Dopo aver identificato i contenuti è necessario decidere la strategia di acquisizione / sequestro.

Alcune delle opzioni possibili sono le seguenti:

- Realizzare una copia forense presso il service provider
- Chiedere l'estrazione dei dati al service provider
- Sequestrare il contenuto presso il service provider
- Effettuare una copia forense a distanza


CLIENT
HTML
log
1
4
5
18
ISP
17
6
2
3
log
DNS SERVER
INTERNET
16
7
ISP
15
8
log
FIREWALL
log
14
9
APP SERVER
HTML
log
13
10
log
WEB SERVER
11
12
log
DB SERVER

Acquisizione on-premise

La modalità on-premise (in sede) consente di prelevare le evidenze direttamente dalla fonte e può prevedere la raccolta dei seguenti elementi:

La copia forense della memoria dei servers (anche parziale)

- I logs dei servers (WEB, APP, DB)
- I logs del traffico dell'ISP che ospita i server
- I logs del traffico dell'ISP da cui è stata effettuata la connessione
- I logs dei DNS server
- I logs del traffico telefonico (per risalire all'utenza telefonica)
- La copia forense del client da cui è stato eseguito il reato

Acquisizione off-premise

È la tecnica utilizzata per realizzare una «preview» del dato e nei casi in cui non è possibile intervenire in presenza sui dispositivi su cui sono memorizzate le evidenze di interesse.

L'acquisizione forense a distanza può essere eseguita quando si verifica uno della seguenti ipotesi:

- il nodo/server non è agevolmente identificabile e raggiungibile. Si pensi, ad esempio, alle infrastrutture dei grandi Social Media o degli Operatori OTT - Over-The-Top ,
- non siamo nelle condizioni giuridiche per chiedere ad un terzo la copia forense di un dato, anche se è pubblico, perché siamo in una fase di precontenzioso;
- il server si trova in uno stato estero per cui è necessaria una rogatoria internazionale di difficile attuazione;
- il dato d'interesse ha un alto grado di volatilità, si pensi ad un post pubblicato su un portale social, e pertanto si rischia di non trovarlo più disponibile;
- il tempo concesso per svolgere l'indagine non è compatibile con le tempistiche scandite da questa modalità di acquisizione.

Prerequisiti

Affinché l'acquisizione a distanza di un contenuto web sia corretta e provi l'esistenza di un dato elemento anche se l'elemento verrà cancellato, ovvero risponda ai requisiti di integrità, autenticità e disponibilità, è necessario garantire le seguenti condizioni:

- l'operatore ha compiuto le operazioni corrette
- l'ambiente di acquisizione è idoneo (p.e. VM)
- la connessione tra il client e il server è affidabile
- Le attività sono riscontrabili all'interno dei logs

Raccolta (Sequestro)

La fase di raccolta (o sequestro) è un'attività posta in essere quando è necessario rimuovere o spostare la fonte di prova dal luogo di origine e, solitamente, viene disposta dall'Autorità Giudiziaria o da chi ne ha competenza.

Nella fattispecie di indagine che stiamo analizzando, ovvero le investigazioni a distanza, questa operazione non può essere realizzata fisicamente, ma, se necessario, può essere portata a termine in uno dei seguenti modi:

- Se la risorsa è pubblica: si ordina all'Internet Service Provider di metterla off-line;
- Se la risorsa è protetta: si acquisiscono tutte le credenziali di accesso (dal proprietario o dall'ISP) e si modificano o disabilitano per renderla inaccessibile agli altri.

Cosa acquisiamo?

Per rispondere ai predetti prerequisiti è utile acquisire:

- I comandi eseguiti dall'operatore
- Il log del traffico di rete generato
- Le richieste effettuate al servizio web
- Le risposte ricevute dal servizio web
- Gli oggetti ipertestuali, multimediali o di altro formato digitale ricevuti dal servizio web
- Altre informazioni a latere utili a dimostrare la validità delle informazioni (data e ora certa, id utente)
- Se disponibile anche i log (o similari) lato server

Come acquisiamo?

L'operatore incaricato di effettuare un'acquisizione di fonti prova online deve preliminarmente effettuare una serie di scelte tra le seguenti opzioni:

1. La modalità di acquisizione:
   automatica o interattiva
2. Il luogo da cui effettuare l'acquisizione:
   hosted o client
3. Gli strumenti e i comandi.

MIME HTML Format (RFC 2557)

È un formato di archiviazione dei dati pensato per il salvataggio di pagine web e documenti ipertestuali. Consente di riunire in un unico file sia il codice HTML che gli altri elementi richiamati dal documento come ad esempio immagini, file audio, applet Java o animazioni Flash.

MHTML non è attualmente considerato uno standard, per quanto già dal 1999 ne sia stata proposta la standardizzazione (RFC 2557), ma è implementato dai principali browser web.

In particolar modo, i browser Chromium based sfruttano la libreria Blink (Rendering Engine) (https://www.chromium.org/blink).

Web ARChive: ISO28500 File Format

Target Websites and Social Media

WARC ISO 28500 File

```
WARC/1.0
WARC-Type: response
WARC-Record-ID: <urn:uuid:7004e5fd-3f87-f10f-0539-
e116845021fe>
WARC-Date: 2011-11-01T18:12:33Z
WARC-Target-URI: http://news.bbc.co.uk/
WARC-Concurrent-To: <urn:uuid:58c7c6ab-458e-008a-
cda5-41ccda1ce188>
X-Hanzo-Page-Id: <bbc.warc>
X-Hanzo-Page-Uri: http://news.bbc.co.uk
X-Remote-Host: 212.58.246.82:80
X-Hanzo-Record-Id: 875a0395-c82e-46b4-a251-0f910535a344
WARC-IP-Address: 212.58.246.82
Content-Type: application/http;msgtype=response
Content-Length: 939
WARC-Block-Digest:
sha256:1c5006cbd371f39a25f3bbae6ee30c853b60
1bf9bb69579f

HTTP/1.1 301 Moved Permanently
Date: Tue, 01 Nov 2011 18:12:33 GMT
Server: Apache
Set-Cookie: BBC-
UID=44ae0be013563901a7a39e9291faeaa9f756127670a0c1ffd299c6b
4a41f72f60Mozilla%2f5%2e0%20%28Macintosh%3b%20U%3b%20Intel
%20Mac%20OS%20X%2010%5f6%5f5%3b%20de%2dde%29%20AppleWebKit
%2f534%2e15%2b%20%28KHTML%2c%20like
Location: http://www.bbc.co.uk/news/
Cache-Control: max-age=0
Expires: Tue, 01 Nov 2011 18:12:33 GMT
X-Original-Content-Length: 234
Keep-Alive: timeout=5, max=693
X-Original-Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1
Content-Length: 234

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="http://www.bbc.co.uk/
news/">here</a>.</p>
</body></html>
```

Metadata

Hash

Headers

Original Native Format Content

Acquisizione dei contenuti online

Alla luce delle **casistiche** *(pagina web, profilo sociale, mail, ecc.)*, del **contesto** *(evidenza principale o secondaria)* e della **volatilità del dato** possiamo distinguere tre modalità:

1. Acquisizione «*On-the-fly*» o «*Smart*»
2. Acquisizione «*Full*» o «*Rich*»
3. Acquisizione «*Paranoid*»

Gli elementi essenziali ed obbligatori, che rendono giuridicamente valida l'acquisizione, sono i seguenti:

Metodologia replicabile e verificabile

Relazione dettagliata delle operazioni eseguite

Firma digitale, con apposizione di una marca temporale, di tutti i contenuti digitali acquisiti

Acquisizione «On-the-fly»

È la modalità più veloce per realizzare un'acquisizione di un contenuto web e può essere attuata anche con qualsiasi browser.

Questa modalità esegue un'istantanea del contenuto web ed è consigliata solo nei casi in cui si teme che l'informazione possa essere alterata o rimossa facilmente dalla rete.

Passi:

Realizzare una copia attraverso uno dei seguenti servizi online:

- https://www.perma.cc (ISO 28500, private, esportabile) *
- https://web.archive.org (ISO 28500, pubblico) *
- https://archive.is (pubblico, non standard) *
- https://conifer.rhizome.org/ (ISO 28500, private, esportabile) **
- PageFrezeer, LegalEye, Hanzo, Cliens Prova Digitale (a pagamento) **

** Download non-interattivo* *** Download interattivo*

Acquisizione «Full»

È la modalità completa perché consente di realizzare l'acquisizione del contenuto web e può essere attuata con più livelli di dettaglio.

Liv. 1: Registrare le uscite audio/video della postazione:

Permette di realizzare un filmato a testimonianza dei comandi e dei programmi adoperati per la realizzazione dell'estrazione.

Programmi utilizzabili:

- **OBS Studio** (obsproject.com free)
- **Icecream Screen Recorder** (icecreamapps.com free/pro)
- **Apowersoft** (apowersoft.it try/pro)

Acquisizione «Full»

Liv. 2: Catturare il traffico di rete:

Consente di memorizzare il traffico di rete generato durante l'interrogazione dei contenuti di interesse.

