ORDINE AVVOCATI TORINO
COMMISSIONE SCIENTIFICA

21 novembre 2019, Tribunale di Torino, Maxi aula 2
LO STRUMENTO INFORMATICO QUALE MEZZO PER LA COMMISSIONE DEL REATO

GLI STRUMENTI INVESTIGATIVI A DISPOSIZIONE DEI DIFENSORI E DEI PROPRI CONSULENTI PER LA RICERCA DELLA PROVA, PROFILI INERENTI ALL'ATTENDIBILITÀ DEL DATO "TECNOLOGICO"

Paolo Dal Checco

Consulente Informatico Forense

Chi sono

- PhD @UniTO nel gruppo di Sicurezza delle Reti e degli Elaboratori
- Passato di R&D su crittografia e sicurezza delle comunicazioni
- Collaborazione con Università degli Studi di Torino e Milano
- Consulente Informatico Forense, Perizie Informatiche per Privati, Aziende, Avvocati, Procure, Tribunali, F.F.O.O.
- Albo CTU e Periti del Tribunale di Torino, Periti ed Esperti CCIAA TO
- Tra i fondatori e nel direttivo dell'Osservatorio Nazionale d'Informatica Forense (www.onif.it)
- Socio IISFA, Tech & Law, Clusit, LAB4INT, Assob.It, AIP
- www.dalchecco.it, www.ransomware.it, www.bitcoinforensics.it, www.osintbook.it
- paolo@dalchecco.it, @forensico

Cosa è l'informatica forense?

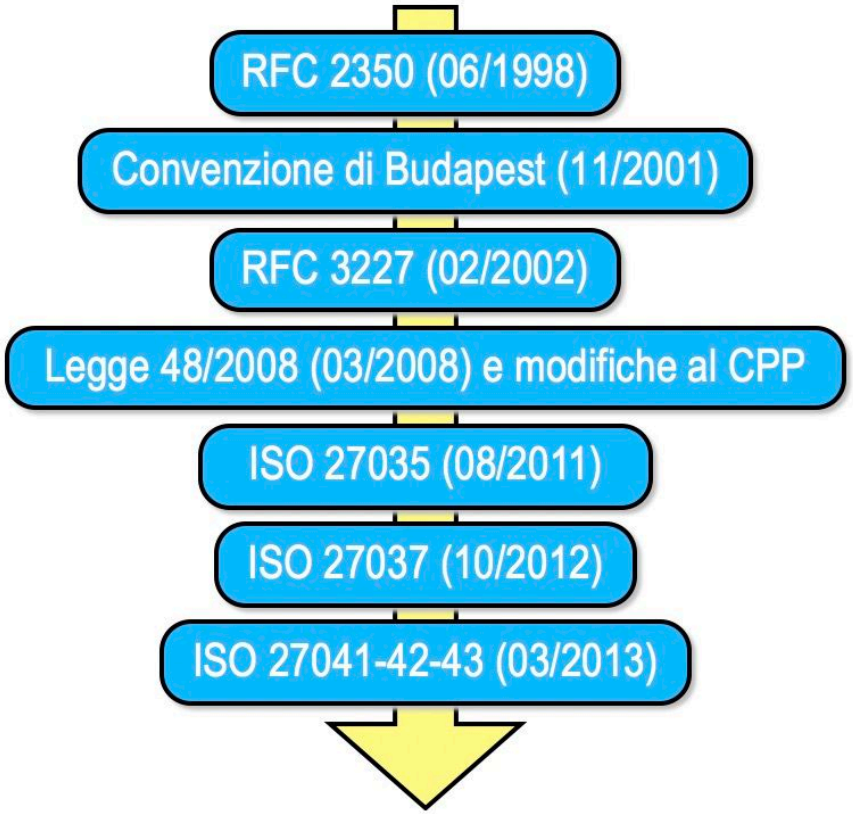
- Ricerca, identificazione, raccolta, preservazione, acquisizione, analisi, presentazione e valutazione dei dati informatici a fini probatori
- Regolata in Italia dalla Legge 48 del 2008, non esistono al momento altre normative o certificazioni
- La «digital forensics» è un ramo della scienza forense che comprende il recupero e l'indagine del materiale trovato nei dispositivi digitali, spesso in relazione a eventi di criminalità informatica ma non solo, ormai qualunque reato ha una componente «digitale».

