Polizia di Stato

DIGITAL FORENSICS

Forma e Sostanza

CAMERINO, 27 Aprile 2015

Raul Guido Capriotti

DEFINIZIONE DI

DIGITAL FORENSICS

Insieme di indagini, rilievi, accertamenti ed altre operazioni tecniche, in relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, necessarie per le determinazioni inerenti all'esercizio dell'azione penale.

The goal of digital forensics is to do a structured investigation and find out exactly what happened on a digital system, and who was responsible for it

Questa in effetti **non è una pipa**, è solo **il dipinto di una pipa**.
L'immagine potrebbe essere:

- la raffigurazione, da parte dell'artista, di una reale pipa;
- la raffigurazione di una pipa completamente immaginaria;
- la raffigurazione composita di molte pipe.

FASI DELLA DIGITAL FORENSICS

- Attività di indagine e investigazione;
- Identificazione;
- Acquisizione;
- Preservazione/Conservazione;
- Analisi;
- Presentazione.

FASI DELLA DIGITAL FORENSICS

LA LEGGE DI MURPHY

"Se qualcosa può andar male lo farà."

che deriva dalla storica frase pronunciata da Edward Murphy:

"se ci sono due o più modi di fare una cosa,
e uno di questi modi può condurre ad una catastrofe,
allora qualcuno la farà in quel modo."

DIGITAL FORENSICS
Ambiti di Applicazione

- Contesto Investigativo/Giudiziario (Penale, Civile, etc.);
- Contesto Investigativo-Privatistico:
  - Familiare (Infedeltà coniugale, Attribuzione testamentaria, etc.);
  - Personale (Recupero dati, etc.);
  - Aziendale (Infedeltà dei dipendenti, Furto di informazioni riservate, Incident Response, Disaster Recovery, etc.);
- Contesto Investigativo-Pubblicistico:
  - Enti Nazionale e/o Sovrannazionali (Antitrust - cartelli, abuso di posizione dominante, etc. - Enti di certificazione, etc.);
  - Multinazionali (VISA, MASTERCAD, AMERICAN EXPRESS, PCI DSS - Payment Card Industry Data Security Standard -, etc.).

LEGGE 18 MARZO 2008, N. 48

"Ratifica ed esecuzione della Convenzione
del Consiglio d'Europa sulla criminalità informatica,
fatta a Budapest il 23 novembre 2001,
e norme di adeguamento dell'ordinamento interno"

Apporta delle modifiche significative al:

- Codice Penale;
- Codice di Procedura Penale;
- D.Lvo 196/2003;
- D.Lvo 231/2001.

DIGITAL FORENSICS

Contesto Investigativo/Giudiziario

Art. 244 c.p.p. - ***Casi e forme delle ispezioni.***

Omissis

L'autorità giudiziaria può disporre rilievi segnaletici, descrittivi e fotografici e ogni altra operazione tecnica, anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.

DIGITAL FORENSICS

Contesto Investigativo/Giudiziario

Art. 247 c.p.p. - *Casi e forme delle perquisizioni.*

Omissis

1-bis. Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.

Art. 254 c.p.p. - *Sequestro di corrispondenza.*

1. Presso coloro che forniscono servizi postali, telegrafici, telematici o di telecomunicazioni è consentito procedere al sequestro di lettere, pieghi, pacchi, valori, telegrammi e altri oggetti di corrispondenza, anche se inoltrati per via telematica, che l'autorità giudiziaria abbia fondato motivo di ritenere spediti dall'imputato o a lui diretti, anche sotto nome diverso o per mezzo di persona diversa, o che comunque possono avere relazione con il reato.

DIGITAL FORENSICS

Contesto Investigativo/Giudiziario

Art. 254-bis. c.p.p.

Sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni.

1. L'autorità giudiziaria, quando dispone il sequestro, presso i fornitori di servizi informatici, telematici o di telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico o di ubicazione, può stabilire, per esigenze legate alla regolare fornitura dei medesimi servizi, che la loro acquisizione avvenga mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità. In questo caso è, comunque, ordinato al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali.