Programmi utilizzabili per catturare il traffico di rete:

- Wireshark
- TCPDump

Occorre fare attenzione al tipo di protocolli utilizzati e alla presenza della cifratura. In quest'ultimo caso è necessario catturare le chiavi concordate tra il server e il client durante la sessione di navigazione. In presenza di chiavi di cifratura (SSL/TLS) si può attivare la variabile temporanea SSLKEYLOGFILE:

set SSLKEYLOGFILE=%USERPROFILE%\Desktop\keylogfile.txt

Acquisizione «Full»

Liv. 3: Catturare il contenuto web:

Consente di memorizzare i contenuti web di interesse.

- Se il contenuto è pubblico o non richiede l'interazione dell'utente si può utilizzare:
  - Wget (crawler open source) anche in formato *warc*
  - Browser in formato *mhtml* (IE, Chrome, Firefox, Opera, ecc.) o *warc* (Safari)

- Se la consultazione del contenuto di interesse richiede l'autenticazione o l'interazione dell'utente è necessario catturare l'intera sessione e si può utilizzare:
  - Chrome (mhtml) + plugin opzionale (Hunchly)
  - Webrecorder (app, ISO 28500)
  - OSIRT - Open Source Internet Research Tool (formato proprietario)
  - FAW - Forensics Acquisition of Websites (formato html)

Acquisizione «Paranoid»

Tutti i passi realizzati nella modalità «*Full*» sono eseguii all'interno di una macchina virtuale «pulita» e preconfigurata che diventa anche il contenitore del materiale acquisito.

- Si configura una macchina virtuale (eventualmente in cloud)
- Si installano i programmi necessari al compimento dell'attività
- Si procede all'acquisizione dei contenuti di interesse
- Dopo aver realizzato l'acquisizione, seguendo i passi citati in precedenza, si chiude la macchina virtuale
- Si appone la Firma digitale con Marca temporale alla cartella contenente la macchina virtuale
- Si redige una Relazione dettagliata dell'attività

Carving

L'acquisizione può riguardare anche informazioni cancellate o rimosse. Per tentare di effettuare il recupero di tali informazioni occorre spostare il target di acquisizione:

Google Cache

- Cliccando sulla freccia verso il basso dell'URL per visionare la SERP di Google.
- Utilizzando l'operatore "cache:", seguito dall'URL della pagina desiderata. (p.e. scrivere su Google "cache: www.repubblica.it")
- Sfruttando i plugin ad-hoc che consentono di visualizzare la cache e la storia di una determinata pagina.

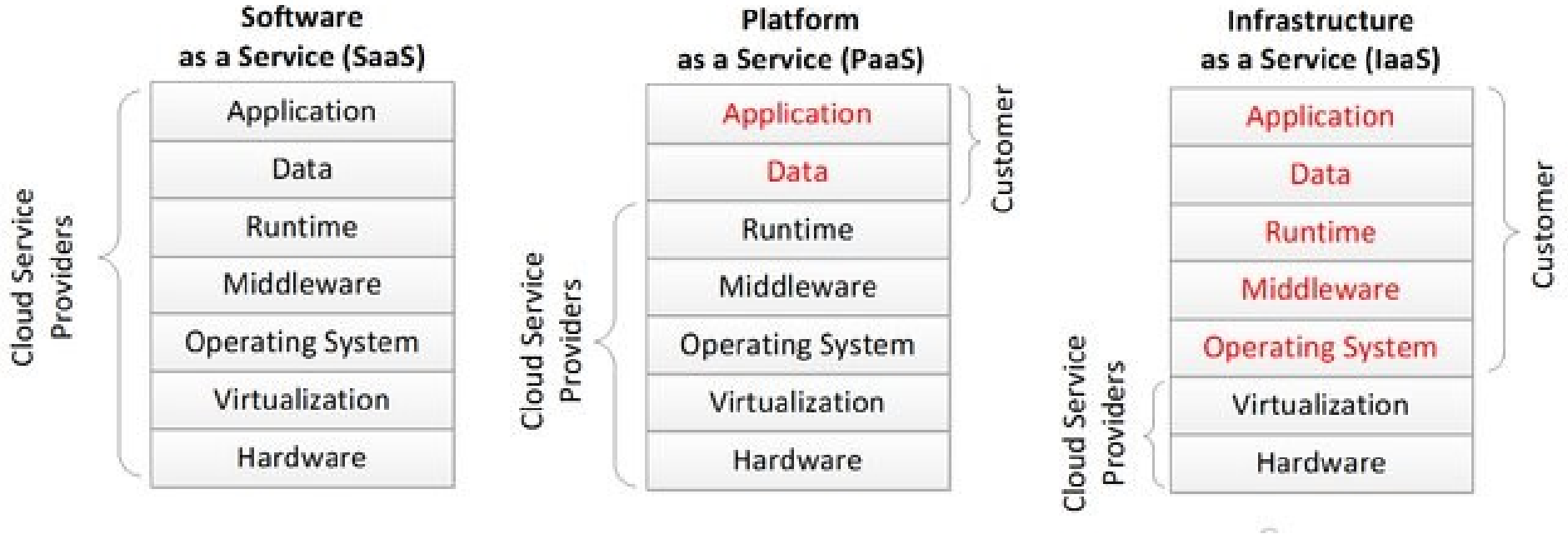
Wayback Machine

Controllando i file robot.txt o sitemap.xml

Esempio: Internet Forensics

Cloud computing forensics

Prima di acquisire le informazioni dal Cloud computing dobbiamo capire che tipologia di servizio stiamo analizzando poiché cambia l'oggetto su cui concentrare l'attività



Cloud computing: SaaS

Nell'ipotesi in cui si tratti il Cloud Service è configurato come Software as a Service (Web server, portale, ecc.) si procede come una qualsiasi acquisizione web:

- Procurarsi le credenziali di accesso all'area riservata
- Acquisire le pagine web interrogate, sia lato pubblico che privato, per visualizzare il contenuto oggetto di interesse
- Documentare, anche attraverso altra acquisizione, lo stato di configurazione e il registro degli eventi (se presente)
- Scaricare il contenuto e il backup dei dati (se disponibile)
- Se necessario, modificare la password di accesso per evitare manipolazione o cancellazioni

Cloud computing: PaaS

Nell'ipotesi in cui si tratti il Cloud Service è configurato come Platform as a Service (cloud storage, ecc.) e non abbiamo alcuna applicazione preconfigurata per accedervi direttamente dalla postazione è necessario:

- Acquisire le credenziali di accesso allo spazio virtuale
- Acquisire le pagine web interrogate per visualizzare il contenuto oggetto di interesse (sia lato pubblico che privato)
- Documentare, anche attraverso altra acquisizione, lo stato di configurazione e il registro degli eventi (se presente)
- Scaricare il contenuto o il backup (se disponibile)
- Se necessario, modificare la password di accesso per evitare manipolazione o cancellazioni

Esempio: Cloud Forensics

Cloud computing: IaaS

Nell'ipotesi in cui si tratti il Cloud Service è configurato come Infrastructure as a Service (Macchina virtuale, ecc.) e non abbiamo alcuna applicazione preconfigurata per accedervi direttamente dalla postazione è necessario:

- Acquisire le credenziali di accesso allo spazio virtuale
- Acquisire le pagine web interrogate per visualizzare l'interfaccia di amministrazione (sia lato pubblico che privato)
- Documentare, anche attraverso altra acquisizione, lo stato di configurazione e il registro degli eventi (se presente)
- Scaricare la macchina virtuale e farne una copia
- Se necessario, modificare la password di accesso per evitare manipolazione o cancellazioni

App forensics

Le app presenti su device fissi o mobile memorizzano alcuni dati sulla memoria interna ed altre sul web.

Inoltre, spesso, le informazioni visionabili consultando il sito web riconducibile alla stessa app sono diverse da quelle mostrate sul device.

Pertanto, al fine di raccogliere più informazioni possibili, è necessario effettuare più acquisizioni:

- Effettuare una copia forense del device o della cartella che contiene l'app
- Acquisire gli screenshot delle videate significative dell'app
- (se presente) acquisire le stesse informazioni sul sito web afferente l'applicazione mobile

Email forensics

Una casella di posta elettronica (ordinaria o pec) può essere consultata attraverso due modalità:

1. Portale «Webmail» (preferibile per acquisizioni di singole mail)
2. Client di posta elettronica (indicato per scaricare tutta la casella)

In entrambi casi, è necessario procurarsi gli indirizzi della casella, dei server e le credenziali di accesso.

