Peculiarità delle perquisizioni dirette alla ricerca di evidenze informatiche. La "preview”

Author : Pier Luca Toselli

Date : 10 Aprile 2019

Siamo al quarto articolo che ho voluto dedicare alle peculiarità delle perquisizioni dirette alla ricerca di evidenze informatiche, ovvero alle operazioni poste in essere immediatamente dopo quella che abbiamo definito l’individuazione del target.

Dopo l’individuazione del target iniziano i veri problemi: già, perché, dopo averlo individuato, nasce il problema di comprendere se effettivamente quel target possa rivestire o meno interesse rispetto all’oggetto della nostra perquisizione, ovvero se la sua apprensione venga legittimata dall’atto coercitivo di perquisizione e conseguente sequestro.

In riferimento a questo problema, oggi oggetto di un fervente dibattito giurisprudenziale, si parla della cosiddetta **“Preview”** che nella sua traduzione letterale viene intesa come “anteprima”; orbene, proprio la sua la traduzione letterale, in questo caso, si attaglia perfettamente al tema che vorrei trattare.

Il legislatore italiano, con il recepimento della **convenzione di Budapest** - ovvero con la **legge 48/2008** - ha voluto in qualche modo legittimare la polizia giudiziaria a effettuare un vaglio preventivo, una valutazione, circa il contenuto di un certo dispositivo digitale prima di procedere, nei confronti del medesimo:

- al suo sequestro talché, riservando poi successivamente operazioni tecniche più approfondite volte alla ricerca e individuazione di evidenze di interesse;
- all’estrazione dei soli elementi ritenuti oggetto del decreto di perquisizione informatica in esecuzione;
- a restituire alla libera disponibilità del soggetto destinatario dell’incombente il dispositivo digitale in esame, in quanto non ritenuto di interesse o comunque estraneo all’oggetto della perquisizione.

Quanto evidenziato è oggi oggetto di un fervente dibattito, tant’è che la giurisprudenza (al di là delle scelte dei titoli giornalistici, purtroppo talvolta fuorvianti) è intervenuta più volte su questo

tema [1], ovvero se sia:

- legittimo il sequestro a “prescindere” di un dispositivo, nella consapevolezza che l’evoluzione tecnologica ed un inarrestabile incremento dei volumi e delle capacità di memorizzazione dei dati rendono spesso **impossibile** un’analisi **immediata** e sul posto del dispositivo, capace di individuare quegli elementi che rientrerebbero a pieno titolo **nell’oggetto** della perquisizione;
- **di contro**, se nella consapevolezza che la perquisizione è diretta alla ricerca delle fonti di prova, risulti “illegittimo” un sequestro a prescindere del dispositivo allorquando lo stesso risulti poi non contenere **nulla** di quanto oggetto del decreto di perquisizione e conseguente sequestro;
- **e ancora…** se la copia di un dispositivo bit to bit (cd. copia forense) non comporti **“comunque”** l’apprensione di elementi estranei all’oggetto della perquisizione, ossia un classico caso di “superamento del sequestro” in letteratura meglio conosciuto come “overreaching seizure” con le conseguenti e ovvie (mi si consenta) censure giurisprudenziali.

Invero il tema appare molto più complesso e di non facile soluzione, nel continuo - e, qui, più che legittimo - bilanciamento tra esigenze investigative e d'indagine da una parte, e tutela della riservatezza e altre “libertà” costituzionalmente riconosciute, dall’altra.

Da un lato vi è una presa di coscienza circa l’impossibilità, nell’attuale contesto tecnologico, di esprimere “sul posto” e in tempi accettabili una prognosi efficace e attendibile, circa l’effettivo contenuto di un dispositivo digitale, ovvero se lo stesso possa effettivamente e consapevolmente ritenersi “estraneo” all’oggetto della perquisizione in quanto non “contenente” nulla di interessante ai fini delle indagini. Dall’altro vi è un rinnovato interesse alla tutela e riservatezza dei propri dati, tanto da “censurare” i sequestri indiscriminati, ovvero che si risolvono nel sequestrare dati del tutto estranei o irrilevanti rispetto al tema di indagine.