DIGITAL FORENSICS

Contesto Investigativo/Giudiziario

Art. 256 c.p.p. - *Dovere di esibizione e segreti.*

1. Le persone indicate negli articoli 200 e 201 devono consegnare immediatamente all'autorità giudiziaria, che ne faccia richiesta, gli atti e i documenti, anche in originale se così è ordinato, nonché i dati, le informazioni e i programmi informatici, anche mediante copia di essi su adeguato supporto

Omissis

Art. 259 c.p.p. - *Custodia delle cose sequestrate.*

Omissis

Quando la custodia riguarda dati, informazioni o programmi informatici, il custode è altresì avvertito dell'obbligo di impedirne l'alterazione o l'accesso da parte di terzi, salva, in quest'ultimo caso, diversa disposizione dell'autorità giudiziaria.

DIGITAL FORENSICS

Contesto Investigativo/Giudiziario

Art. 260 c.p.p.

Apposizione dei sigilli alle cose sequestrate. Cose deperibili. Distruzione di cose sequestrate.

1. Le cose sequestrate si assicurano con il sigillo dell'ufficio giudiziario e con le sottoscrizioni dell'autorità giudiziaria e dell'ausiliario che la assiste ovvero, in relazione alla natura delle cose, con altro mezzo, anche di carattere elettronico o informatico, idoneo a indicare il vincolo imposto a fini di giustizia.

Omissis

Quando si tratta di dati, di informazioni o di programmi informatici, la copia deve essere realizzata su adeguati supporti, mediante procedura che assicuri la conformità della copia all'originale e la sua immodificabilità

Omissis

DIGITAL FORENSICS

Contesto Investigativo/Giudiziario

Art. 348 c.p.p. - *Assicurazione delle fonti di prova.*

Omissis

4. La polizia giudiziaria, quando, di propria iniziativa o a seguito di delega del pubblico ministero, compie atti od operazioni che richiedono specifiche competenze tecniche, **può avvalersi di persone idonee le quali non possono rifiutare la propria opera**.

Art. 352 c.p.p. - *Perquisizioni.*

Omissis

1-bis. Nella flagranza del reato, ovvero nei casi di cui al comma 2 quando sussistono i presupposti e le altre condizioni ivi previsti, gli ufficiali di polizia giudiziaria, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione, procedono altresì alla perquisizione di sistemi informatici o telematici, ancorché protetti da misure di sicurezza, quando hanno fondato motivo di ritenere che in questi si trovino occultati dati, informazioni, programmi informatici o tracce comunque pertinenti al reato che possono essere cancellati o dispersi.

DIGITAL FORENSICS

Contesto Investigativo/Giudiziario

Art. 354 c.p.p.

Accertamenti urgenti sui luoghi, sulle cose e sulle persone. Sequestro.

Omissis

In relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, gli ufficiali della polizia giudiziaria adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità.

DIGITAL FORENSICS

Contesto Investigativo/Giudiziario

Art. 359 c.p.p. - *Consulenti tecnici del pubblico ministero.*

1. Il pubblico ministero, quando procede ad accertamenti, rilievi segnaletici, descrittivi o fotografici e ad ogni altra operazione tecnica per cui sono necessarie specifiche competenze, può nominare e avvalersi di consulenti, che non possono rifiutare la loro opera.
2. Il consulente può essere autorizzato dal pubblico ministero ad assistere a singoli atti di indagine.

DIGITAL FORENSICS

Contesto Investigativo/Giudiziario

Art. 360 c.p.p. - *Accertamenti tecnici non ripetibili.*

1. Quando gli accertamenti previsti dall'articolo 359 riguardano persone, cose o luoghi il cui stato è soggetto a modificazione, il pubblico ministero avvisa, senza ritardo, la persona sottoposta alle indagini, la persona offesa dal reato e i difensori del giorno, dell'ora e del luogo fissati per il conferimento dell'incarico e della facoltà di nominare consulenti tecnici.
2. Si applicano le disposizioni dell'articolo 364 comma 2.
3. I difensori nonché i consulenti tecnici eventualmente nominati hanno diritto di assistere al conferimento dell'incarico, di partecipare agli accertamenti e di formulare osservazioni e riserve.
4. Qualora, prima del conferimento dell'incarico, la persona sottoposta alle indagini formuli riserva di promuovere incidente probatorio, il pubblico ministero dispone che non si proceda agli accertamenti salvo che questi, se differiti, non possano più essere utilmente compiuti.
5. Se il pubblico ministero, malgrado l'espressa riserva formulata dalla persona sottoposta alle indagini e pur non sussistendo le condizioni indicate nell'ultima parte del comma 4, ha ugualmente disposto di procedere agli accertamenti, i relativi risultati non possono essere utilizzati nel dibattimento.