Prima di procedere con l'acquisizione è utile conoscere i protocolli abilitati e i relativi port per l'accesso tramite client:

- Post Office Protocol version 3 (**POP3** / **POP3s**)
- Internet Message Access Protocol (**IMAP** / **IMAPs**)
- Simple Mail Transfer Protocol (**SMTP** / **SMTPs**)

Email forensics

Acquisizione tramite interfaccia web:

- Si accede con le credenziali fornite
- Si documenta la configurazione della casella, le impostazioni di ripristino, il log degli accessi (se presente) e lo stato delle cartelle visibili (Inbox, Sent, Draft, Trash, ecc.)
- Si acquisisce la pagine web che riporta l'elenco dei messaggi di interesse
- Si apre e si scarica il messaggio nel formato standard MIME RFC 5322 **(eml o msg) perché è quello che contiene anche gli header utili per l'analisi della mail**
- Se necessario, si modifica la password di accesso per bloccare l'accesso

Email forensics

Acquisizione tramite client di posta elettronica:

Dopo aver appreso:

- le credenziali di accesso (se necessario si modifica la password)
- l'indirizzo del server di posta in entrata
- i protocolli abilitati e i parametri necessari

Si configura il client di posta elettronica per trasferire tutti i messaggi presenti nella casella lasciando sul server la copia originale

Se possibile, utilizzare il protocollo IMAP perché riproduce la stessa struttura delle cartelle visibile tramite interfaccia web

L'acquisizione tramite client consente di effettuare un analisi approfondita per verificare eventuali anomalie o manomissione dei messaggi

Esempio: Email Forensics

Problematiche

- Sistemi di autenticazione / Area riservate
- Cifratura del traffico (SSL/TLS)
- Ambiente di acquisizione non verificato (*macchina condivisa*)
- Canale di comunicazione non affidabile (*connessione condivisa*)
- Caratteristiche della postazione forense (*s.o., software*)
- Localizzazione della postazione forense (*nazione o regione*)
- Lingua della postazione forense
- Versione del browser utilizzato (*user agent*)
- Contenuti dinamici (*HTML5 o AJAX*)

Mobile Forensics

Problema

I dispositivi digitali portatili (cd. Mobile device) - come il telefono cellulare, il palmare, lo smartphone, lo smartwatch, il tablet, il laptop, il lettore digitale, il riproduttore digitale, il navigatore portatile gps, ecc. - rappresentano, spesso inconsapevolmente, il diario multimediale di ognuno di noi.

Nati per consentire la comunicazione in mobilità, oggigiorno, grazie all'evoluzione tecnologica e all'avvento di un'infinità di applicazioni rivolte prevalentemente alla socializzazione e all'intrattenimento, sono diventati i contenitori di un'infinità di informazioni personali e professionali in grado di raccontare la nostra vita.

Per questo motivo gli apparati mobili sono diventati oggetto di interesse non solo dei provider di informazioni e di comunicazione, ma anche degli esperti di sicurezza informatica, che, rispondendo alle esigenze degli utenti, tentano di rendere protette e riservate le informazioni trasmesse e memorizzate, e parallelamente, su fronti opposti, dei criminali e degli investigatori, quest'ultimi a caccia di evidenze digitali per fini di giustizia.

Mobile Challenges

- Frammentazione del mercato
- Generazione di nuovi dispositivi
- Aggiornamenti continui dei sistemi operativi
- Passcode e cifratura
- Personalizzazioni utente
- Milioni di applicazioni
- Giga di dati
- Cloud
- …

Mobile Technology

DEVICE

- Telefono cellulare
- Fotocamere digitali
- Smartphone o Tablet
- Smart watch o smart band
- Dispositivi Wearable
- Lettori Mp3
- Navigatori GPS
- Sistema Infotainment
- Droni
- Smart TV
- Assistenti Vocali
- IoT

COMMUNICATION

- TACS - ETACS
- GSM – GPRS - EDGE
- UMTS – HSPA+
- LTE / LTE-A
- 5G NR
- Wi-Fi
- WiMAX
- BLUETOOTH
- NFC
- IrDA

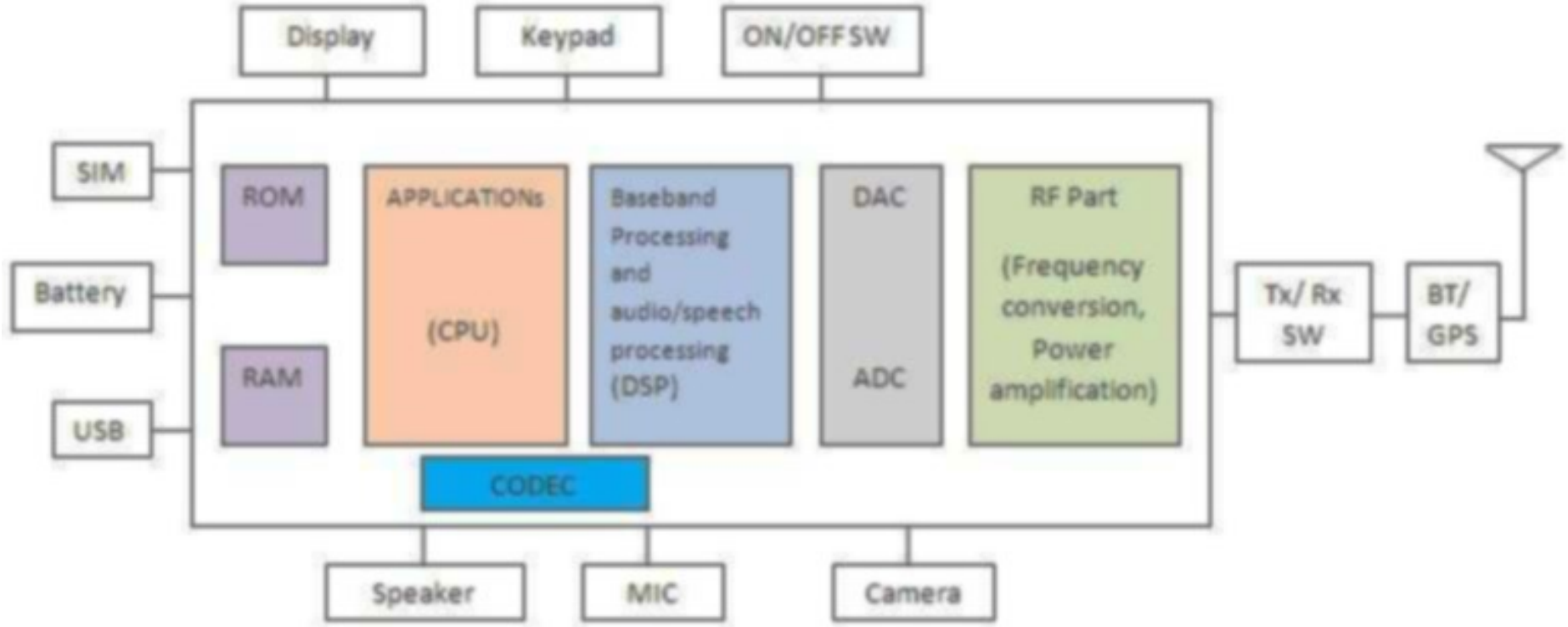
Mobile Technology - Hardware

	Basic Phone	Feauture Phone	Smartphone/Tablet
Processor	Limited Speed	Improved speed	Superior speed
Memory	Limited Capacity	Improved capacity (~5MB)	Superior capacity
Display	Grayscale	Small size color, 4k - 260k	Large size color, 16,7 million
Card Slots	None	None, MicroSD	MicroSDXC
Camera	None	Still, Video	Still, Panoramic and Video
Text Input	Numeric Keypad	Numeric Keypad QUERTY-style keyboard	Touch Screen, Handwriting Recognition, QUERTY-style keyboard
Voice Input	None	None	Voice Recognition (Dialing and Control)
Cell Interface	Voice and Limited Data	Voice and Limited Data	Voice and High Speed Data (4g e 5G)
Positioning	None	None, GPS receiver	GPS recevier
Wireless	IrDA	IrDA, Bluetooth	Bluetooth, WIFI and NFC
Battery	Fixed/Removable Rechargeable Li-Ion Polymer	Fixed/Removable Rechargeable Li-Ion Polymer	Fixed/Removable Rechargeable Li-Ion Polymer

Mobile Technology - Software

	Basic Phone	Feauture Phone	Smartphone/Tablet
OS	Proprietary	Proprietary	Android, BlackBerry OS, iOS, Symbian, WebOS and Windows Phone
PIM	Simple Phonebook	Phonebook and Calendar	Enhanced Phonebook, Calendar and Reminder List
Applications	None	MP3 Player, Notepad, Games	Applications (games, office, social media)
Call	Voice	Voice	Voice, Video
Messaging	Text Messaging	Text with Simple Embedded Images and Sounds MMS	Text Enhanced Text, Full Multimedia Messaging
Chat	None	SMS Chat	Enhanced Instant Messaging
Email	None	Via Network Operator's Service Gateway	Via POP e IMAP Server
Web	None	Via WAP Gateway	Direct HTTP

