Peculiarità delle perquisizioni dirette alla ricerca di evidenze informatiche. PC acceso/PC spento, cosa fare?

Author : Pier Luca Toselli

Date : 17 ottobre 2018

Siamo al secondo articolo dedicato alle peculiarità delle perquisizioni dirette alla ricerca di evidenze informatiche, che ho voluto dedicare alle operazioni immediatamente conseguenti a quella che abbiamo definito l'individuazione del target.

Per ovvie ragioni di sintesi nel prosieguo farò essenzialmente riferimento a: PC Desktop, Laptop, Notebook, Netbook ed altri supporti quali hard-disk e pen-drive e pertanto volutamente tralascerò al momento, Tablet, Smartphone e "resto del mondo" intendendo in quest'ultima categoria tutto ciò che non risulta ricompreso nelle precedenti.

Sento già i primi mormorii, che ci portano inevitabilmente alla prima delle considerazioni, ovvero che una volta individuato il target, il passaggio immediatamente successivo e necessario è quello di tentare di ricondurlo ad una delle categorie suindicate. Operazione tutt'altro che facile ed immediata quella di capire cosa si ha davanti, e che richiede non poche conoscenze tecnico-informatiche, atteso che ormai quotidianamente si rinvengono nuovi dispositivi spesso sconosciuti o ancora peggio "ibridi" che in ogni caso non solo non facilitano la loro identificazione, ma rendono anche più complessa e difficile la loro successiva gestione in termini di individuazione, acquisizione e repertamento.

Invero, quanto alla loro gestione, nei termini suindicati, uno dei fondamentali problemi da affrontare è la comprensione dello "stato" di acceso o spento in cui si trova il dispositivo in questione, attese le profonde e spesso irreversibili modifiche che il dispositivo subisce allorquando è acceso e viene spento o viceversa; ma anche gli inevitabili riverberi sul piano processuale strettamente correlati a tale "stato" quanto alla consapevolezza di trovarsi a compiere accertamenti ripetibili (ex art. 359 c.p.p.) o irripetibili (ex art. 360 c.p.p.). Lasciando ai giuristi più esperti il dibattito che ormai da tempo orbita intorno alla qualificazione di accertamenti ripetibili/irripetibili, in questo articolo mi soffermerò in particolare sugli aspetti tecnico-pratici.

Ora se stabilire se ciò che abbiamo davanti è acceso o spento, appare (sottolineo appare)

facile, per alcuni dispostivi, in altri è tutt'altro che così agevole ed immediato, cito a titolo di esempio tutti quegli stati di "stand-by" di alcuni dispositivi, non sempre accompagnati da spie luminose che ne indichino in qualche modo tale stato; o ancora quei dispositivi di nuova generazione comandati da remoto nei quali non sempre sono presenti spie luminose o altro (tasti on/off) utili a comprenderne/dedurne lo stato di acceso/spento.

È risaputo come le canoniche fasi di ACQUISIZIONE e PRESERVAZIONE che consistono in una serie di BEST PRATICES da applicarsi per assicurare i migliori risultati in termini di integrità e disponibilità dei dati digitali, sono strettamente correlate e dipendenti dallo stato di acceso o spento del dispositivo oggetto d'attenzione; tant'è che a seconda dello stato del target si è soliti distinguere tra l'esecuzione di dette fasi in *post mortem forensic o live forensic.*

Tale distinzione è tutt'ora presa a riferimento, tant'è che potremo affermare che non esiste "corso di digital forensics" e derivati che non parta da tale fondamentale assunto (strettamente collegato allo "stato" di acceso/spento del dispositivo), prima di specificare le "best pratices" da applicarsi per una corretta acquisizione e gestione del dispositivo attenzionato.

La L. 48/2008 ha di fatto sancito l'introduzione nel nostro ordinamento dei principi fondanti la digital forensics o per dirla meglio, con quel mantra: "*adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione"*[1], il legislatore nazionale ha voluto richiamare l'adozione delle "best pratices" internazionali prevedendone importanti aspetti legati alla gestione di quegli elementi di prova "digitali" che, presentano peculiari caratteristiche di volatilità, fragilità e modificabilità.