- Alcuni esempi di reati:
  - Furto credenziali, Accesso abusivo a dati o sistemi
  - Violazione di Corrispondenza, Danneggiamento
  - Diffamazione su internet, Concorrenza sleale e dipendente infedele
  - Ransomware (accesso abusivo, danneggiamento, estorsione)
  - Phishing (truffa, sostituzione di persona, accesso abusivo)
  - Omicidio, furto, suicidio, sostituzione di persona
  - Etc…

Chi si avvale dell'Informatica forense?

- Giudici
  - CTU in procedimenti civili
  - Perito in procedimenti penali
- Pubblici Ministeri
  - Consulente Tecnico del PM
- Avvocati
  - Consulente Tecnico di Parte
  - Perizie stragiudiziali
- Aziende
  - Investigazioni difensive
  - Gestione di incidenti di sicurezza
- Società di investigazione
- Privati

Basi tecniche e normative della digital forensics



Legge 48/2008

- Contiene alcune importanti definizioni/requisiti:
- «adottando **misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione**».
- **«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»**
- «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**».
- **«la copia deve essere realizzata su adeguati supporti, mediante procedura che assicuri la conformità della copia all'originale e la sua immodificabilità**; in tali casi, **la custodia degli originali può essere disposta anche in luoghi diversi dalla cancelleria o dalla segreteria»**
- **«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»**

Un esempio di necessità di best practice

49016-17

In caso di diffusione del presente provvedimento omettere le generalità e gli altri dati identificativi, a norma dell'art. 52 d.lgs. 196/03 in quanto:
☐ disposto d'ufficio
☐ a richiesta di parte
☐ imposto dalla legge

REPUBBLICA ITALIANA
In nome del Popolo Italiano
LA CORTE SUPREMA DI CASSAZIONE
QUINTA SEZIONE PENALE

Composta da:

PUBBLICA UDIENZA
DEL 19/06/2017

MARIA VESSICHELLI - Presidente -
CATERINA MAZZITELLI
SERGIO GORJAN
GIUSEPPE DE MARZO
IRENE SCORDAMAGLIA - Rel. Consigliere -

Sent. n. sez.
1660/2017

REGISTRO GENERALE
N.9109/2017

http://www.processopenaleegiustizia.it/materiali/49016.pdf

Un esempio di necessità di best practice

2. Va giudicata ineccepibile la decisione della Corte territoriale di non acquisire la trascrizione delle conversazioni svoltesi sul canale informatico denominato '*whatsapp*', tra l'imputato e la parte offesa il 2 gennaio 2014, che la difesa dell'imputato avrebbe voluto versare agli atti del processo a riprova della inattendibilità della persona offesa, che aveva sostenuto che la relazione con l'imputato si era interrotta nell'ottobre 2013.

Deve, infatti, osservarsi che, per quanto la registrazione di tali conversazioni, operata da uno degli interlocutori, costituisca una forma di memorizzazione di un fatto storico, della quale si può certamente disporre legittimamente ai fini probatori, trattandosi di una prova documentale, atteso

Un esempio di necessità di best practice

che l'art. 234, comma 1, cod. proc. pen. prevede espressamente la possibilità di acquisire documenti che rappresentano fatti, persone o cose mediante la fotografia, la cinematografia, la fonografia o qualsiasi altro mezzo (in tema di registrazione fonica cfr. Sez. 1, n. 6339 del 22/01/2013, Pagliaro, Rv. 254814; Sez. 6, n. 16986 del 24/02/2009, Abis, Rv. 243256), l'utilizzabilità della stessa è, tuttavia, condizionata dall'acquisizione del supporto – telematico o figurativo - contenente la menzionata registrazione, svolgendo la relativa trascrizione una funzione meramente riproduttiva del contenuto della principale prova documentale (Sez. 2, n. 50986 del 06/10/2016, Rv. 268730; Sez. 5, n. 4287 del 29/09/2015 – dep. 2/02/2016, Pepi, Rv. 265624): tanto perché occorre controllare l'affidabilità della prova medesima mediante l'esame diretto del supporto onde verificare con certezza sia la paternità delle registrazioni sia l'attendibilità di quanto da esse documentato.