Mobile Technology

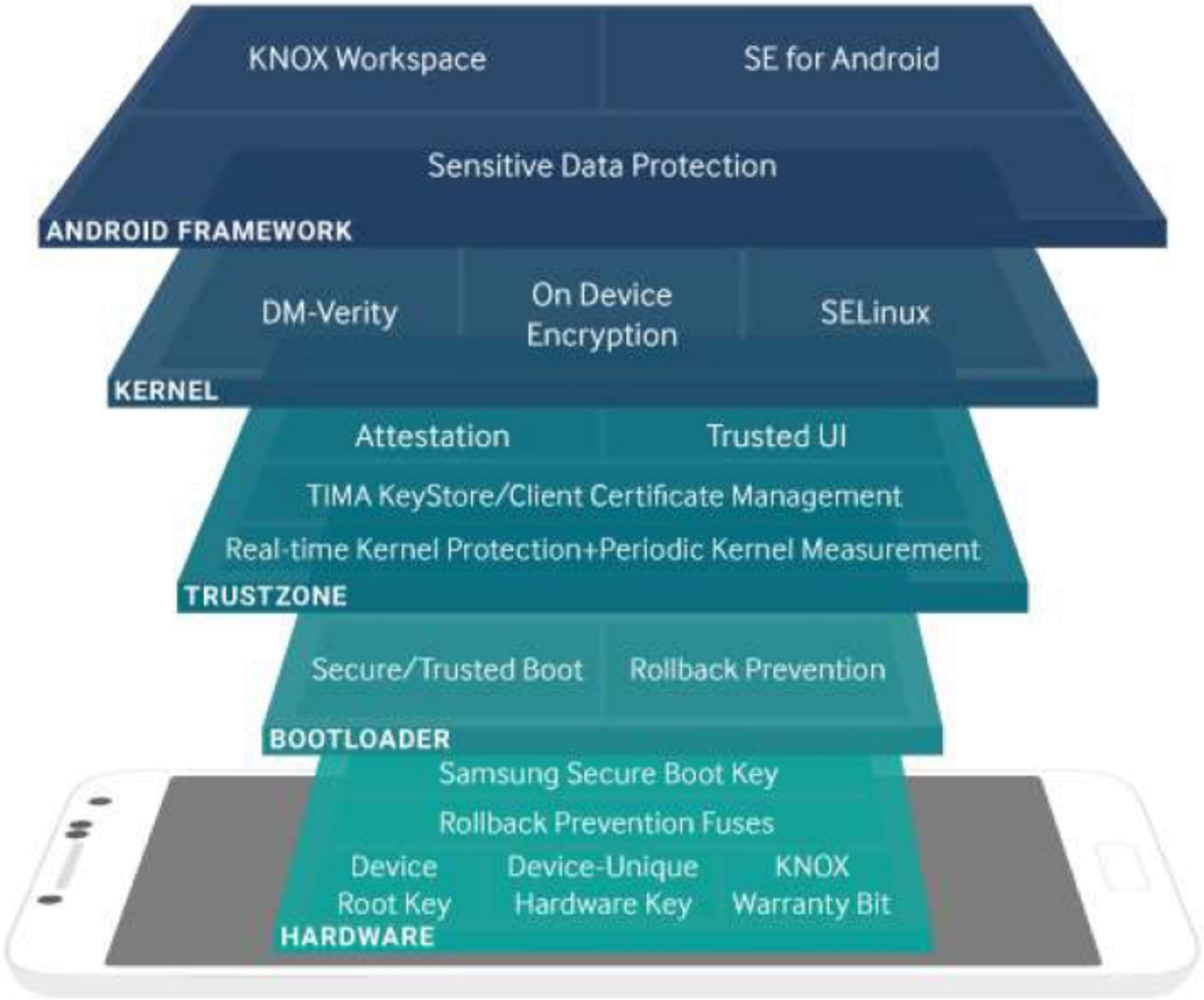


Mobile Technology

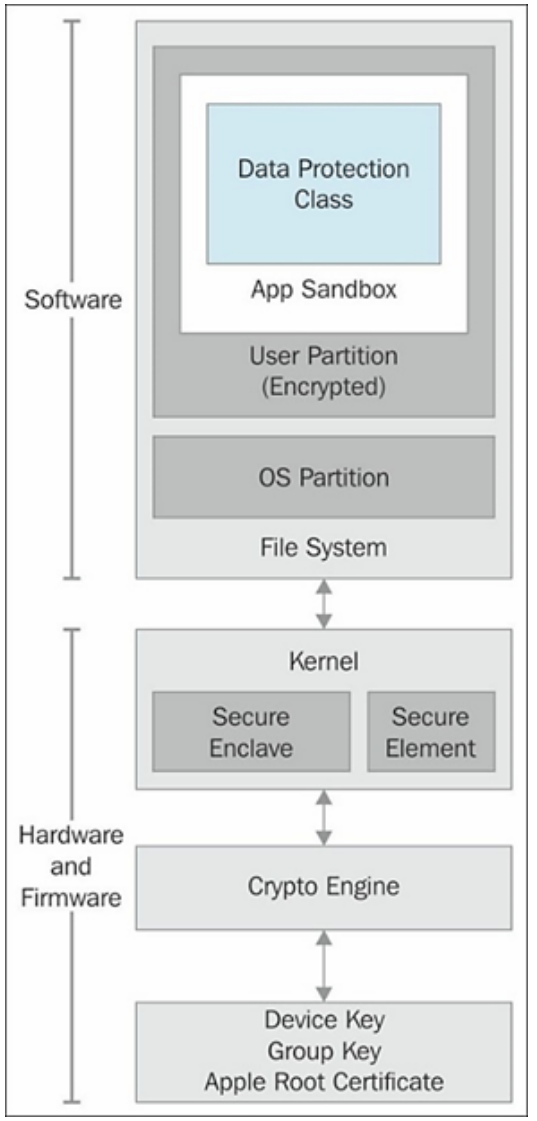
Elementi caratteristici del device mobile:

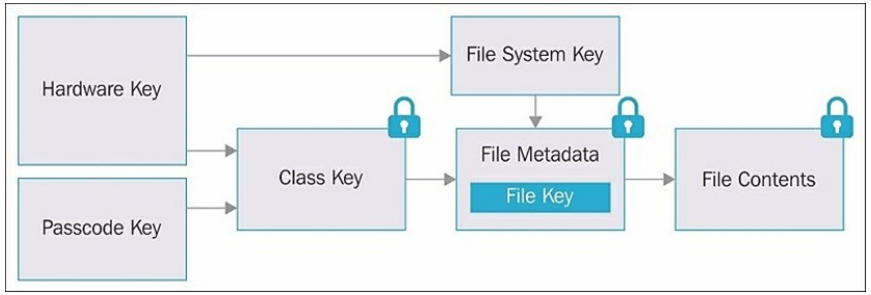
- **Firmware**
- **Sistema operativo**
- **Memoria interna per le app e i dati utente**
- **Microfono - Altoparlante**
- **Fotocamera**
- **Antenne** (GSM, UMTS, LTE, 5G, WIFI, Bluetooth, NFC, IrDA, ecc.)
- **Sensori** (GPS/Glonass, Accelerometro, Giroscopio, Magnetometro, Sensore di prossimità, Sensore di luminosità, Barometro, Lettore impronte digitali, Frequenza Cardiaca, SpO2 e VO2 Max, ecc.)
- **Touch screen**
- **SIM - Subscriber Identity Module**
- **Memoria esterna o aggiuntiva**
- **Dati sul cloud**

Samsung Knox Security Solution



Security architecture diagram of iOS





Mobile Technology

Dati che possono essere memorizzati:

- Chiamate entrata, uscita, perse
- Contatti
- Calendario
- Messaggi di testo
- Email
- Messaggi istantanei o chat
- Web pages
- Audio / Foto / Video
- Transazioni / Logs di varie Apps

Identificazione

L'identificazione delle specifiche del dispositivo è fondamentale perché ci consente di capire:

- Il modello di dispositivo (marca, modello, serial number, IMEI)
- Il sistema operativo installato di default
- Il processore e il sistema di sicurezza
- Il tipo di memoria interna
- Stato (acceso/spento, bloccato/sbloccato, integro/danneggiato, completo/incompleto)

E, di conseguenza, **scegliere la metodologia di acquisizione** migliore, ovvero quella che consente di preservare il dato originale ed estrarre più informazioni possibili.

Alcune di queste informazioni permettono di selezionare la tecnica di acquisizione che sfrutta la vulnerabilità nota per una specifica configurazione (hardware e software).

IMEI - International Mobile Equipment Identifier

I terminali radiomobili GSM sono caratterizzati da un codice di quindici cifre detto IMEI utilizzato per identificare il dispositivo all'interno della rete cellulare. Tale codice rappresenta in maniera univoca la casa costruttrice, il modello e la nazione in cui il terminale è stato prodotto.

Analysis of IMEI numbers

All mobile phones are assigned a unique 15 digit IMEI code upon production. Below you can check all known information regarding manufacturer, model type, and country of approval of a handset.

Tip! The IMEI can be displayed on most mobile handsets by dialling ***#06#**. Otherwise check the compliance plate under the battery.