Forse **un esempio** può meglio aiutarmi a definire ciò che intendo, consapevole che il “confine” su cui si combatte quella battaglia è spesso alquanto sfumato e labile non essendo sempre facile, soprattutto nei contesti operativi, propendere per l’una o l’altra scelta.

Prendiamo a riferimento una semplice pen-drive da 2 GB. Facciamo una “preview”, un'anteprima del suo contenuto (come meglio vedremo nel prosieguo) e decidiamo “sul posto” se la stessa verrà a costituire oggetto del sequestro conseguente alla perquisizione, attraverso una copia bit to bit o il sequestro fisico del device, o se di contro la stessa, a seguito della “preview”, debba essere restituita alla libera disponibilità della parte in quanto non contenente alcunché di riconducibile all’oggetto del sequestro.

Sento già qualcuno che grida “ti piace vincere facile”: è vero, su una pen-drive da 2GB si gioca facile mentre su un disco da 1, 2 o più Tb le cose cambiano. Pur essendo medesimi i concetti di fondo, è innegabile come siano esponenzialmente diversi e più elevati i tempi necessari a effettuare siffatta prognosi su consistenti volumi di dati.

Ora, senza entrare nel merito di sentenze giurisprudenziali (non è nostro compito) e senza

abbandonarci a facili conclusioni (su una pen-drive da 2gb ci vuole, tutto sommato, poco tempo; su un disco da 2Tb, molto più tempo), cerchiamo di comprendere che la cd. “preview” ha comunque una certa importanza nell’ambito di ogni perquisizione informatica.

Senza di questa, ci si ritroverebbe a sequestrare **"a prescindere"** tutti i dispositivi digitali presenti sul luogo della perquisizione, con conseguenti possibili censure da parte degli organi giudiziari; ma anche a sequestrare dispositivi (una pen drive contenente “solo” film per bambini) del tutto inutili ed estranei all’*argumentum ad disputationem*, che si risolverebbero solo in un aggravio dei tempi di analisi.

Ora i più attenti mi contesteranno che: “come fai a dire che in uno di quei film non ci sia qualcosa che ti interessa e che attiene, ogni oltre tua valutazione e interpretazione, all’*argumentum ad disputationem*?” . Ottima domanda e spunto di riflessione, al quale, a onore del vero, non saprei rispondere e non saprei neanche indicare chi sarebbe in grado di farlo! Ma questo lo rimettiamo alle considerazioni che spero qualche giurista - questo è il loro compito - formulerà in un prossimo ricorso alla Suprema Corte, cercando di far comprendere come oggi di fatto sia improbo, al di là della preview e di una prognosi superficiale, rispondere al quesito. Invero, nulla toglie che qualche “smanettone” abbia inserito (l’esempio è più facile con le immagini) del testo (steganografia) all’interno di una foto e che proprio quel testo contenga la famosa frase: “sono io l’assassino!”.

Ad ogni buon conto, fermo restando che le “prognosi” sul posto oggi sono di difficile realizzazione - data l’entità dei “volumi” rinvenibili anche nei più ordinari contesti domestici - e che, se veramente volessimo escludere la presenza di files di interesse, dovremmo anche concentrarci su tutto ciò che è IOT a livello domestico (e ciò non può essere sottovalutato: allora portiamoci anche il frigo, la lavastoviglie e il forno IOT); ritorniamo alla nostra “preview” e andiamo avanti con l’auspicio che queste criticità possano essere l’oggetto di un costruttivo dibattito a più parti (FFPP, Magistratura, Dottrina, Tecnici Informatici, Digital Forensics, etc.).

La preview

Al di là di quanto sinora detto è evidente come, comunque, una preview possa risultare utile.