Non mi addentrerò negli aspetti prettamente giuridici che a **10 anni dall'introduzione della L. 48/2008**[2] costituiscono ancora un fertile terreno di dibattito tra le parti processuali interessate, ma mi vorrei soffermare su alcune considerazioni legate alla gestione dei dispositivi accesi/spenti che si possono rinvenire in sede di perquisizione.

Va premesso, che le considerazioni espresse nel prosieguo andranno sempre distinte e calibrate in ordine al soggetto/operatore che materialmente si troverà faccia a faccia con il dispositivo, dovendosi considerare e non sottovalutare che talune operazioni tecniche sono patrimonio e riservate a personale specializzato/qualificato che per ragioni di sintesi definirò in seguito **"esperto",** usando invece al contrario, la definizione di **"ordinario"** per indicare tutti quei soggetti, privi di particolari qualifiche/specializzazioni, ma che comunque, si trovano per svariati motivi e cause a dover affrontare un target[3], nel corso delle operazioni di polizia.

È innegabile, anche se costituisce "amara" considerazione, rilevare come oggi più che mai chi perviene a contatto con i dispositivi digitali nel corso delle operazioni di perquisizione non sia sempre personale qualificato/specializzato, ma un **"ordinario"** operatore di polizia giudiziaria. Invero, nonostante le sollecitazioni della L.48/2008 ad oltre un decennio dalla sua introduzione, ancora tanta strada resta da fare su questo piano. Il panorama "anglo-americano" che vede la presenza di diverse figure nell'ambito della digital forensics (il riferimento è ad esempio alla ISO/IEC 27037 Guidelines for identification, collection an/or acquisition and preservation of digital evidence, la quale individua differenti soggetti che intervengo nel governo e nella gestione della prova digitale e precisamente: Digital Evidence First Responder (DEFR); Digital

Evidence Specialist (DES); Incident Responder Specialist, Forensics Laboratory Manager (FLM)) fatica ancora, a prendere piede nel nostro paese, salvo recenti tentativi da parte delle FF.PP. che stanno sempre più orientandosi verso la formazione di personale specializzato/qualificato (assimilabile al DES suindicato) che verrà affiancato/coaudiuvato soprattutto nelle preliminari fasi della digital-forensic da personale assimilabile al succitato DEFR.

Cito ad esempio la Guardia di Finanza, ove nell'ultima circolare n. 1/2018 – Manuale Operativo in materia di contrasto all'evasione e alle frodi fiscali – Vol. II pag. 28, si legge che: *"In linea generale, pertanto, in tutti gli accessi nel corso dei quali si ritenga ragionevolmente di dover eseguire acquisizioni informatiche, è opportuno disporre la partecipazione di personale in possesso di adeguate cognizioni tecniche,* ***ancorché non munito di specifiche qualifiche****. Con riguardo alla formazione del personale, questo Comando Generale ha avviato iniziative volte alla definizione di specifici percorsi formativi per la preparazione dei cosiddetti* ***first responder****, cui saranno trasferite specifiche competenze proprio nella fase di acquisizione, in linea con le previsioni degli standard internazionali in materia (ISO/IEC 27037 – Guidelines for identification, collection, acquisition, and preservation of digital evidence – Annex A)."*

E' evidente come il riferimento al personale munito di specifiche qualifiche vada invece ricondotto ai cosiddetti (C.F.D.A., di cui la medesima circolare si occupa nel successivo capoverso: *"Nelle situazioni di maggiore complessità, invece, è necessario prevedere il supporto di personale qualificato* ***Computer Forensics e Data Analysis*** *(di seguito, CFDA), come, ad esempio, negli accessi rivolti a imprese appartenenti a gruppi multinazionali che potrebbero perciò impiegare sistemi di comunicazione e di memorizzazione delle informazioni condivisi al proprio interno, di talché l'estrazione informatica presso la singola entità in verifica potrebbe avere riverberi sulle altre consociate ovvero sul sistema nel suo complesso…*".

Anche in assenza di specifiche "denominazioni", tuttavia, il panorama nazionale presenta diversi ed eterogenei corsi, incontri, giornate studio etc., nel corso dei quali, ad opera di formatori interni ed esterni alle FF.PP., si cerca di sensibilizzare il personale "tutto" ad un corretto approccio verso i dispositivi digitali contenenti probabili "evidenze" informatiche, mediante l'indicazione di poche ma essenziali "best pratices".