Enter IMEI number below

350077-52-323751-3 analyse

Example: 350077-52-323751-3

Information on IMEI 350077523237513

Type Allocation Holder	Siemens
Mobile Equipment Type	Siemens S40
GSM Implementation Phase	2/2+
IMEI Validity Assessment	>|< Very likely

Information on range assignment

Est. Date of Range Issuance	Around Q2 2000
Reporting Body	British Approvals Board of Telecommunications (BABT
Primary Market	Europe
Legal Basis for Allocation	EU R&TTE Directive

Information on number format

Full IMEI Presentation	350077-52-323751-3
Reporting Body Identifier	35
Type Approval Code	350077
Final Assembly Code	52
Serial Number	323751
Check Digit	3

http://www.numberingplans.com
http://www.trackimei.com

Identificazione

DEVICE

IDENTIFICATION

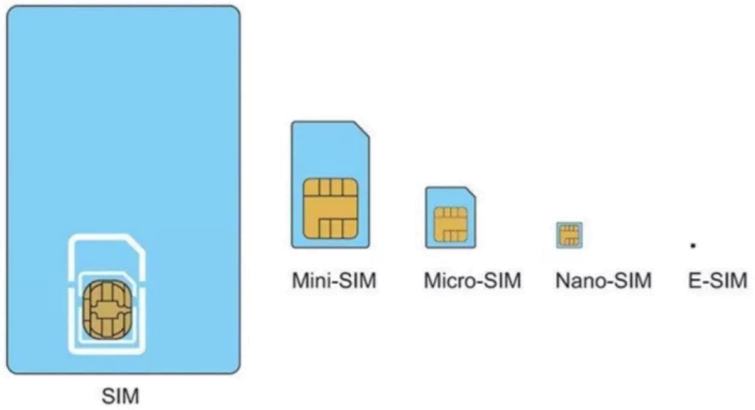
INFORMATION

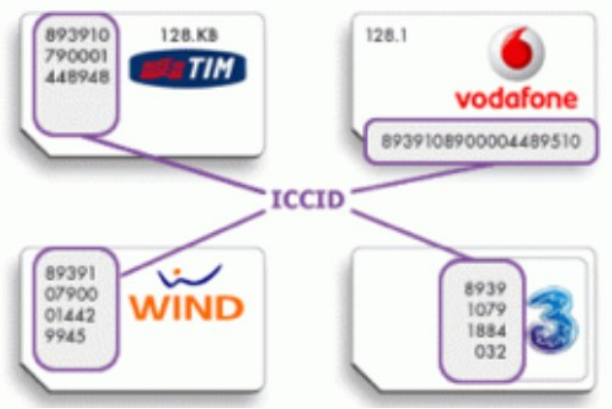
Website	URL
Firmware.mobi	https://desktop.firmware.mobi/
GSM Arena	https://www.gsmarena.com/
Hard Reset.info	https://www.hardreset.info/
IMEI.INFO	https://www.imei.info/
IMEIPRO	https://www.impeipro.info/
Numbering Plans	https://www.numberingplans.com/
PhoneDB	http://phonedb.net/
PhoneScoop	https://www.phonescoop.com/
Sammobile	https://www.sammobile.com/
The iPhone Wiki	https://www.theiphonewiki.com/

Identificazione

L'UICC (Universal Integrated Circuit Card), generalmente indicato come modulo d'identità (detto Subscriber Identity Module [SIM], Universal Subscriber Identity Module [USIM], CDMA Subscriber Identity Module [CSIM]), è un componente rimovibile contenete le informazioni relative al sottoscrittore del servizio mobile (utente).
È composto di due codici:

- ICCID (Integrated Circuit Card IDentification): Codice lungo 20 cifre stampato sulla scheda e la identifica univocamente
- IMSI (International Mobile Subscriber Identity): Codice lungo 15 cifre che identifica la coppia SIM-operatore telefonico

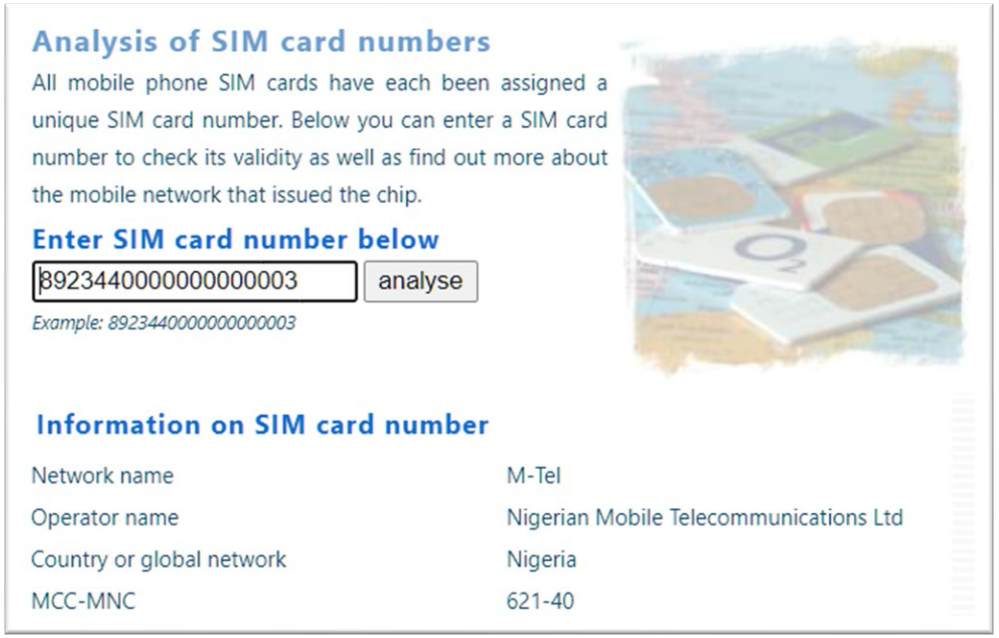


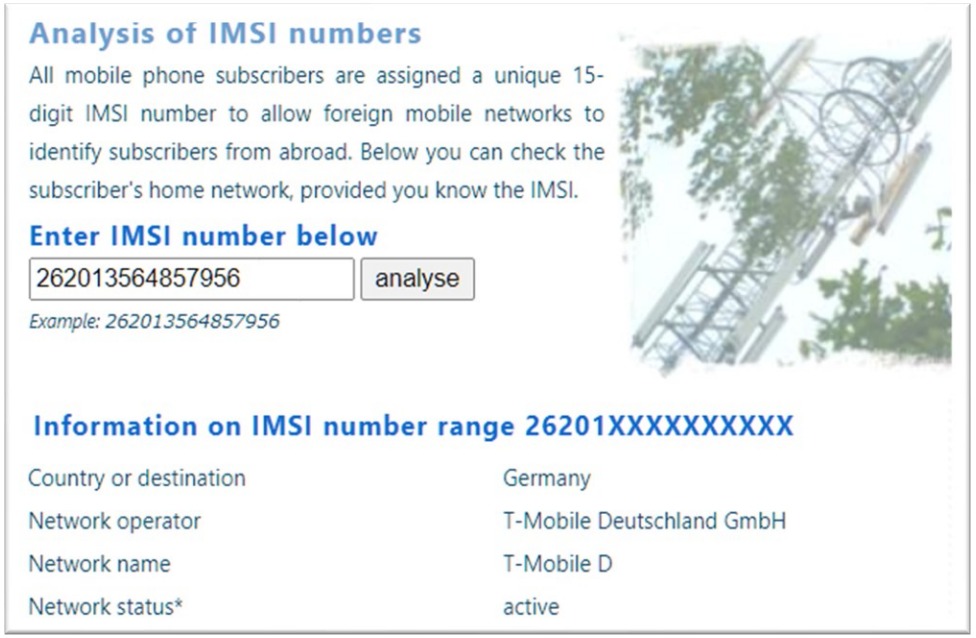


Identificazione

IDENTIFICAZIONE DELL'OPERATORE DA ICCID o IMSI:

Nel caso in cui fosse necessario identificare l'operatore di una SIM (scheda bloccata o per richiedere il codice PUK) si può utilizzare il portale www.numberingplans.com





Identificazione

IDENTIFICAZIONE DELLE MEMORIE AGGIUNTIVE:

- Può contenere diversi dati essenziali:
  - fotografie, filmati, SMS, backup, Whatsapp, etc…
- In fase di sequestro: cercare tutte le memorie compatibili con gli slot del dispositivo
- L'esame può essere effettuata in parallelo, con gli strumenti della mobile forensics, o separatamente, con gli strumenti tradizionali per digital forensics.
- Non escludere che altre copie di backup siano state trasferite su altri dispositivi di memoria (pen drive, dischi esterni, ecc.)

Identificazione

COPIE DI BACKUP

- Possono essere presenti copia di backup del dispositivo su:
  - Personal computer
  - Cloud
  - SD card
  - Altre Memorie rimovibili
- Le copie di backup possono contenere informazioni cancellate non più rinvenibili dal dispositivo,
- oppure rappresentare l'unica fonte di dati per un dispositivo non rinvenibile o non funzionante o bloccato

DATI SUL CLOUD

- Il dispositivo può non contenere tutti i dati, ma i riferimenti per potervi accedere
- Valutare la presenza di client per Cloud come Dropbox, iCloud, Google Drive, Huawei cloud, Mi Cloud, Samsung, SkyDrive, etc…
- Attenzione perché in taluni casi (es. iCloud) permette all'utilizzatore di operare da remoto sul cellulare

Repertamento

Quando ci viene consegnato un dispositivo dobbiamo assicurarci che:

- Non siano perse informazioni volatili
- Non sia compromessa la fase di acquisizione
- Non sia possibile alterare o cancellare il contenuto anche a distanza
- Non si attivino i sistemi di sicurezza che impediscono la successiva fase di acquisizione
- Sia valutata attentamente la scena del crimine

Repertamento: preservation

Abbiamo quattro scenari:

1. Acceso e sbloccato
2. Accesso e bloccato
3. Spento, con codice
4. Spento, senza codice

Se conosciamo i codici di protezione possiamo procedere, altrimenti dobbiamo fare qualcosa.