Oltre alle altre considerazioni che ciascun lettore potrà fare calandosi nel proprio quotidiano, richiamerei l’attenzione in particolare sulle seguenti:

- possibilità di individuare prontamente e analiticamente i files di interesse (si pensi a tutti quei casi, sempre più remoti, in cui il decreto di perquisizione si riferisce a specifici files. Il tal documento, tutti i pdf, la specifica email del…) ;
- verificare che il dispositivo, oltre ai file “allocati”, contiene centinaia di files cancellati, tra i quali potrebbero essere presenti anche files di interesse (la preview è in grado di svelare, attraverso l’utilizzo di specifici software, la presenza dei files cancellati o meglio di quei files che non risultano più allocati);
- escludere che il dispositivo contenga files di interesse: questo, come detto prima, è più difficile e talvolta improbo, ma non va escluso a prescindere, ad esempio, per volumi ridotti (la famosa pen drive da 2GB, soprattutto quando anche la ricerca di eventuali files

cancellati abbia dato esito negativo); inoltre per quanto concerne, per esempio, la steganografia, anche qui abbiamo software in grado di rilevarne, quantomeno, le tracce;
- verificare la funzionalità di un dispositivo (personalmente custodisco decine di dispositivi non funzionanti e direi che tutti ne abbiamo almeno uno, al quale siamo affezionati e conserviamo per ricordo…);

Tuttavia permangono le criticità sopra evidenziate, che consigliano comunque il ricorso a detto espediente anche al solo fine di "giustificare" il sequestro fisico dell'intero dispositivo o l'effettuazione di un suo clone anche attraverso una copia bit to bit.

Invero ritengo ancora preferibile, per le problematiche meglio specificate nell'articolo a mia firma e qui richiamato[2], procedere laddove possibile a una copia bit to bit dei dispositivi di interesse, essendo tale procedura l'unica che può assicurare, a seguito di più approfondite ricerche, di escludere che il "target" in oggetto possa contenere "evidence" d'interesse. E allo stesso tempo ritengo che l'esito della preview possa aiutare l'operatore nella **difficile decisione** di procedere al sequestro del dispositivo o al suo clone/copia sul posto.

Già nel 2012, alcuni miei "mentori"[3] (Altalex, 7 maggio 2012. Articolo di Cesare Maioli ed Elisa Sanguedolce. Con ringraziamenti ad Antonio Gammarota, Donato E. Caccavella, Michele Ferrazzano, Ulrico Bardari, Corrado Federici, Andrea Paselli), evidenziavano che:

"Ad avallare tale tesi è altresì il dato normativo che individua nel sistema informatico o telematico l'ambito di intervento ispettivo, più ampio rispetto alla disciplina della perquisizione che invece si rivolge a dati, informazioni o programmi: la ratio *della norma sembra infatti rimarcare il fine ultimo delle attività dato dall'osservazione del sistema e al più all'accertamento in ordine all'esistenza nel sistema di determinate applicazioni.* ***Il panorama si complica ulteriormente nel caso di utilizzo delle cd preview: attraverso l'utilizzo di software* ad hoc *viene permesso agli inquirenti in sede d'ispezione, ma anche di perquisizione (fattore, questo, che alimenta ulteriormente la "confusione applicativa" fra i due istituti), di poter analizzare in maniera grossolana il contenuto di un dispositivo per poi scegliere il materiale interessante e, se del caso, procedere a sequestro del dato****. Si osserva, tuttavia, come tale operazione debba essere condotta da personale altamente qualificato, stante l'alto rischio di alterazione dei contenuti con conseguente dispersione di una possibile prova e, altresì, debba essere valutata caso per caso non rappresentando ad oggi operazione di routine applicabile indiscriminatamente a qualsiasi fattispecie concreta. Si vedano le riflessioni di parte della dottrina che ne suggerisce un uso attento e calibrato a seconda dell'indagine in essere: ad esempio, se si procede per pedopornografia online, sarà rilevante il materiale detenuto con dolo (presente e non cancellato) all'interno della memoria per cui la preview potrebbe rappresentare un'opportunità utile al fine di evitare il sequestro di materiale "neutro" rispetto al reato per cui si procede; di contro, la confutazione di c.d. alibi informatici necessita l'apprensione di tutti i dati memorizzati per poter ricostruire, anche attraverso l'ausilio di macchine, le attività poste in essere dalla macchina e sulla macchina e quindi, in questa ipotesi, tale strumento appare inidoneo ai fini dell'accertamento".*