E ciò, nell'ovvia ed inconfutabile considerazione che oggi non esiste "contesto operativo" privo di elementi "digitali" che direttamente o indirettamente risultano coinvolti nello stesso[4].

Tornando ai corsi sopra citati, si cerca da più parti con più o meno riuscite "full-immersion" di impartire ai discenti quel minimo di nozioni che gli permettano di orientarsi nel complesso, sempre in evoluzione e spesso sconosciuto mondo, della digital forensics.

Riguardando le "best pratices" ci si accorge come le stesse ricomprendano di fatto numerosi protocolli o linee guida internazionali per l'acquisizione della prova digitale. Protocolli e linee guida differenti per finalità e presupposti, ma riconosciuti internazionalmente come validi, ovvero, per dirla in sintesi, capaci di salvaguardare quegli aspetti fondamentali e vincolanti della "digital evidence" costituiti da integrità ed immodificabilità del dato acquisito.

Tali best pratices risultano ad oggi, elaborate essenzialmente da[5]:

- Agenzie Governative (DoD, USS, A.C.P.O, FBI, etc) finalizzati a coniugare aspetti tecnici a quelli procedurali/processuali;

- Elaborati a scopi commerciali: sono prevalentemente orientati all'incident response aziendale;

- Organizzazioni/agenzie nazionali o internazionali di standardizzazione (ISO 27037, RFC 3227, NIST), estremamente tecnici senza diretti rimandi al panorama giurisdizionale;

- Associazioni di "categoria" (ONIF Osservatorio Nazionale Informatica Forense[6], IISFA International Information System Computer association, DFA Digital Forensics Association, IACIS International Association of Computer Specialists , etc.).

Ma torniamo al tema di questo articolo! Chi ha partecipato a corsi, convegni, incontri, dibattiti in materia di digital forensics avrà sentito almeno una volta un altro "mantra"…: " se il PC è spento lo lasci spento se il PC è acceso lo spegni", alla fine non è un ordine perentorio (vedremo poi il perché!), ma una sorta di formula di sintesi consolidatesi a parere di chi scrive, essenzialmente per questi motivi:

- Come ho già avuto modo di evidenziare la legge 48/2008, ha sollecitato ed indotto le FF.PP. a seguito della sua introduzione, ad allargare la platea del personale dotato di "sufficienti" conoscenze in materia di digital forensics, affinché come previsto dal vigente codice di procedura penale un sempre maggior numero di Ufficiali di polizia giudiziaria fosse in grado di effettuare una perquisizione informatica. Di qui la necessità, di pervenire all'effettuazione di corsi di istruzione, brevi, concisi e "only once in life" (non è detto che sia la soluzione giusta… anzi!) capaci di fornire un minimo di nozioni in prevalenza pratiche, capaci di essere apprese da chiunque ma soprattutto efficaci nel rispettare le prescrizioni imposte dal legislatore in materia. Appare evidente allora, come l'indicazione: "se il PC è spento lo lasci spento se il PC è acceso lo spegni" sia probabilmente quella che arreca "meno danni" nella generalità dei contesti operativi, ma soprattutto sia quella che può essere adottata da **chiunque** (intendo personale non specializzato/qualificato – digital forensics), atteso che fatte salve le difficoltà di individuazione circa il reale stato del dispositivo, il resto si risolve nella mera apprensione e repertamento del target (quando spento) o nello spegnimento dello stesso, attraverso diverse tecniche ancora oggetto di considerazione e dibattito tra i più esperti, che vanno dallo spegnimento ordinario (attraverso il tasto START di Windows per capirci), a metodi più "hard" quali il distacco dell'alimentazione elettrica dalla presa a muro o da dietro il "case".. ..nei notebook e netbook ove possibile (sempre meno) ricordo anche di staccare la batteria![7] O ancora a metodi già più complessi per l'operatore ordinario in quanto richiedono l'apertura di una consolle e la digitazione di una stringa per esempio : # shutdown -h now .
- Può risolversi in una situazione di "comodo" trovo il dispositivo spento, lo sequestro senza se e senza ma, lo trovo acceso lo spengo e lo sequestro lo stesso, ritrovandomi nel caso precedente. Tale assunto costituisce un fertile terreno di dibattito anche giurisprudenziale tra esigenze contrapposte di adeguatezza e proporzionalità da un lato,

