La perquisizione (e l'ispezione) informatica: tecniche, norme e modalità operative

Prof. Sebastiano Battiato

A.A. 2023/2024

Corso di Laurea in Informatica
Università di Catania
Dipartimento di Matematica e Informatica

1

La Perquisizione (Art. 247 cpp)

- è un mezzo di ricerca della prova <u>a sorpresa</u> volto al rintraccio del corpo del reato o di cose pertinenti al reato che una volta rinvenute dovranno essere sottoposte a sequestro.
- La perquisizione può essere:
  1. PERSONALE:
     - Quando vi è fondato motivo di ritenere che taluno occulti sulla persona il corpo del reato o cose pertinenti al reato.
       Sono cose pertinenti al reato quelle cose che hanno la funzione di provare il reato
     - Modalità? Dev'essere consegnata una copia del decreto all'interessato con avviso della facoltà di farsi assistere da persona di fiducia. Nel rispetto della dignità.
  2. LOCALE:
     - È disposta quando vi è fondato motivo di ritenere che il corpo del reato o cose pertinenti al reato si trovino in un determinato luogo o che in esso possa eseguirsi l'arresto dell'imputato o dell'evaso.
     - <u>Modalità</u>? Dev'essere consegnata copia del decreto all'imputato e a chi abbia disponibilità del luogo con l'avviso della facoltà di farsi rappresentare o assistere da persona di fiducia.
     - Può disporre con decreto motivato che siano perquisite anche le persone presenti quando ritiene che le stesse possano occultare il corpo del reato o cose pertinenti al reato.
- In **udienza preliminare** e **dibattimento** è disposta dal giudice
- Durante le **indagini preliminari** è ordinata dal PM
  SOLO durante le indagini preliminari, la PG può procedere di propria iniziativa ma solo in flagranza di reato o nel caso di evasione.
- Le cose rinvenute a seguito di perquisizione sono sottoposte a sequestro.
- Se si trova la persona ricercata, si dà esecuzione all'ordinanza di custodia cautelare, o ai provvedimenti di arresto fermo.

2

Perquisizione informatica

Per scoprire la prova di un illecito, la **perquisizione informatica** è un approfondimento forense che viene sempre più richiesto dall'autorità giudiziaria, per la grande quantità di dati che si possono ottenere.

Il lavoro di consulenti e polizia giudiziaria inizia **dall'isolare** i sistemi dalla rete, procedendo ad approfondire ogni aspetto.

Perquisizione informatica

La **perquisizione informatica** è sempre più utilizzata per **individuare**, **acquisire** e **preservare** le informazioni.

All'interno delle memorie dei dispositivi vengono inviati, ricevuti e immagazzinati infatti dati essenziali per la vita quotidiana e lavorativa dell'uomo, utili in caso di indagini contro il **cyber crime** ma anche per reati non informatici.

Perquisizione informatica

Come viene spesso osservato, nella maggior parte dei casi, la **prova dell'illecito** è sempre più abitualmente **annidata nel dispositivo elettronico**, anche tutte in quelle ipotesi in cui il sistema informatico non costituisce il destinatario dell'offesa né il mezzo attraverso il quale si è compiuto l'illecito.

La perquisizione nella normativa italiana

La perquisizione consiste nell'**attività di ricerca di determinati elementi** che devono essere acquisiti al fine di renderli disponibili per l'Autorità Giudiziaria.

Viene disposta **da un decreto del magistrato** e nella maggior parte dei casi viene compiuta da ufficiali di Polizia Giudiziaria delegati, spesso accompagnati da Consulenti Tecnici e Ausiliari esperti della disciplina interessata, nel nostro caso da uno o più consulenti in informatica forense.

L'atto di perquisizione personale o locale è normata dall'articolo n. 352 del Codice di Procedura Penale.

Mentre la legge n. 48 del 18 marzo 2008 rappresenta le **norme** e le **best practices** da seguire per l'acquisizione della fonte di prova, in particolare del dato informatico, sancendo l'introduzione dei principi fondanti **della digital forensics all'interno del nostro ordinamento**, prevedendo importanti aspetti legati alla gestione di quegli elementi di prova che, per loro natura, presentano caratteristiche di estrema **volatilità** e **fragilità**.

Digital Forensics

7

Seppur il legislatore si sia mosso cautamente nell'introdurre i nuovi principi per l'assunzione delle prove informatiche, non indicando cioè nel dettaglio le modalità esecutorie da applicare nell'utilizzo di tali istituti, si è comunque focalizzata l'attenzione su due basilari aspetti, sicuramente più vincolati al risultato finale che non al metodo da utilizzare, ovvero la corretta procedura di copia dei dati utili alle indagini e la **loro integrità e non alterabilità in sede di acquisizione**.