P.e. Sui dispositivi IOS è utile acquisire l'identificato UDID e cercare, su altri dispositivi, un certificato recente di lockdown (*device_UDID.plist*)

Repertamento: preservation

Se il dispositivo è spento:

- lasciarlo spento
- sequestrare anche eventuali schede di memoria e la batteria (per risparmiarsi problemi in seguito se disponibili prendere anche cavetti, caricabatteria, confezione SIM, software, etc…)
- documentare lo stato del telefono (foto)
- non lasciare la batteria all'interno o isolarla per evitare che si accenda inavvertitamente o suoni la sveglia o si possa accendere su timer

Se il dispositivo è acceso:

- mantenerlo acceso con una powerbank, ma isolato da tutto (jammer, gabbia di faraday, airplane mode)
- documentare data/ora ed eventuali info su display, valutare possibile encryption o lock
- se si dispone dei codici di sblocco spegnerlo, altrimenti ragionare!!!

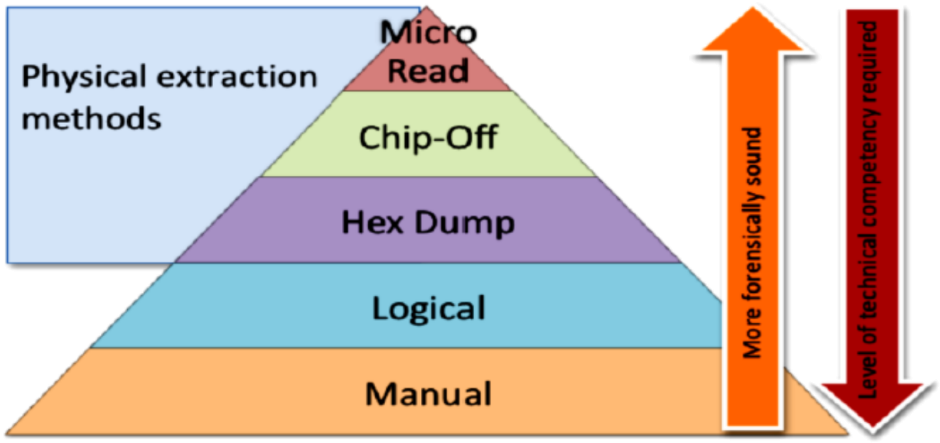


Repertamento: collection

E’ fondamentale riuscire a:

- Procurarsi i codici di sblocco del dispositivo e, se possibile, disabilitare i sistemi di protezione
- Disabilitare l’autenticazione biometrica
- Procurarsi i codici PIN e PUK della SIM
- Procurarsi eventuali credenziali di accesso al Cloud
- Se il dispositivo è collegato ad un computer, o si acquisisce che lo sia stato in passato, repertare anche il computer perché potrebbe contenere informazioni correlate al dispositivo
- Imballaggio, trasporto e conservazione sicuro

Acquisizione



L'acquisizione è il processo che consente di ottenere l'immagine o, in alternativa, le informazioni da un dispositivo mobile e dai supporti di memoria associati.

Se si esegue un'acquisizione sulla scena del crimine si ottiene il vantaggio di evitare la perdita di informazioni a causa dell'esaurimento della batteria, oppure per i danni che possono sopravvenire durante il trasporto e lo stoccaggio.

Le acquisizione on-site, a differenza di quelle effettuate in laboratorio, possono essere più complicate a causa dell'assenza di un ambiente dedicato in cui lavorare con un'attrezzatura adeguata e che soddisfa ulteriore prerequisiti.

Metodi di acquisizione

Prima di procedere all'acquisizione dobbiamo stabilire in quale scenario siamo e identificare con precisione le caratteristiche del dispositivo:

- Dispositivo acceso o spento?
- Dispositivo sbloccato o bloccato?
- Dispositivo con sistema di cifratura?
- Dispositivo di cui conosciamo le credenziali di accesso?

L'ultima domanda è importante poiché dobbiamo ricordare che, nonostante siano disponibili tecniche di hacking che ci consentono di bypassare le misure di sicurezza impostati dall'utente, dobbiamo assolutamente preservare la genuinità del dato presente all'interno della memoria del dispositivo.

Per cui, se ci trovassimo in questa situazione dobbiamo:

1. Chiedere espressamente l'autorizzazione ad usare le tecniche di hacking
2. Informare il committente delle alternative e quali rischi stiamo accettando
3. Utilizzare procedure testate e, se possibile, provarle prima su un clone

Metodi di acquisizione

MANUALE:

- Il metodo di estrazione manuale consiste nel visualizzare i dati memorizzati sul dispositivo e memorizzarla sottoforma di screenshot o filmato
- Si usa quando non è possibile acquisire i dati in altro modo
- Non è possibile rinvenire le informazioni cancellate
- È un metodo che comporta un dispendio notevole di tempo
- Durante l'interrogazione le informazioni possono essere modificate, cancellate o sovrascritte
- La lingua impostata sul device deve essere conosciuta dall'investigatore

Metodi di acquisizione

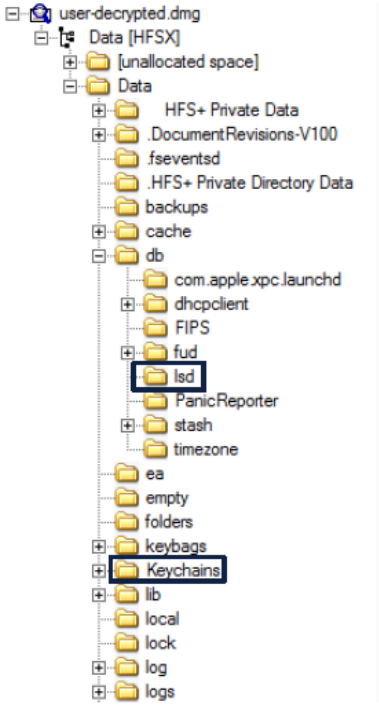
LOGICA:

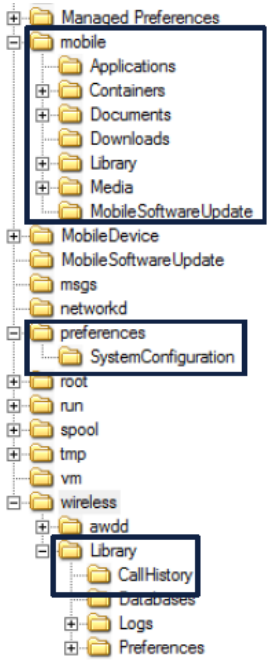
- Attraverso funzionalità del sistema operativo o tramite agent
- Estrazione dei dati visibili ed esposti dal sistema operativo
- Non recupera i files cancellati
- Non recupera i dati protetti (WA, FB, TW)
- Tipicamente è necessario avere il dispositivo sbloccato
- Si collega il dispositivo ad una postazione forense
  - Wired (USB RS-232)
  - Wireless (IrDA, Bluetooth, WiFi)

Metodi di acquisizione

FILE SYSTEM:

- È un tipo di acquisizione logica più completa
- Si può eseguire attraverso:
  - Funzionalità di backup del dispositivo
  - Vulnerabilità/funzionalità dello specifico sistema
  - Rooting/Jailbreaking (per ottenere i permessi di amministratore)
  - Flashing delle partizioni (dove non sono presenti dati utente)
- L'accesso ai dati dipende se si ottiene un **partial file system** oppure una **full file system**
- Permette di recuperare i contenuti cancellati presenti all'interno di altri file (es. record cancellati in database SQLite)
- Tipicamente necessario avere il dispositivo sbloccato, tranne in caso di specifiche vulnerabilità





Metodi di acquisizione

HEX DUMPING / JTAG:

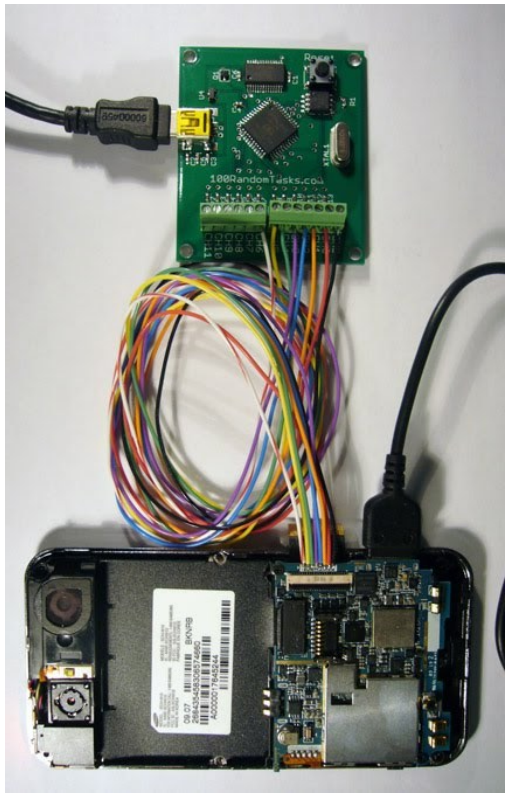
Si può eseguire attraverso:

- Vulnerabilità/funzionalità dello specifico sistema
- Rooting/Jailbreaking (per ottenere i permessi di amministratore)
- Approccio diretto sul dispositivo (JTAG/ISP/Chip-Off)
- Contro: file system cifrato

Contiene l'intera struttura di partizioni e file system del dispositivo

Permette di recuperare:

- I contenuti cancellati presenti all'interno di altri file (es. record cancellati in database SQLite)
- I files cancellati all'interno del dispositivo (carving)



Metodi di acquisizione

MICRO READ

La tecnica Micro Read consiste nell'osservazione fisica delle porte NAND e NOR del chip attraverso l'uso di un microscopio elettronico.

