L’Ufficiale di P.G. 4.0: quali strumenti per le operazioni più comuni che coinvolgono dati digitali?

Author : Pier Luca Toselli

Date : 15 Giugno 2020

Da alcuni anni ho il privilegio di scrivere su questa rivista e durante l’emergenza COVID, che ci ha costretto a modificare diverse nostre abitudini, ho riletto i miei articoli pubblicati dal 2017 al mese di febbraio u.s.[1]. Tra questi mi hanno sollecitato nuove riflessioni e considerazioni - guarda caso - il primo e l’ultimo.

Nel primo del 2017[2] concludevo così: ”*...auspico che il raggiunto traguardo dei dieci anni della Legge 18 marzo 2008, n. 48, non sopisca gli animi degli addetti ai lavori, ma anzi, serva come rinnovato impegno a continuare nella formazione di personale tra le forze di polizia. La speranza è quella di poter vedere uscire dalle scuole di formazione di polizia un “ufficiale di polizia giudiziaria 4.0”, pronto e preparato ad affrontare le sfide future di un inarrestabile e velocissimo progresso tecnologico che vedrà sempre di più presenti sulla scena del crimine dispositivi digitali prova dei delitti o elementi utili al prosieguo delle indagini e all’accertamento dei fatti".*

Mentre nell’ultimo del 2020[3] concludevo considerando che: “*le FF.PP. devono essere adeguatamente “formate” a ogni livello per saper affrontare “i nuovi spazi” del crimine. È impensabile non dotare chi si trova in prima linea (come gli uffici denunce) degli strumenti culturali (corsi) e tecnologici (hardware e software) che possano aiutarli a ricevere, in modo adeguato ed efficace, una denuncia per fatti criminosi commessi attraverso una chat”.*

Se sarebbe ingeneroso non evidenziare i lodevoli **sforzi compiuti dalle FF.PP** a soluzione delle problematiche sopra tratteggiate, e i passi finora brillantemente compiuti, il tema della formazione e della dotazione di strumenti adeguati ad affrontare le nuove “frontiere” del crimine è tema “caldo” e sempre più all’attenzione[4] nell’evidenza - ormai innegabile, come ho ribadito più volte che al di là delle classificazioni dottrinali tra crimini informatici e no - che oggi sia sempre più raro, se non impossibile, sviluppare indagini in contesti avulsi dal “digitale”; per dirla più brevemente, oggi potremo dire che non esiste “caso” che non veda per la sua soluzione, prova o documentazione la necessità di dover “trattare” dati digitali.

Con trattare mi riferisco genericamente a tutte quelle *best practices*, ormai internazionalmente riconosciute, che permettono alla **prova digitale** di essere considerata genuina, autentica e

affidabile fin da quella fase embrionale del procedimento, rappresentata dalla denuncia di un fatto di reato che le FF.PP. sono obbligate a ricevere. Ho già avuto modo più volte di segnalare esempi concreti e casi specifici, che evidenziavano come le “tradizionali” modalità di acquisizione di una notizia di reato da parte della polizia giudiziaria richiedano alcune rivisitazioni, allorquando l’allegato alla denuncia è ormai, quasi sempre, rappresentato da un elemento “digitale” (un file). Ritengo che l’articolo richiamato in nota 2 possa essere ampliamente esplicativo ed esaustivo rispetto a queste criticità.

Nonostante i tratteggiati sforzi posti in essere dalle FF.PP., il **personale “qualificato”/”specializzato” in *digital forensics***, o per dirla in altri modi “capace” di gestire fin dalla denuncia una “*evidence* digitale” non ha ancora raggiunto una così capillare diffusione da poter assicurare in ogni ufficio denunce la presenza di una di queste figure. Anzi, la loro fisiologica scarsità destina tale personale esperto verso reparti e attività maggiormente impegnati nel contrasto al crimine informatico, lasciando così “scoperto” quell’ambito - delicatissimo - rappresentato dalla denuncia: e si sa, come si dice in gergo, che *“chi nasce male…"* L’assenza di tale personale fin da quella fase embrionale riverbera, spesso, “errori” che si ripercuotono nella fase dibattimentale, ove magari dopo mesi di indagini, ci si può ritrovare con la cd. “prova regina” invalidata perché non acquisita, gestita e trattata nel rispetto di poche regole che ormai dovrebbero essere state “standardizzate” da ogni ufficiale di polizia giudiziaria.