Digital Forensics

8

Gli strumenti del mestiere

Il **Consulente Informatico Forense** deve presentarsi preparato all'appuntamento, è opportuno che sia dotato di tutta l'attrezzatura necessaria ad effettuare **copie forensi ed acquisizioni in loco** di dispositivi informatici e dati online.

Strumentazione (1/2)

Un possibile Kit di strumenti sono:

- **Numerosi hard disk** di diverse dimensione utilizzati per parallelizzare le acquisizioni di copie forensi da più dispositivi e per effettuare la duplice copia dei dati;
- **Duplicatori Forensi** (come ad esempio il Logicube Falcon e il Tableau TD1, TD2u, TD3, ecc.) per effettuare copie forensi di memorie quali hard disk, pendrive USB e memorie di massa;
- **Write blocker hardware e software** per bloccare in scrittura le memorie collegate al Pc;
- **Distribuzioni Linux** su pendrive USB da avviare in locale, quali **Kali, Caine, Deft e Parrot Security** sono tra i più utilizzati;

Strumentazione (2/2)

- **Suite per acquisire dati da dispositivi mobili** come smartphone, tablet o navigatori satellitari, come ad esempio Cellebrite UFED e Oxygen Forensics;
- **Software per acquisire dati presenti su servizi cloud** di Google e iCloud ad esempio, come Cellebrite UFED Cloud Analyzer, Axiom Cloud e Elcomsoft Phone Breaker;
- **Tool per effettuare il download delle email**, Securecube Imap Downloader e Thunderbird Portable sono tra i più utilizzati;
- **Suite di software portable** per facilitare le fasi di acquisizione, come ad esempio FTK Imager Portable e Hash My Files.
- **Kit di cacciaviti, pinzette e strumentazione** varia per smontare e rimontare dispositivi.

Quando si effettua **una perquisizione in azienda**, ad esempio, molto spesso la polizia giudiziaria e i consulenti in principio si recano presso **l'abitazione dell'indagato alle prime ora dell'alba**, prima che generalmente quest'ultimo esca per andare a lavoro o per andare a fare le proprie attività.

Se sono da effettuare perquisizioni in diversi obiettivi (vari indagati, diverse località, abitazioni, aziende, proprietà e pertinenze varie), le varie squadre **dovranno sincronizzare gli accessi in modo da entrare su ciascun obiettivo contemporaneamente**.

Le operazioni necessarie

La prima operazione svolta dall'Autorità competente è l'esibizione del **Decreto di Perquisizione** che autorizza le operazioni, in quanto prima di poter perquisire viene data la possibilità di **nominare un Avvocato, un Consulente Tecnico di parte** o di farsi **assistere da una persona di fiducia**.

L'Autorità Giudiziaria può disporre che siano perquisite anche le persone presenti o sopraggiunte, quando ritiene che le stesse possano custodire o nascondere importanti fonti di prova.

Fase operativa

Espletate le formalità può cominciare la fase operativa vera e propria:

- Individuazione ed isolamento **dei sistemi informatici** (Pc, Server, smartphone, tablet, ecc);
- Individuazione ed isolamento **di account online** (e-mail, file sharing, archiviazione online, ecc);
- Richiesta di **credenziali per l'accesso, codici di blocco, PIN e password** e cambio delle stesse;
- Richiesta della presenza di **dati cifrati e relativa password di decifratura**;
- Perquisizione di tutti i locali e **sequestro del materiale di interesse** con descrizione dello stato e luogo in cui è stato rinvenuto.

Fase operativa

Una volta concluse le operazioni in abitazione queste ultime si trasferiscono in azienda.

Effettuato l'accesso ai locali vanno immediatamente isolati tutti i sistemi, **facendo allontanare eventuali collaboratori e dipendenti** dalle proprie postazioni di lavoro, al fine di quantificare il numero dei dispositivi da sequestrare o acquisire.

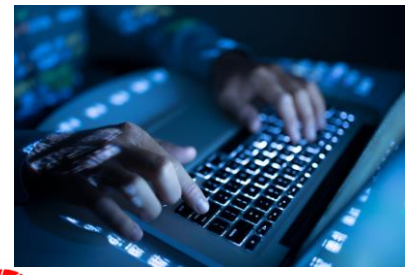
Subito va richiesta l'assistenza **di un tecnico interno**, se disponibile, per agevolare il lavoro e inquadrare immediatamente i componenti dell'infrastruttura informatica, specialmente per le aziende di grandi dimensioni. Ogni **singolo elemento va isolato dalla rete**, attivando la modalità aereo sui dispositivi mobili e sui notebook, rimuovendo i cavi di rete dai Pc fissi e dal server, ad esempio.