DIGITAL FORENSICS

Contesto Investigativo/Giudiziario

Art. 327-bis c.p.p. - ***Attività investigativa del difensore.***

1. Fin dal momento dell'incarico professionale, risultante da atto scritto, il difensore ha facoltà di svolgere investigazioni per ricercare ed individuare elementi di prova a favore del proprio assistito, nelle forme e per le finalità stabilite nel titolo VI-bis del presente libro (Libro Quinto - Titolo I - Cod. Proc. Pen.).
2. La facoltà indicata al comma 1 può essere attribuita per l'esercizio del diritto di difesa, in ogni stato e grado del procedimento, nell'esecuzione penale e per promuovere il giudizio di revisione.
3. **Le attività previste dal comma 1 possono essere svolte, su incarico del difensore, dal sostituto, da investigatori privati autorizzati e, quando sono necessarie specifiche competenze, da consulenti tecnici.**

DIGITAL FORENSICS

Contesto Investigativo/Giudiziario

Art. 220 c.p.p. - ***Oggetto della perizia***

1. La perizia è ammessa quando occorre svolgere indagini o acquisire dati o valutazioni che richiedono specifiche competenze tecniche, scientifiche o artistiche.

Art. 221 c.p.p. - ***Nomina del perito***

1. Il giudice nomina il perito scegliendolo tra gli iscritti negli appositi albi o tra persone fornite di particolare competenza nella specifica disciplina .....
3. Il perito ha l'obbligo di prestare il suo ufficio, salvo che ricorra uno dei motivi di astensione previsti dall'art. 36.

Art. 225 c.p.p. - ***Nomina del consulente tecnico.***

1. Disposta la perizia, il pubblico ministero e le parti private hanno facoltà di nominare propri consulenti tecnici in numero non superiore, per ciascuna parte, a quello dei periti.

Peculiarità del
Codice di Procedura Penale Italiano

Art. 134 c.p.p. ***Modalità di documentazione.***

1. Alla documentazione degli atti si procede mediante verbale.
2. Il verbale è redatto, in forma integrale o riassuntiva .....

Art. 136 c.p.p. ***Contenuto del verbale.***

1. **Il verbale contiene la menzione del luogo, dell'anno, del mese, del giorno e, quando occorre, dell'ora in cui è cominciato e chiuso, le generalità delle persone intervenute, l'indicazione delle cause, se conosciute, della mancata presenza di coloro che sarebbero dovuti intervenire, la descrizione di quanto l'ausiliario ha fatto o ha constatato o di quanto è avvenuto in sua presenza nonché le dichiarazioni ricevute da lui o da altro pubblico ufficiale che egli assiste.**
2. Per ogni dichiarazione è indicato se è stata resa spontaneamente o previa domanda e, in tale caso, è riprodotta anche la domanda; se la dichiarazione è stata dettata dal dichiarante, o se questi si è avvalso dell'autorizzazione a consultare note scritte, ne è fatta menzione.

Peculiarità del
Codice di Procedura Penale Italiano

Art. 137 c.p.p. ***Sottoscrizione del verbale.***

1. ..... **il verbale, previa lettura, è sottoscritto alla fine di ogni foglio dal pubblico ufficiale che lo ha redatto, dal giudice e dalle persone intervenute, anche quando le operazioni non sono esaurite e vengono rinviate ad altro momento.**
2. Se alcuno degli intervenuti non vuole o non è in grado di sottoscrivere, ne è fatta menzione con l'indicazione del motivo.

Art. 142 c.p.p. ***Nullità dei verbali.***

1. Salve particolari disposizione di legge, **il verbale è nullo se vi è incertezza assoluta sulle persone intervenute o se manca la sottoscrizione del pubblico ufficiale che lo ha redatto.**

Peculiarità del
Codice di Procedura Penale Italiano

Art. 227 c.p.p. ***Relazione peritale.***

1. Concluse le formalità di conferimento dell'incarico, il perito procede immediatamente ai necessari accertamenti e risponde ai quesiti con parere raccolto nel verbale.