ed investigative e di prova informatica, dall'altro. Da un lato anche da ultimo la giurisprudenza con sentenza n.25527/2017[8], ha ribadito che non è censurabile sotto il profilo dell'adeguatezza e proporzionalità, il sequestro dell'intero PC con successiva estrazione della cosiddetta copia "bit a bit", essendo l'attività di analisi per la selezione dei documenti contabili particolarmente complessa, ed investendo nel caso di specie l'intera attività "imprenditoriale dell'indagato"; aggiungendo a ciò, che le operazioni di estrazioni di copia dei documenti "rilevanti" a tal fine non avrebbero potuto essere condotte in loco in un limitato arco temporale, in quanto la selezione avrebbe comportato una significativa attività di studio e analisi. Dall'altro lato sempre la giurisprudenza[9] tende a valutare il cd. Sequestro indiscriminato superfluo se non illegittimo allorquando viola il principio di proporzionalità ed adeguatezza. Per chi volesse approfondire quest'ultimo aspetto mi permetto di segnalare, anche, altro mio articolo su questa rivista, nel quale propongo analoghe riflessioni[10].
- Il personale "ordinario" spesso non è in grado di effettuare operazioni che vanno al di là del mero spegnimento e repertamento del dispositivo accesso e repertamento del dispositivo spento, non avendo alcuna cognizione circa l'ordine di volatilità del dato e purtroppo … non avendo neppure a disposizione il più delle volte l'hardware ed il software necessari all'effettuazione delle operazioni necessarie a preservarne lo stato in cui è stato trovato il reperto acceso. Neppure, detto personale "ordinario" si sente adeguatamente responsabilizzato o meglio non è adeguatamente formato ed informato sulle proprie responsabilità, preferendo nel dubbio delegare qualsivoglia operazione a personale "esperto" che però purtroppo ad oggi risulta ancora in numero inadeguato rispetto le concrete necessità operative.

Ne consegue che il mantra "se il PC è spento lo lasci spento se il PC è acceso lo spegni" può apparire una soluzione adatta alla maggior parte dei contesti operativi e che vedono la presenza di personale "ordinario" addetto alle operazioni di perquisizione.

Le cose, tuttavia, appaiono diametralmente opposte allorquando nel medesimo contesto venga invece a trovarsi personale "esperto". In tal caso le operazioni potranno a seconda dello scenario distinguersi nelle canoniche "live" o "post mortem" forensics. Invero tale differenziazione prenderà spunto proprio dalla condizione di acceso/spento in cui verrà rinvenuto il target. Differente sarà quindi l'approccio che il personale esperto dovrà avere a seconda che il target sia rinvenuto in modalità acceso o spento.

Potremo vedere a mero titolo esemplificativo e pratico una situazione operativa nella quale vengono rinvenuti due PC uno acceso e uno spento.

Riguardo a quello spento verrà rimessa al personale esperto, eventualmente, l'opportunità di procedere attraverso l'utilizzo delle cd. "Live_Linux_Forensics" (es. DEFT, CAINE, PALLADIN, etc.) all'effettuazione di una "preview" volta ad apprenderne il contenuto. Tale operazione svolta in modalità RO (read-only) non andrà ad alterare in alcun modo i dati e permetterà al personale di perquisirne, il contenuto. In merito a tale operazione che in determinati contesti operativi e nel rispetto del decreto di perquisizione, deve trovare, ove possibile, applicazione, rimando per gli approfondimenti a quanto da me già evidenziato nell'articolo in nota 8 che precede. Ad ogni buon conto, e rimessa ogni migliore valutazione, ai responsabili

dell'operazione, dopo la preview svolta sul pc spento si deciderà se procedere al sequestro dell'HD, di una partizione dello stesso o dell'intero PC (ricordo il problema spesso sottovalutato della confisca – 240 C.P.); ovvero ritenere lo stesso PC non interessante o comunque non rientrante nell'oggetto del decreto. Occorre da ultimo evidenziare come in tale ipotesi, il rischio di alterabilità dei dati presenti è più basso sempreché vengano adottate le cautele previste dalle *best practices (*a titolo di esempio accesso alle memorie in modalità RO (read only)*.*