A causa delle difficoltà estreme che comporta lo svolgimento di una lettura Micro Read, questa tecnica di acquisizione è utilizzata solo per i casi di alto profilo equiparati ad una crisi della sicurezza nazionale e dopo che sono state escluse tutte le altre tecniche di acquisizione. Per questo tipo di intervento occorre un team di esperti, l'attrezzatura adeguata, il tempo e la conoscenza approfondita delle informazioni riservate.

Attualmente non c'è in commercio un tool per applicare questa tecnica.

Metodi di acquisizione

Una volta che è stato identificato il dispositivo occorre scegliere la metodologia più adatta.

- Verificare il supporto da parte dei tools di Mobile Forensics
- Provare per prima le metodologie meno invasive o che siano già state verificate
- Identificare metodologie alternative (*)
- Individuare specifiche vulnerabilità il cui sfruttamento non è implementato nei tools (*)
- Valutare la possibilità di approcci fisici (*)

(*) Ricordarsi che la fonte di prova deve essere preservata, quindi se occorre effettuare tentativi di exploit non vanno eseguiti sul dispositivo originale, ma su un «muletto» e prima di attuarli sul dispositivo originale occorre farsi autorizzare dal proprietario o dall'Autorità competente.

Framework di acquisizione

Open/Free:

- Android SDK
- Xda-developers.com
- Twrp
- CF-Auto-Root
- SuperSU
- Smart Phone Flash Tools
- Andriller
- AFLogical
- Autopsy
- iTunes
- SQLite Browser
- Plist Editor
- WpInternals

Commerciali:

- Cellebrite UFED4PC / Physical Analyzer
- Oxygen Forensics
- Magnet Axiom
- Elcomsoft Phone Breaker
- Elcomsoft iOS Forenics Toolkit
- Elcomsoft Cloud Explorer
- Blackbag Blacklight Mobilyze
- Scanderson SQLite Forenisic Browser
- MSBA XRY
- Mobiledit
- SPF Pro (SmartPhone Forensic System Professional)

Metodi di acquisizione

CARATTERISTICHE DI UNA SIM

Acquisizione dei dati memorizzati nella SIM

Informazioni utili da recuperare:

- ICCID
- IMSI
- Ultima cella agganciata
- Elenco chiamate
- Rubrica
- SMS (anche cancellati)

Se protetta tramite PIN sconosciuto, chiedere il PUK al Gestore

Metodi di acquisizione

CARATTERISTICHE DI UNA SD-CARD

Può essere acquisita insieme al dispositivo d'origine oppure direttamente con un software di clonazione come FTK-Imager.

All'interno è possibile recuperare dati utente quali:

- Immagini, video, audio
- App installate dall'utente
- Database delle app
- Backup

L'analisi è di norma effettuata insieme alla copia del dispositivo

Metodi di acquisizione

BACKUP - La funzionalità di backup può variare per il tipo di supporto di destinazione:

- **Backup su memorie esterne**: con questa terminologia si identificano quelle copie dei dati effettuate direttamente dal dispositivo d'origine su schede o dispositivi di memoria collegati allo stesso. Questa opzione è preferita nel caso si desideri spostare velocemente i dati da un dispositivo ad un altro;
- **Backup o sincronizzazione su PC**: con questo tipo si individuano quelle copie effettuate attraverso appositi programmi di sincronizzazione (Apple iTunes, Nokia PC Suite, Samsung Kies, Microsoft ActiveSync), presenti contemporaneamente sul terminale sorgente e su quello di destinazione, e consentono di effettuare backup o ripristino dei dati in entrambi i versi. Questa operazione è preferita nel caso in cui si desidera effettuare una copia sicura dei dati, eventualmente protetta da password, o per elaborarli in formati diversi;
- **Backup su Cloud storage**: la presenza di connettività ad Internet sempre attiva e veloce ha permesso la diffusione di quest'altro tipo di backup che consiste nel copiare o trasferire i dati dal dispositivo su uno spazio di archiviazione online. Spesso lo spazio è offerto dalla stessa casa madre del s.o. installato sul dispositivo (p.e. Apple iCloud, Google Drive, Microsoft OneDrive), l'accesso è protetto da credenziali e i dati vengono cifrati. Questa funzionalità è molto apprezzata da parte degli utenti perché, rispetto alle altre, non richiede nessun accessorio aggiuntivo ed avviene in maniera del tutto automatica.

Metodi di acquisizione

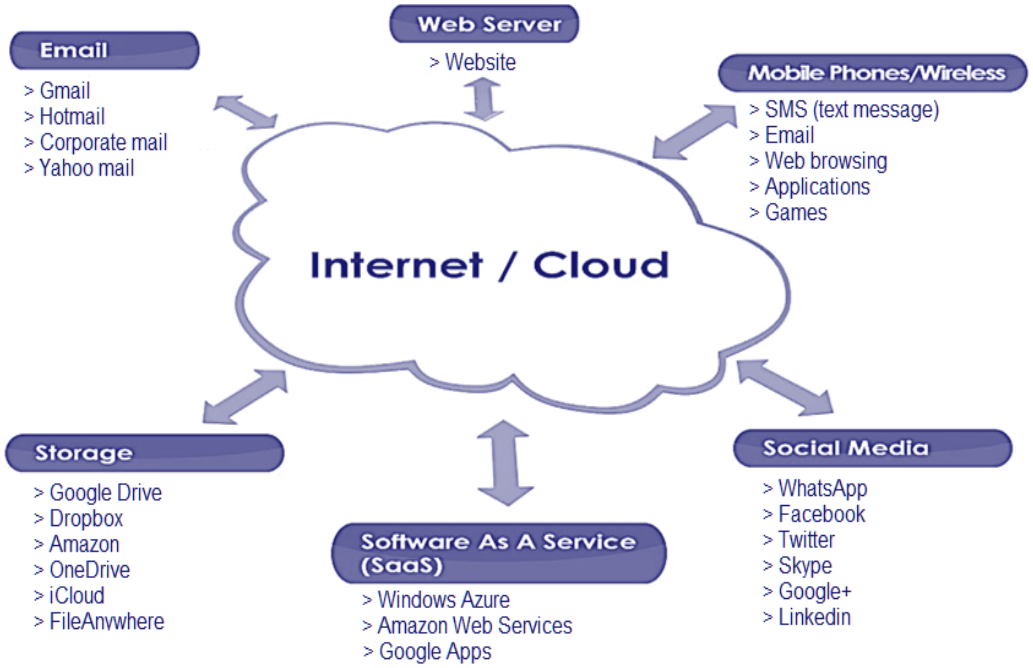
CLOUD STORAGE

I maggiori produttori di smartphone o di mobile app forniscono uno spazio di archiviazione per estendere la memoria del dispositivo o per effettuare il backup dei dati.

Accedendo a tale spazio di memoria, sia tramite il dispositivo stesso, oppure utilizzando le credenziali di autenticazione, è pertanto possibile acquisire:

- Il backup dei dati del dispositivo (produttore del dispositivo)
- Una copia di backup dei dati utente (piattaforma dell'app: Meta: Facebook, Instagram, Whatsapp, Linkedin, TikTok, ecc.)

Metodi di acquisizione



CLOUD STORAGE

L'acquisizione può essere effettuata:

- Direttamente dal dispositivo su cui sono registrate le credenziali di accesso
- Dall'interfaccia WEB del provider (Grazie, soprattutto, al GDPR)
- Tramite software di analisi forense che sfruttano le WEB API messe a disposizione del provider

Metodi di acquisizione

CAPTATORE INFORMATICO

Il captatore informatico è un malware che costituisce, per le forze di polizia e per la magistratura (???), uno strumento in grado di bypassare i sistemi di cifratura dei sistemi e delle app.

Esso viene inoculato negli smartphone e nei personal computer e, in base alle norme in vigore, può attivare il microfono per ascoltare le conversazioni, geolocalizzare lo smartphone, attivare la telecamera e scattare le foto, leggere il contenuto della memoria all'insaputa dell'indagato.

In realtà è in grado di fare moltissime altre attività (tecnicamente impossibili con altri strumenti meno invasivi) che la legge non prevede e non disciplina.

Inoltre, non viene gestito in prima persona sempre e solo da ufficiali di polizia giudiziaria ma da società private.

Rientra tra i metodi di captazione da remoto.

Esempio: Mobile Forensics

Analisi

Il processo di ricerca consente di trovare le prove digitali, comprese quelle nascoste o bloccate.