Omissis

5. Qualora sia indispensabile illustrare con note scritte il parere, il perito può chiedere al giudice di essere autorizzato a presentare relazione scritta.

Art. 228 c.p.p. ***Attività del perito.***

1. Il perito procede alle operazioni necessarie per rispondere ai quesiti. A tal fine può essere autorizzato dal giudice a prendere visione degli atti, dei documenti e delle cose prodotti dalle parti dei quali la legge prevede l'acquisizione al fascicolo per il dibattimento.

Omissis

Peculiarità del
Codice di Procedura Penale Italiano

Art. 229 c.p.p. ***Comunicazioni relative alle operazioni peritali.***

1. Il perito indica il giorno, l'ora e il luogo in cui inizierà le operazioni peritali e il giudice ne fa dare atto nel verbale.
2. Della eventuale continuazione delle operazioni peritali il perito dà comunicazione senza formalità alle parti presenti.

Art. 230 c.p.p. ***Attività dei consulenti tecnici.***

1. I consulenti tecnici possono assistere al conferimento dell'incarico al perito e presentare al giudice richieste, osservazioni e riserve, delle quali è fatta menzione nel verbale.

FASI DELLA DIGITAL FORENSICS

PRESENTAZIONE

La rappresentazione oggettiva dei risultati dell'attività di acquisizione e analisi dell'evidenza informatica, è prodromica ma non coincidente con le conclusioni in ordine all'investigazione. La presentazione deve essere tesa all'illustrazione dell'accertamento di determinati atti o fatti ed esposta in modo tale da essere pienamente comprensibile, anche da persone con scarse conoscenze informatiche. La necessità di rendere comprensibile l'esito dell'esame di un sistema informatico è, non di rado, la maggiore delle difficoltà che si incontrano nella pratica della materia in trattazione. E' necessario limitarsi ad inserire nella relazione conclusiva solo gli elementi utili per l'investigazione, al fine di evitare che l'autorità giudiziaria, cui l'atto è diretto, sia costretta e disporre apposita consulenza per estrapolare, da una relazione inutilmente omnicomprensiva, i dati di specifico interesse. Qualora vi sia necessità di utilizzare terminologie di carattere tecnico/scientifico, è opportuno prevedere in nota o in appendice una apposita spiegazione dei detti vocaboli.

FASI DELLA DIGITAL FORENSICS

PRESENTAZIONE

La relazione di presentazione dei risultati di ricerca sull'evidenza informatica dovrebbe contenere:

- il nominativo della persona che ha eseguito l'analisi o attività richiesta;
- breve descrizione del caso sotto esame ed elencazione dei quesiti posti;
- la data e l'ora di inizio e di termine dell'operazione di acquisizione dell'evidenza informatica;
- i dati dei supporti su cui la copia dell'evidenza informatica è stata riversata;
- i codici di validità (checksum o message digest, sia esso riferito all'algoritmo MD5 o SHA1) dell'evidenza informatica e delle copie speculari, nel caso di accertamenti ripetibili;
- la descrizione delle caratteristiche del sistema posto sotto analisi (hardware e software)
- la descrizione di tutte le operazioni effettuate sul supporto originale, che costituisce l'evidenza informatica;
- la descrizione delle operazioni di analisi e ricerca effettuate sulla copia dell'evidenza;
- l'elencazione e la descrizione delle caratteristiche dei programmi eventualmente utilizzati, con particolare riferimento a quelli impiegati per ricercare informazioni in zone non allocate del "filesystem";
- la collocazione esatta (percorso logico o path) delle informazioni utili per le indagini (siano essi testi, immagini, video, suoni o programmi);
- la stampa, in caso sia possibile e necessario, dei dati rinvenuti;
- la registrazione possibilmente su supporto non alterabile, dei dati di interesse;
- le conclusioni relative il caso trattato.

Polizia di Stato

DIGITAL FORENSICS

Forma e Sostanza

CAMERINO, 27 Aprile 2015

Raul Guido Capriotti