A ogni buon conto, rimettendo a ciascuno la scelta circa l'opportunità o meno di effettuazione della cd. preview, cosa a mio parere legata anche a una corretta "analisi di contesto" (ho già

espresso il concetto in altri articoli ma chi mi conosce sa che non parlo d'altro dalla mattina alla sera, atteso che, senza una corretta analisi di contesto, posso ritrovarmi - come direbbe il comico Albanese - "con tutto tutto… niente niente". Spiegherò meglio il concetto nel prossimo paragrafo) rimarco che detta operazione, al fine di rispettare i dettami imposti dalla legge 48/2008, va posta in essere da personale qualificato e non rimessa a chicchessia, potendosi attraverso detta operazione alterare, **anche,** la prova stessa (magari proprio quella che serviva!) con conseguenze spesso irreparabili. Pertanto tale operazione andrà posta in essere solo da personale esperto e qualificato e che abbia, in ogni caso, piena cognizione e consapevolezza di ciò che sta facendo.

Mi sia però permesso, in conclusione a queste considerazioni e prima di addentrarci in aspetti più pratici, evidenziare come la "preview" venga a costituire anche un necessario elemento per il superamento di eventuali "contestazioni" relative a ipotesi di "superamento del sequestro".

Se a seguito della preview vengono rilevati alcuni files di interesse (ovvero riconducibili all'oggetto del sequestro) anche solo individuati attraverso una ricerca per parola chiave, tale assunto, accompagnato dalla considerazione che "sul posto e nell'immediatezza" non è stato possibile analizzare adeguatamente l'intero volume, permette di "resistere" (al riesame) a eventuali eccezioni circa un eventuale superamento del sequestro, giustificando l'atto di sequestro o di effettuazione di clone/copia dell'intero supporto.

Medesime considerazioni posso rimandarsi al rinvenimento di numerosi files cancellati, la cui sola individuazione permette già di propendere per il sequestro del dispositivo o sua copia/clone per un successivo esame approfondito e (per esempio) *data carving* dei dati recuperabili.

Viceversa, il mero sequestro o copia/clone privo di una preview che abbia individuato una delle casistiche testé enunciate rischia, in sede di riesame, di vedere cassato il sequestro, assumendo di fatto la natura di un sequestro "indiscriminato" a prescindere non supportato da alcun elemento che lo ricolleghi all'oggetto designato.

In conclusione, potremmo quindi dire che in assenza di una "preview - positiva" o di adeguate motivazioni che giustifichino il sequestro (motivazioni che dovranno risultare nel verbale di perquisizione e sequestro all'uopo redatto) il sequestro rischia di apparire come un sequestro indiscriminato e conseguentemente passibile di censure (vedi sentenze in nota 1).

La preview: quando?

Quando non è affatto casuale, in quanto ritengo che la preview, se effettuata correttamente, cercando di apportare meno modifiche possibili allo "stato" del dispositivo e tenendone traccia (documentando le operazioni svolte), sia un'operazione che può essere svolta sia su pc spenti che accesi, oltre che su HD, Pendrive, SD etc. Mi è capitato talvolta di ricevere "osservazioni" laddove si voleva procedere alla preview di un pc spento in quanto detta attività avrebbe, a prescindere dagli strumenti utilizzati, "modificato lo stato" di quel dispositivo. Osservazione che non posso che condividere quale "principio", peraltro espresso abbastanza chiaramente nelle best practices, salvo contro-osservare che le mie esperienze si rifanno a situazioni con la presenza di decine - a volte centinaia - di pc che spesso risultano altresì "strategici" per la

sopravvivenza di attività professionali, commerciali, industriali e sanitarie.