Proprio su questa criticità rappresentata dall’assenza di personale “esperto” proprio laddove può nascere la *notitia criminis* (l’ufficio denunce di qualsiasi posto di polizia) mi sono giunte richieste su quali siano gli **strumenti** (magari *open-source* o comunque gratuiti) **di cui l’U.P.G. 4.0. potrebbe dotarsi** per raccogliere al meglio una denuncia ed evitare, così, di veder andare in “fumo” mesi di indagini. In merito, se da un lato è vero che molti avvocati ed esperti del settore prestano le propri capacità professionali anche nella redazione di notizie di reato indenni da queste problematiche, è altrettanto vero che l’ignaro cittadino comune è tutt’oggi convinto che la “stampa” del file dell'email o della chat siano di per sé abbondantemente sufficienti a supportare le loro ragioni in denuncia. Ma di questo abbiamo già ampiamente dibattuto in altri articoli.

Tornando alla domanda, la risposta non è così scontata e semplice e rivolta a più specialisti della materia si risolverebbe - e sono sicuro di non sbagliarmi - nella segnalazione di **decine di prodotti diversi** (anche se, in definitiva, fanno la stessa cosa) che spesso ottengono la preferenza rispetto ad altri sulla scorta di diverse ragioni:

- *"è il primo che ho utilizzato e lo conosco meglio";*
- *"lo usano tutti quelli di...";*
- *"ho sempre avuto solo questo";*
- *"quell'altro non funzionava, mi dava sempre errore";*
- ...e tante altre che abbiamo sentito molte volte ("*non gira su… io uso solo Linux… non digerisco MacOs"*).

Penso che la scelta, per quanto legata a preferenze personali che possono essere le più diverse, richieda per una risposta esauriente un approfondito collaudo dei diversi *tool* e

programmi, volto a testare:

- il rispetto delle *best practices* e della disciplina codicistica in materia;
- la loro efficacia ed efficienza rispetto il “fine” per cui vengono utilizzate;
- la loro facilità di apprendimento e utilizzo rispetto a una platea di utilizzatori che, sulle premesse fatte sopra, va allargata ben oltre quella più limitata e preparata dei cd. *First Responder* e *Digital Evidence Specialist* cui siamo soliti riferirci, dovendo ricomprendere quella che vorremo chiamare U.P.G. 4.0. e che dovrebbe quindi rivolgersi a tutti gli ufficiali di P.G. (quand’anche a quelli che lo sono solo nell’esercizio di determinate funzioni) e che non hanno particolari “cognizioni” in materia di *digital forensics.*

È evidente, come ho già avuto di evidenziare, che solo la “scuola” di formazione delle FF.PP. potrà in futuro colmare questo *gap* introducendo, tra le discipline del corso di formazione, anche **corsi di *digital forensics*** capaci di fornire a ciascun operatore le conoscenze minime per poter operare in un campo che ormai ha pervaso ogni ambito investigativo.

Nel panorama *digital forensics* esistono diverse *suite* del tipo *“digital-forensics-oriented”* quali BENTO, DART, TSURUGI, DEFT, KALI: tutte danno la possibilità in diversi contesti – *live, post-mortem*, laboratorio - di fare *digital forensics* a “costo-zero”, con eccellenti risultati, anche rispetto più rinomate e titolate *suite* commerciali; tuttavia il loro utilizzo richiede solide cognizioni e buone capacità e conoscenza anche della riga di comando (CLI), requisiti che, se patrimonio del personale *First Responder* e *Digital Evidence Specialist* delle varie specialità di polizia, si riscontrano più raramente nella “generalità” degli U.P.G. che, nella migliore delle ipotesi, hanno “minime”, se non “alquanto modeste”, cognizioni in materia.