I risultati ottenuti, attraverso l'applicazione di metodi scientificamente provati, dovrebbero descrivere in maniera completa il contenuto, lo stato dei dati, la fonte ed il loro potenziale significato.

Una volta che tutti i dati sono stati estratti, si può procedere alla loro riduzione effettuando la separazione dei dati pertinenti dalle informazioni irrilevanti.

Il processo di analisi differisce dalla ricerca in quanto considera i risultati della ricerca per il loro significato ed il valore probatorio che possono assumere per il caso.

Analisi: la regola delle 6 W

LE "6" W / I DATI	WHO	WHAT	WHERE	WHEN	WHY	HOW	
Identificativi intestatario o dispositivo	■						ALL PHONE
Registri di chiamate	■			■			
Rubrica	■						
Calendario	■	■	■	■	■	■	
Messaggi	■	■	■	■	■	■	
Messaggi chat / mail	■	■	■	■	■	■	SMARTPHONE
Localizzazione spaziale			■	■			
Weburl / Contenuti web	■	■	■	■	■	■	
Immagini/Audio/Video	■	■	■	■			
Altri dati	■	■	■	■	■	■	

Analisi

Il Dipartimento di Giustizia Americano ha realizzato la **Forensic Examination of Digital Evidence – A Guide for Law Enforcement** con cui evidenzia i seguenti suggerimenti utili all'analisi dei dati estratti:

- **Proprietario e utilizzatore**: Identifica le persone che hanno creato, modificato o acceduto un file; chiarisce il dubbio di chi, tra proprietario e utilizzatore, abbia utilizzato il dispositivo in una particolare data; localizza i file di interesse in posizioni non predefinite; recupera le password che indicano utente o proprietario; identifica il contenuto dei file specifici di un utente.
- **Analisi delle applicazioni e dei file**: Identifica le informazioni rilevanti all'indagine, attraverso l'esame del contenuto dei file; correla i files alle applicazioni installate; individua le relazioni tra files (per esempio e-mail con allegati); determina il significato dei tipi di file sconosciuti; verifica le impostazioni di configurazione del sistema; analizza i metadati del file;
- **Analisi temporale**: Attraverso l'esame dei file di log e delle date e ore presenti sul file system si può determinare quando si sono verificati determinati eventi sul sistema, in modo da poter associare l'utilizzo con un determinato individuo. A tal fine possono rivelarsi utili anche i registri delle chiamate, le date e le ore contenute nei messaggi e nelle e-mail. (Questi ultimi possono essere confermati anche con i tabulati del fornitore del servizio);
- **Analisi dei dati nascosti**: Individuare e recuperare i dati nascosti può aiutare a approfondire le conoscenza, il proprietario e il movente; accedere ai file cifrati o protetti da password; accedere alla immagini trattate con la steganografia; accedere allo spazio non allocato del file system.

Analisi

I passi che solitamente si posso intraprendere sono:

- Verificare la configurazione del dispositivo e le app installate
- Interpretare i database (SQLite, Plist) di sistema, delle app native e di quelle installate dall'utente
- Rinvenire le informazioni di interesse
- Recuperare eventuali informazioni cancellate
- Ricostruire la timeline
- Connettere i contatti di più dispositivo (voice, sms, chat)
- Vedere i log delle app di interesse
- Verificare la presenza di malware

Consultare il paper: **for585.com/course**

Tools di analsi

Open/Free:

- **APOLLO** Apple Pattern of Life Lazy Output'er https://github.com/mac4n6/APOLLO
- **iLEAPP** iOS Logs, Events, And Properties Parser https://github.com/abrignoni/iLEAPP
- **iOS-Mobile-** iOS installation and uninstallation https://github.com/abrignoni/iOS-Mobile-Installation-log parser
- **iOS Triage** Incident response tool for iOS devices https://github.com/ahoog42/ios-triage
- **fplist** Converts plist files to json, https://www.hack42labs.com/tools/fplist/details/
- **iOS_sysdiagnose_** Scripts for parsing various iOS https://github.com/cheeky4n6monkey/iOS_forensic_scripts
- **ALEAPP** Android Logs Events & Protobuf Parser https://github.com/abrignoni/ALEAPP
- **Android Parser** for Android Usagestats files in https://github.com/abrignoni/Android-Usagestats-XML-Protobuf
- **ftree** Identifies, hashes and destructures all https://www.hack42labs.com/tools/ftree/details/
- **FAPK** Extracts apk files from an https://www.hack42labs.com/tools/fapk/
- **DFIR-SQL-REPO** Collection of SQL query templates https://github.com/abrignoni/DFIR-SQL-Query-Repo
- **SQLite-Deleted-** Recovers deleted entries from https://github.com/mdegrazia/SQLite-Deleted-
- **SQLECmd** Automates the identification and https://github.com/EricZimmerman/SQLECmd
- **sqlite_miner** Mines SQLite databases for BLOBs and https://github.com/threeplanetssoftware/
- **4n6-scripts** Collection of forensic and third-party scripts https://github.com/cheeky4n6monkey/4n6-scripts

Commerciali:

- Cellebrite UFED4PC / Physical Analyzer
- Oxygen Forensics
- Magnet Axiom
- Elcomsoft Phone Breaker
- Elcomsoft iOS Forenics Toolkit
- Elcomsoft Cloud Explorer
- Blackbag Blacklight Mobilyze
- Scanderson SQLite Forenisic Browser
- MSBA XRY
- Mobiledit Forensic Express
- SPF Pro (SmartPhone Forensic System Professional)

Analisi

DATI DAL CLOUD

Se siamo stati in grado di estrarre di dati dai profili social associati al dispositivo possiamo ricavare:

- Informazioni cancellate o non presenti sul dispositivo
- Informazioni provenienti da altri dispositivi associati
- Informazioni sulla localizzazione del dispositivo

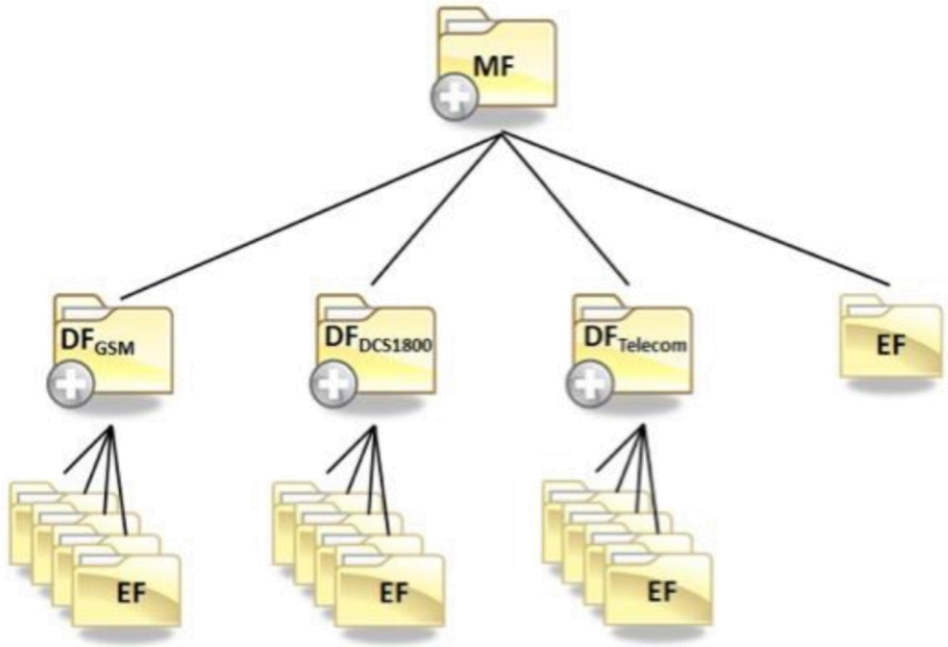
Analisi

STRUTTURA DATI DI UNA SIM

È un "File system" con una struttura ad albero n-ario

Contiene tre tipologie di strutture file

- MF – Master File
  - Composto da un header
  - E' la radice del file system della SIM card
- DF – Dedicated
  - File Composto da un header
  - una directory
- EF – Elementary File
  - Composto da header + body
  - Rappresenta il file (es. contatto, sms)



MF - Master File (root and main container of DF and EF)
DF - Directory File
EF - Elementary File

Analisi

TABULATI

Spesso l'analisi forense avente ad oggetto un dispositivo mobile si incrocia con l'analisi forense dei tabulati telefonici del gestore

Tale incrocio è utile a corroborare le informazioni contenute:

Per esempio è possibile:

- Integrare il registro delle chiamate
- Confutare la genuinità di un messaggio chat
- Migliorare la localizzazione del dispositivo
- Arricchire la timeline di utilizzo del dispositivo

Conclusioni

La maggior parte delle azioni umane sono svolte interagendo, direttamente o indirettamente, con gli strumenti dell'ICT, pertanto anche gli incidenti informatici, i reati e gli illeciti possono essere oggetto ovvero tracciati da queste tecnologie.

La digital forensics ha il duplice ruolo di:

- Analizzare in dettaglio cosa è accaduto
- Individuare le responsabilità degli autori

Si basa su metodi scientifici che assicurino: genuinità, non ripudiabilità, imputabilità, integrità, verificabilità, ripetibilità delle operazioni di analisi.