Può accadere (sempre più spesso) che alle 6 o 7 del mattino molti di quei PC siano spenti e che scelte del tipo: “è spento, lascialo spento, mi raccomando, lo sequestriamo così com'è!” risultino ormai appartenere al nostro passato e richiedano un cambio di mentalità, laddove personale qualificato sia in grado, senza apportare modifiche “rilevanti” alle sorti dell’indagine (e questo deve trovare risposta in un’analisi di contesto del tipo: interessa il contenuto o il contenitore? Mi interessa l’integrità del sistema o i files che contiene?), di avere un’anteprima del contenuto del PC dalla quale, anche se in via del tutto presuntiva, può propendere per ritenerlo d’interesse o meno per il contesto in trattazione. Al di là delle best practices, è evidente come in determinati “contesti” sia giocoforza propendere per azioni che non potranno prescindere dall’effettuazione di una preview, viceversa si ricade nel “prendete tutto a prescindere” che si traduce però anche nel sequestrare tutto ciò che potenzialmente invia, riceve e conserva “bit”; il che, nell’era dell’ IOT, si traduce nel sottoporre a sequestro tutti i pc di un’azienda (stampanti comprese) impedendone ogni attività o, ancora, prelevare da un'abitazione tutti i dispositivi connessi (frigoriferi, allarmi, lavastoviglie, lavatrici, etc. etc.) con la conseguenza di ritrovarsi per le mani decine, se non centinaia, di dispositivi che potrebbero poi non avere alcuna rilevanza nell’indagine.

Quali strumenti e tecniche?

Ritengo che ognuno abbia i propri strumenti e tecniche per effettuare una preview; ogni mia indicazione sconterebbe di essere considerata “partigiana” e di facile contestazione, atteso che quelli che per me possono essere considerati pregi in un determinato contesto per altri possono essere difetti.

Nel premettere che non ne farò una questione tra software commerciali e open source, tratterò solo di questi ultimi (non perché disdegni gli altri!) e in termini generali.

Sono orgoglioso del “genio” italico che ha partorito diverse distribuzioni Linux specificatamente orientate alla digital forensics: alcune le sento più vicine, altre più lontane, ma tutte sono apprezzabili ed encomiabili in quanto hanno elementi di specificità che le contraddistinguono nei vari ambiti e contesti operativi.

Le più utilizzate hanno ormai comunemente adottato anche una “componente” Windows oriented che permette di operare (con tutte le implicazioni del caso) anche su sistemi Windows in modalità “Live”. Pertanto, quando citerò “distro_linux_forensics”, il riferimento è (a mero titolo di esempio) a DEFT, CAINE, TSURUGI e i loro lati Windows (ma ricomprendendovi anche le distro linux forensics quali KALI, SANTOKU, PALADIN, che non vanno certo sottovalutate).

In merito voglio evidenziare che nel tempo ho imparato a non “disdegnare" nulla e a non "affezionarmi" a nulla; e finora non posso lamentarmi. Spesso la distro preferita può avere problemi di compatibilità con il target, o la “suite di strumenti” (anche se ormai tutte tendono ad allinearsi a un certo standard) può non essere adatta al contesto di specie. Pertanto mettete nella cassetta degli attrezzi un bel po' di - anzi tutte - queste distro su CD/DVD e pen drive multi o uniboot… e buon lavoro!

Per quanto concerne le distro_linux_forensics, mi limito a ricordare che la cosiddetta “altra faccia della luna” costituita dalla parte “Windows” prevede, in diverse di queste, la possibilità di tenere traccia in un apposito file di log delle operazioni svolte, così da aiutare l’operatore nel riepilogo a verbale delle azioni poste in essere sul target.
Ripeto, solo a mero titolo di esempio – DART (DEFT) chiede all’avvio dove salvare l’apposito file che tiene traccia dei programmi utilizzati. Invero, la “tracciabilità” dei programmi utilizzati su sistemi live risulta essere di fondamentale importanza per segnalare e tenere traccia delle operazioni svolte che in tal caso possono apportare “sostanziali” modifiche al target.

Diversa la preview effettuata su di un pc spento (qualora si rendesse necessaria per i motivi già sopra meglio esplicati, ovvero su altri target quali HD portatili, Pen drive, SD, etc. per i quali si renda necessaria una preview prima del loro sequestro). In tali casi si può propendere per l’avvio della distro linux forensic sullo stesso PC target, attraverso Boot Disk, al fine di poter utilizzare la distro bypassando le richieste di password e accedendovi in modalità “read only” (sola lettura). Dette distro Forensics Oriented sono utilizzabili nell’attività di digital forensics in quanto, durante il loro utilizzo, garantiscono l’inalterabilità della struttura dei file o del sistema sottoposto ad analisi. Le stesse distro non utilizzano le partizioni di swap presenti nel sistema sottoposto ad analisi; non effettuano o creano automatismi di mount delle memorie di massa all’avvio del sistema; e **non vi sono automatismi di alcun tipo durante l’attività di analisi** delle evidenze. Il tutto è rimesso dopo il boot alle capacità e competenze dell’operatore il quale può avvalersi, per le successive operazioni, di mount e analisi di software sia GUI (Graphical User Interface) che CLI (Command Line Interface).