Si è tentato più volte e in diversi modi di istruire tutto il personale sull’utilizzo di queste *suite*, quanto meno nell’uso dei *tool* cd. “essenziali”, ma la **vastità degli strumenti** a disposizione, anziché rassicurare, tende spesso a spaventare il profano che si orienta verso prodotti singoli che conosce meglio e sui quali si addestra più facilmente all’uso. Non è un caso, del resto, che le stesse *suite* abbiano delle versioni *“acquire”* destinate solo a questo scopo, “sfoltite” di quei *tool* che risulterebbero meno necessari in tale fase; e penso di non essere smentito nel considerare come il loro utilizzo sia “riservato” a personale esperto, in quanto solo un'approfondita conoscenza dei diversi *tool* di queste *suite* permette di riscontrarne appieno l’elevata efficacia e di apprezzarne gli effetti, essendo spesso costituite da un insieme di *tool* molto efficaci in singole attività e che, se sapientemente combinati tra loro, possono davvero competere - e talvolta superare - *tool* commerciali di più facile approccio.

Altrettanto evidente è considerare che chi non ha conoscenze “approfondite” è alla ricerca di **soluzioni *“one-click”*** che, seppur criticabili sul piano dell’efficienza ed efficacia, risultano comunque apprezzate per la loro facilità di utilizzo da chi non ha competenze specialistiche e non ha alcuna intenzione di acquisirle, ma è tuttavia disposto a seguire poche, semplici istruzioni.

Prendiamo per esempio un'operazione che potrebbe sembrare banale: come quella del calcolo di un *hash* su di un file operazione che, se affidata ad un “esperto” della materia, può vedere il ricorso a decine di *tool* e tecniche (da CLI è abbastanza semplice per l’esperto calcolare l’*hash*

di un file).

Tutti ormai dovrebbero sapere cosa sia un *“hash”* ma, soprattutto, dovremmo aver raggiunto un grado di cultura informatica che ci permetta di dire che non dovrebbe esistere l’indicazione di un file priva del suo *hash* che lo “identifichi” compiutamente. Purtroppo non sempre è così e ancora pervengono notizie di reato e denunce corredate da files privi di qualsivoglia *hash* con la **pericolosa conseguenza** che, anche involontariamente, nei vari passaggi di mano della stesse può capitare che quei files vengano “modificati”, quant’anche involontariamente, con tutti gli “imbarazzanti” effetti che possono derivarne.

Non dovrebbe allora essere così complicato imporre a ogni UPG, qualora si ritrovi dinanzi a un elemento digitale (foto, file, video), di dover procedere al calcolo dell’*hash* e verbalizzarlo nell'atto della denuncia.

La già ricordata **circolare della GDF**, a pagina 31 del Volume 2, recita testualmente: *"In ogni caso, e quale regola generale cui conformarsi anche in assenza dei militari CFDA, anche per l’acquisizione di singoli documenti informatici, è opportuno, ove tecnicamente possibile in relazione alle competenze degli operanti, calcolare un’impronta logico-matematica detta hash. La determinazione dell’impronta (*rectius *valore di hash e funzione di verifica) del documento informatico attraverso gli algoritmi di hash consente, infatti, unitamente alla documentazione delle attività svolte, di ricostruire le azioni svolte sui documenti informatici di interesse".*

Sottolineo “*ove tecnicamente possibile in relazione alle competenze degli operanti”,* vi è quindi consapevolezza che non tutto il personale abbia quelle competenze così minime.

Da tempo, quindi, occupandomi anche di formazione dei cd. *First Responder* - che, ribadisco, in quest’ottica rappresentano già un livello più avanzato rispetto all’ordinario U.P.G. - mi sono posto la domanda di come si possa, anche a livello di qualsiasi ufficio periferico di polizia, **standardizzare procedure di acquisizione di denunce corredate da allegati digitali**.

Inizialmente l’attenzione è caduta su singoli *tool* (per esempio HASH MY FILE[5], peraltro presente in diverse delle suite sopra citate) che, se contraddistinte da un'elementare facilità d’uso (basta trascinare il file di cui si vuole calacolare l’*hash* all’interno della finestra), presentano un certo grado di complessità in ordine alla scelta dell’algoritmo, esportazione del report e tutta una serie di operazioni di copia/incolla, ridimensione della finestra per essere incollata in un file word, etc. non sempre di così facile e immediata realizzazione per un profano. Qui sento già qualcuno dire*“basta allegare il report”*: verissimo, tuttavia, per esperienza, spesso l’allegato si stacca dal verbale e si perde magari nel corso di fotocopie e quindi consiglio sempre di integrare gli *hash* direttamente nel verbale che non si perde (quasi) mai… sarò paranoico, ma preferisco così.