Fase operativa

Durante le operazioni è necessario da parte dell'indagato mantenere la calma, risultare disponibili e **collaborare con le forze dell'ordine** al fine di concludere le operazioni nel minor tempo possibile ed evitare che avvenga **il sequestro** dei supporti informatici, **la quale situazione porterebbe certamente ad un maggior disagio** per i tempi di eventuale conferimento incarico per l'effettuazione della copia forense.

Una volta effettuate le operazioni di acquisizione e doppia copia di sicurezza va compilato assieme alla P.G. il verbale, andando a dettagliare tutte **le operazioni tecniche effettuate** inserendo anche i **valori di HASH** che certificano le attività di copia forense effettuate.

Ovviamente al termine dei lavori tutti i componenti del sistema informatico, se non vengono sequestrati, vanno nuovamente resi disponibili e funzionanti, al fine di non recare danno interrompendo il processo lavorativo.



Il ruolo del Consulente Informatico Forense

Viene di seguito proposto un esempio della giornata tipo che deve affrontare un **Consulente Informatico Forense** durante un processo di perquisizione.

- Luogo di intervento, **solitamente la P.G. non comunica preventivamente l'indirizzo e il target esatto**, al fine di non compromettere l'operazione ed evitare inutili responsabilità al CT.
- Una volta riuniti tutti gli attori si cerca di fare un veloce punto della situazione, quantificando a grandi linee la mole di dati da acquisire e la tipologia di **reato per cui si sta indagando**.
- Una volta terminata la fase preparatoria si effettua l'accesso ai locali, le Forze dell'ordine mostrano il decreto e informano l'indagato delle operazioni che andranno effettuate.

Il ruolo del Consulente Informatico Forense

Inizia quindi la fase di individuazione e ricerca delle evidenze di interesse, trattasi in questo caso esemplificativo di uno **smartphone Apple** e un backup dello stesso salvato nell'area personale iCloud, un notebook **con sistema operativo Windows 10, due pendrive USB, un account di posta elettronica Gmail e dei dati presenti sul server**.

Il ruolo del Consulente Informatico Forense

Subito vanno **intercettati** ed **isolati** dalla rete i dispositivi informatici.

Per quanto riguarda lo smartphone Apple va richiesto il codice di blocco, la presenza della cifratura iTunes e le credenziali per accedere all'account iCloud, la cui password deve essere immediatamente modificata.

Vanno poi individuate le **credenziali dell'account Google**, al fine di impedire l'accesso all'area riservata.

Mediante procedura apposita si richiede il **takeout**, acquisendo oltre alle comunicazioni tutti i dati dell'universo Google, come **cronologia delle ricerche web** e **Youtube**, **dati sul Drive**, **accessi**, **posizioni**.

Sia per **l'hard disk** che per le **pendrive USB** va chiesto se i dati sono cifrati prima di acquisire l'intero contenuto della memoria **mediante duplicatore forense**, verificando quanto dichiarato.

Una volta avviato il processo va effettuata anche la **copia forense dello smartphone Apple** ed effettuato il download del **backup iCloud**.

Infine si potrà effettuare l'accesso al server. Individuati i dati di interesse che potranno essere acquisiti (**per esempio mediante il tool di acquisizione live FTK Imager Portable)**.

Effettuare la copia forense dell'intero Server sarebbe un'incredibile spreco di tempo e risorse, operazione che prolungherebbe di molto le fasi operative, pertanto è sempre buona norma ragionare e consultarsi con la P.G. operante su quanto estrapolare.

Al termine del lavoro il Consulente Informatico Forense deve assicurarsi che le varie **copie forensi** siano **integre** e **conformi** alle originali, **effettuare la doppia copia dei dati e restituire tutti i dispositivi funzionanti**.

Infine va compilato il verbale di operazioni, letto e siglato da tutti i partecipanti, concludendo quindi l'operazione di perquisizione.