Di tutt'altra complessità è invece la gestione del PC rinvenuto acceso, al di là delle già complesse modalità di spegnimento che dovranno adottarsi. Nel caso di un dispositivo acceso e collegato alla rete è evidente come il disposto previsto dall'art. 247, comma 1-*bis* del codice di procedura penale assuma particolare discriminante, importanza ed attenzione, atteso l'alto tasso di modificabilità del sistema a cagione della sua continua, silente e non sempre palese dinamicità. Ecco che allora perquisire un sistema attivo diventa anche per l'"esperto" un'attività molto rischiosa in termini di genuinità, inalterabilità ed immodificabilità dei dati rinvenuti al momento dell'atto, nonché in termini di garanzie difensive da riconoscersi alla controparte.

Inoltre, e qui preme sottolineare ed evidenziare come quel mantra "se è acceso lo spegni", non è detto che risulti essere la soluzione migliore ed ottimale… anzi!

Mi limito qui ad accennare che per eseguire una **perizia informatica**[11] lo spegnimento del PC comporta la perdita di tutta una serie di dati ed informazioni contenute nella RAM, purtroppo spesso sottovalutate, ma che poi si rilevano di importanza fondamentale ad esempio: processi in esecuzione, volumi crittografati "aperti" (Truecrypt, Veracrypt, BitLocker etc.) connessioni attive, chat aperte, moduli caricati ed in utilizzo, ed aggiungerei una serie infinita di informazioni anche risalenti nel tempo che potrebbero comunque essere di interesse per il caso in trattazione. Non si esclude poi che il PC rinvenuto acceso costituisca in quel preciso momento uno stato di "flagranza di reato" che richiede un tempestivo ed immediato congelamento di determinati dati, costituenti prova del reato, che a seguito dello spegnimento dello stesso potrebbero andare persi (volumi criptati, connessioni on banking, etc).

Ancora una volta si richiede allora una sinergia tra personale esperto e responsabili delle attività finalizzata ad una accurata e precisa "analisi di contesto".

Potrebbe invero rendersi necessario "un congelamento" dello stato della RAM del PC in esecuzione in tutti quei casi in cui uno degli elementi volatili sopra citati costituisse elemento necessario e strategico per l'indagine. Tale operazione tecnicamente di "dump" della RAM non è certo scevra di controindicazioni atteso che per procedervi sarà giocoforza necessario avviare specifici tool che in modo più o meno incisivo e diretto andranno comunque ad alterare lo stato preesistente anche della RAM. Di qui si comprende come l'analisi di contesto divenga allora imprescindibile costituendo l'ago della bilancia che andrà ad indicare all'esperto se procedere ad un mero spegnimento in tutti quei casi in cui il contenuto della RAM e le altre connessioni attive non assumono alcuna rilevanza ovvero procedere consapevolmente ad un "dump" della stessa, prima di procedere allo spegnimento del sistema. Ovviamente, analoga considerazione andrà effettuata in ordine agli eventuali volumi "decriptati" e a quelli di rete collegati in quel

momento, nella considerazione che lo spegnimento del PC comporterà la perdita di detti collegamenti e della possibilità di accedere ai volumi criptati in assenza delle password/credenziali[12].

In assenza di personale esperto e dei necessari strumenti si potrà comunque procedere con metodi “alternativi” a cristalizzare in qualche modo “lo stato delle cose” video e foto sono ormai strumenti nelle mani di tutti (avete uno smartphone?), pertanto si potrà procedere anche con tali strumenti a documentare (il termine qui è giuridico) lo stato delle cose.

In conclusione l’analisi di contesto assurge ancora ad elemento strategico e fondamentale per la buona riuscita di qualsiasi operazione. Ancora una volta occorre fermarsi a riflettere, senza farsi prendere troppo la mano da indicazioni ed istruzioni che possono risultare corrette per la maggior parte dei casi ma non per tutti! Occorrerà quindi di volta in volta calarsi nel “caso” concreto e svolgere un’attenta valutazione, circa l’opportunità di procedere o meno allo spegnimento di un PC ovvero procedervi dopo aver posto in atto una serie di operazioni che quant’anche “prima facie” contrarie al dettato dell’art. 247 bis cpp possono poi invece risultare necessarie e strategiche.