Sempre alla ricerca di soluzioni più facili per tutti (anche per i profani), l’attenzione è caduta su HashGen All in One [6]. A scapito dell’etimologia (che lo farebbe apparire, a prima vista, un software dedicato solo all’*hash*), quand’anche non corredato delle centinaia di *tool* delle più blasonate *suite* già sopra citate, capaci di assicurare con strumenti *open-source* una *digital forensics* a 360°, questo software presenta alcune “novità” e *features* meritevoli di particolare

apprezzamento da parte degli operatori di P.G.

Ciò che mi ha positivamente colpito rispetto al caso che stiamo trattando - calcolo dell'*hash* - è la possibilità di **generazione automatica del verbale di operazioni tecniche** originato sulla base dei dati forniti di volta in volta dall'operatore che di fatto elimina quelle operazioni di copia/incolla dal programma o CLI di calcolo dell'*hash* al verbale che potrebbero ingenerare errori. Una procedura in pratica "automatizzata" attraverso la quale, con alcuni "pulsanti" di inequivocabile interpretazione, chiunque è in grado di poter generare l'*hash* di un file e redigere un adeguato "verbale" delle operazioni compiute.

Lo stesso, ovvero la generazione di un verbale, avviene in maniera semplificata anche con riferimento al cd. interprete di conversazioni whatsapp che permette, in maniera alquanto intuitiva, di redigere una verbalizzazione delle conversazioni di una chat whatsapp corredata di testo e immagini.

Molto utile anche l'acquisizione di riproduzioni fotografiche e l'estrazione automatica di **tabulati telefonici** che, unite a una funzione *write-blocker* altrettanto intuitiva e di facile attivazione, permettono di avere una "piccola" casetta di attrezzi essenziali per le più comuni attività di ricezione di denuncia (e non solo) che un comune U.P.G. 4.0 può trovarsi ad affrontare.

Conclusioni

Occorre sempre più **cultura e formazione digitale** per saper affrontare le nuove sfide tecnologiche: i reati sono sempre gli stessi, anche se sono profondamente cambiate le "dinamiche" e gli "oggetti" coinvolti, tanto da costringere gli U.P.G. 4.0 ad avvalersi di nuovi strumenti e tecniche fin dalla ricezione della denuncia. L'acquisizione, in sede di denuncia, di un file (magari prova regina!) non effettuata correttamente potrebbe solo, in sede dibattimentale e magari dopo mesi di impegnative indagini, venire "censurata" perché non "affidabile", "genuina", "garantita".

Ben vengano allora, al fianco delle più blasonate *suite* forensi dedicate a personale maggiormente formato ed esperto, anche software come quello qui sopra citato che permettono anche al personale meno esperto di corredare correttamente una denuncia, acquisire un piccolo *device* e svolgere, in modo più agevole e sicuro, le "operazioni" più comuni che oggi l'U.P.G. 4.0 si trova ad affrontare fin da quella fase "embrionale" che è la denuncia.

Note

[1] https://www.ictsecuritymagazine.com/author/pier-luca-toselli/

[2] https://www.ictsecuritymagazine.com/articoli/legge-18-marzo-2008-n-48-lufficiale-polizia-

giudiziaria-dieci-anni/

[3] https://www.ictsecuritymagazine.com/articoli/giovani-e-whatsapp-come-introdurre-una-chat-nel-processo/

[4] La Guardia di Finanza, con la circolare 1/2018, ha dimostrato grande sensibilità su questi temi, in considerazione di un rinnovato panorama operativo connaturato sempre più dalla dimensione digitale bisognoso di nuove “regole” e “procedure” per una corretta “gestione” dei dati. Ma anche le altre FF.PP. sono continuamente impegnate nella formazione di personale capace, fin dalle fasi preliminari, di gestire correttamente “l’*evidence* digitale”, nella consapevolezza che ormai “tutto è digitale”.

[5] https://www.nirsoft.net/utils/hash_my_files.html

[6] https://www.hashgen.it

Articolo a cura di **Pier Luca Toselli**