Link e approfondimenti

- https://www.cybersecurity360.it/cybersecurity-nazionale/la-perquisizione-informatica-tecniche-norme-e-modalita-operative/
- https://www.bit4law.com/blog/consulenza-tecnica-perizia-informatica-forense/perquisizione-informatica-che-cosa-e-norme-strumenti/

Ispezioni (Art. 244 cpp)

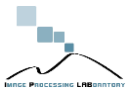
- L'ispezione è un mezzo di ricerca di prova.
- Disciplina all'art. 244 , è disposta con decreto motivato quando occorre accertare le tracce e gli altri effetti materiali del reato.
- Se necessario, può svolgersi con l'impiego di poteri coercitivi. Il PM e il giudice possono disporre l'intervento della polizia giudiziaria.
- Abbiamo due tipologie di ispezioni:
  1. ISPEZIONE PERSONALE:
     - la quale ha ad oggetto il corpo di un essere umano vivente o parti di esso.
     - Prima che si proceda, è necessario che l'interessato sia avvertito della facoltà di farsi assistere da una persona di fiducia.
     - L'ispezione dev'essere eseguita nel rispetto della dignità e del pudore.
  2. ISPEZIONE DI LUOGHI O DI COSE:
     - L'imputato e la persona che ha la disponibilità del luogo hanno diritto ad avere copia del decreto che autorizzato l'atto.
     - L'autorità giudiziaria può ordinare che taluno non si allontani.
- In **udienza preliminare** e **dibattimento** l'ispezione è disposta dal giudice
  Nella fase di **indagini preliminari** è disposta dal PM
- Il difensore dell'indagato dev'essere preavvisato almeno 24 ore prima.
  in casi di assoluta urgenza: il PM può procedere anche prima del termine fissato dandone avviso al difensore senza ritardo o anche senza darne avviso se vi è fondato motivo di ritenere che le tracce possano essere alterate.

Ispezione Informatica

- L'ispezione informatica è un mezzo di ricerca della prova, cioè una modalità con la quale il soggetto competente (la Polizia Giudiziaria, eventualmente avvalendosi di un ausiliario di Polizia Giudiziaria) ispeziona dei supporti informatici per consentire all'Autorità Giudiziaria di verificare e acquisire direttamente o indirettamente le prove in formato digitale necessarie per procedere con l'indagine.

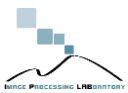
Ispezione Informatica

- Dal punto di vista normativo, l'ispezione informatica è disciplinata dall'art. 244 c.p.p. che, in maniera più ampia, regole le modalità dell'ispezione.
- Da un punto di vista operativo, **l'ispezione informatica consiste nella ricerca di prove digitali all'interno di supporti informatici**, quali ad esempio computer, tablet, smartphone ed ogni altro tipo di dispositivo digitale, utilizzando misure tecniche idonee ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.



Come si realizza un ispezione informatica?

- L'ispezione informatica può essere ordinata dal Pubblico Ministero con decreto motivato la cui copia va consegnata all'interessato solo nel caso in cui l'ispezione è relativa a luoghi o cose (ad esempio in caso di ispezione su apparecchiature informatiche). L'ispezione informatica può essere effettuata sia durante le indagini preliminari ad opera della Polizia Giudiziaria (art. 354, 2 comma c.p.p.) o del Pubblico Ministero (art. 364 c.p.p.), sia durante il dibattimento ad opera del Giudice.



Come si realizza un ispezione informatica?

- Nell'ispezione informatica, così come in tutti i tipi di ispezione, il difensore dell'indagato ha sempre e comunque il diritto di assistere e al preavviso per le ispezioni disposte dal giudice, tranne i casi di assoluta urgenza (artt. 364 e 370 c.p.p.). Al termine dell'ispezione informatica va redatto un verbale nel quale vengono descritte nel dettaglio le operazioni e le attività svolte, al cui interno devo essere presenti informazioni come:
  - dettagli dei dispositivi ispezionati: tipo (ad esempio notebook, smartphone, personal computer…), serial number, marca, modello…;
  - strumenti tecnici adottati per evitare alterazioni: ad esempio write blocker, marca, modello, versione…
  - dettagli delle operazioni svolte: ad esempio, "sono stati aperti i file immagine" oppure "sono stati cercati i file per parola chiave con la stringa fattura"…
  - esito dell'ispezione informatica: ad esempio "durante l'ispezione è emerso che…"

Modalità operative

- L'ispezione informatica può avvenire in modalità:
- **post-mortem**, cioè a sistema spento, collegando il supporto di memoria ad appositi strumenti che evitino le alterazioni, oppure
- **live**, caso che si verifica solo quando il sistema è già rinvenuto acceso all'atto dell'intervento della Polizia Giudiziaria e si opera riducendo al minimo le alterazioni che però sono inevitabili

Prof. Sebastiano Battiato
Dipartimento di Matematica e Informatica
University of Catania, Italy
www.dmi.unict.it/~battiato
battiato@dmi.unict.it

Image Processing LAB – iplab.dmi.unict.it
iCTlab - www.ictlab.srl

Digital Forensics