Di qui il consiglio a ponderare sempre con attenzione le indicazioni fornite dalle best pratices che non a caso all’attento lettore appaiono spesso generiche e mai imperative lasciando a ragione, all’operatore un certo margine di discrezionalità circa il metodo da adottare.

Se i manuali e le indicazioni di massima assurgono a corretta indicazione per la generalità dei casi, occorre sempre valutare con attenzione il caso concreto, calandosi di volta in volta in un analisi di contesto che sappia adeguatamente valorizzare, valutare e ponderare ogni decisione intrapresa.

Troppo spesso la pedissequa applicazione delle indicazioni di massima (se acceso lo spegni, se spento lo lasci spento) non aiutano l’operatore a valutare attentamente gli effetti delle proprie azioni, purtroppo con effetti irreversibili sul piano investigativo.

Si auspica allora da parte di tutti i soggetti interessati un rinnovato interesse volto magari ad abbandonare certe definizioni asseritamente assolute e ad abbracciare invece un nuovo metodo di affrontare i variegati contesti con ferma e piena coscienza delle azioni che si intraprendono.

Pertanto e veramente in conclusione … da oggi prima di spegnere il PC … pensateci, “esperti” od “ordinari”, … pensateci!

Note

- [1] Cfr. artt. 244, 247 e 352 c.p.p.
- [2] https://www.csigbologna.it/referenze/giurisprudenza/la-legge-48-2008-a-dieci-anni-dalla-pubblicazione/
- [3] Per un approfondimento su tali aspetti rimando il lettore ad altro mio articolo:

https://www.ictsecuritymagazine.com/articoli/legge-18-marzo-2008-n-48-lufficiale-polizia-giudiziaria-dieci-anni/

- [4] Anche quando non costituiscono elementi di prova, corpo del reato etc. , sempre più spesso gli elementi digitali risultano strategici nel fornire numerose informazioni utili al prosieguo delle indagini o altre informazioni indiziarie che pur non costituendo una prova vengono comunque considerate in sede dibattimentale dall'organo giudicante.
- [5] Ringrazio per questo elenco di sintesi e l'approfondimento sul tema "best pratices" l'eccellente articolo di Maurizio Tonellotto - http://www.vittimologia.it/rivista/articolo_tonellotto_2014-02.pdf
- [6] www.onif.it
- [7] Il dibattito su come spengere il pc è tutt'altro che sopito tra gli esperti. I motivi si attestano sostanzialmente tra una posizione prudente volta alla tutela dell'hardware e software del PC (per capirci … non è sempre buona cosa interrompere bruscamente l'alimentazione ad un pc), tanto da consigliare sempre lo spegnimento attraverso le procedure "ordinarie"; che si scontra con altra prudenzialmente volta ad impedire che attraverso lo spegnimento "canonico"/ "ordinario" si possano attivare procedure di "erase" (cancellazione sicura dei dati) dei dati con ovvie irreparabili conseguenze sul piano della successiva acquisizione "probatoria"; tra i due estremi compaiono poi diverse tecniche "intermedie" che cercano di mediare le criticità dell'una e dell'altra. Esistono diverse tecniche di spegnimento che non utilizzano le procedure indicate dal S.O. (attraverso START) solo a titolo di esempio alcune combinazioni di tasti o l'utilizzo di comandi da terminale/shell che impediscono di cadere nella trappola del tasto START.
- [8] Sez. V n.25527 del 27/10/2016 dep. 2017 Storari
- [9] Sez. VI n. 24617 del 24702/2015.
- [10] https://www.ictsecuritymagazine.com/articoli/bit-stream-image-dellintero-supporto-digitale-ieri-oggi-domani/
- [11] https://www.bit4law.com/servizi-offerti/perizia-informatica/
- [12] In tal caso si renderà necessario procedere con riferimento ad eventuali volumi criptati "aperti" alla loro copia attraverso tool specifici atteso che al seguito dello spegnimento ed in assenza delle password/credenziali necessarie alla loro "riapertura" sarà molto difficoltoso, se non impossibile procedervi successivamente.

Articolo a cura di **Pier Luca Toselli**