Il livello di eccellenza raggiunto da tali distro_linux_forensics è testimoniato dall’adozione delle stesse da parte di molti Law Enforcement nazionali ed esteri. Del resto la “suite” di programmi e funzioni di cui sono corredate ne fa dei piccoli “laboratori digital forensics” portatili, in quanto tale corredo è in grado di coprire buona parte delle esigenze di indagini digitali richieste all’operatore.

Non basterebbe un libro per descrivere nel dettaglio i programmi di cui sono corredate e, pertanto, le loro effettive potenzialità, anche se alcune risultano accompagnate da manuali che ne permettono anche al neofita un uso pressoché immediato, purché accompagnato da solide cognizioni di digital forensics (fallo solo se sai cosa stai facendo!)

Una volta ottenuto l’accesso ai dischi (in modalità read-only) si aprono (tra le tante), per l’operatore Digital Forensics, diverse opportunità, con specifico riferimento alla ricerca di di files e alla rilevazione di files nello spazio non allocato (cancellati). Tra le molte cito, sempre a mero titolo di esempio, tutt’altro che esaustivo, le seguenti GUI (perché da alcuni ritenute di più facile e immediato utilizzo) riservando agli “amanti” della riga di comando più grandi soddisfazioni e opportunità:

- la possibilità di effettuare una preview del disco attraverso programmi quali DFF (Digital Forensics Framework) o AUTOPSY FORENSIC BROWSER;
- effettuare ricerche di specifici termini, parole chiave e altro (ricerca per estensione, per esempio) attraverso programmi quali CATFISH e FINDWILD, quest’ultimo ricerca anche parole all’interno di files;

- indicizzare cartelle e volumi e poi effettuare ricerche, anche all’interno dei files, attraverso RECOLL.

Una rapida individuazione di files di potenziale interesse, unitamente all’evidenziazione - laddove presenti - di files cancellati, potrà meglio giustificare le operazioni di copia del dato che potranno spingersi, nei casi più complessi, finanche alla copia bit to bit dell’intero dispositivo qualora l’analisi di contesto ne consigli l’effettuazione; parimenti tale operazioni di preview potranno giustificare il “sequestro” del dispositivo laddove non si possa, per ragioni tecniche e di tempo, effettuarsi “sul posto” una copia bit to bit o un'analisi completa dello stesso.

Il futuro ci presenterà sempre **maggiori difficoltà**, non solo nell’individuazione del target ma anche nella gestione dei volumi (capacità di memoria) che ormai appare inarrestabile ed esponenziale. Le maggiori difficoltà consisteranno appunto nel potere, in tempi accettabili, escludere o includere i target dall’oggetto delle attenzioni degli investigatori delegati alle perquisizioni informatiche. Ci dovremo abituare a un nuovo “paradigma”, che abbandoni i canoni dell’analisi di dettaglio di ogni target e file presente sulla “crime-scene” dirigendosi verso l’individuazione dei target sulla scorta di altri elementi. Forse si rivaluteranno le scienze legate alla “profilazione” di un soggetto che, unite a quella che continuo a definire “analisi di contesto”, possano aiutare l’investigatore ad orientarsi sul giusto “bersaglio”.

Note:

[1] Vgs. principalmente le seguenti sentenze che richiamano quanto illustrato: Sez. 6 n. 53168 del 11/11/2016 Amores, Rv. 268489 – Sez. 6 n. 4857 del 14/11/2018 – 30/01/2019, Pres. Fidelbo.

[2] https://www.ictsecuritymagazine.com/articoli/bit-stream-image-dellintero-supporto-digitale-ieri-oggi-domani/.

[3] https://www.altalex.com/documents/news/2012/05/03/i-nuovi-mezzi-di-ricerca-della-prova-fra-informatica-forense-e-l-48-2008.

Articolo a cura di **Pier Luca Toselli**