Le possibilità tecniche e giuridiche dei difensori e del CTP

- Difensori e CT spesso **non hanno accesso ad alcuni i dati**. Ad esempio:
  - Dati di traffico (telefonico, email, etc...)
  - Dati cancellati da Profili web
- Per alcuni dati, invece, la parte ha accesso diretto, talvolta persino più dettagliato dell'A.G. o più facile da ottenere (no rogatoria) come ad esempio:
  - Backup Facebook
  - Google Takeout
  - Export Telegram, Whatsapp, etc… (chat cifrate)

Tre livelli di acquisizione e ricerca della prova

- Tre livelli di autonomia per i difensori e CT

- 1) Contatto e accesso diretto alle evidenze digitali
- 2) Precauzioni nell'accesso e ricerca, richieste protocollate
- 3) Best Practices (digital forensics)

1) Contatto e accesso diretto alle evidenze digitali

- Spesso errato perché non conferisce validità alla prova o la altera
- Alcuni esempi:
  - richiesta di file di log via email (spesso nessuna risposta o risposta informale)
  - inserimento pendrive con evidenze su un PC per visione (modifica evidenza)
  - apertura documenti (modifica metadati, es. Word)
  - screenshot pagine web, chat (non valido a fini probatori)

2) Precauzioni nell'accesso e ricerca, richieste protocollate

- Approccio autonomo da parte dei legali, permette una sorta di «triage» sulle evidenze senza alterarle garantendo nel contempo validità probatoria, ad esempio:
  - Richieste via PEC per log di accesso (i log delle PEC per sono accedibili spesso via web)
  - Accesso protetto a dispositivi (read-only tramite Disk Arbitrator, USB WriteProtector, Linux)
  - Accessi e acquisizioni di risorse web mediante servizi/strumenti appositi
  - Export dei dati tramite servizi (spesso inseriti dopo il GDPR) forniti dai provider:
    - Google Takeout (anche email, posizioni GPS, navigazione, etc...)
    - Twitter, Linkedin, Facebook (includono indirizzi IP che l'AG spesso non riesce ad avere)
    - Chat Export da Telegram, Whatsapp
  - Backup di smartphone tramite HiSuite, Xiaomi Backup oppure iTunes o Smart Switch/ADB

3) Best Practices (digital forensics)

- Richiede assistenza di un CTP che esegua attività dedicate di digital forensics, con produzione di perizia informatica. Es:
  - Acquisizione forense
    - Hard disk tramite copiatori forensi
    - Smartphone
    - Email
    - Log di accesso, tabulati, chat, pagine web, gruppi Facebook, chat, etc…
- Accessi acquisiti tramite strumentazione forense
- Produzione di perizia informatica con certificazione integrità tramite valori hash e timestamp digitale (apposizione data certa, anche via blockchain)

Possibilità di contraddittorio

- Se tutto viene eseguito nel modo corretto, sia dalle parti sia dall'AG/PG, si ha poi possibilità di contraddittorio nell'analisi dei dati, attività che diventa quindi **ripetibile**
- SI comincia con il **confronto dei valori hash** e **verifica integrità dei dati**
- Frequenti **errori di valutazione** da parte di entrambe le parti
  - Errori dovuti a interpretazione errata di risultati di strumenti forensi (attenzione nell'interpretazione di report dubbi o contrastanti, es. SMS cancellati o no, file cancellati, etc…)
  - Errori dovuti a risultati errati prodotti da strumenti forensi (bug, mancato aggiornamento, utilizzo su sistemi non compatibili)
  - Forzature interpretative (es. accesso a 10 file su server → copia intero database aziendale)

Alcune fonti di prova

1. PC, dischi, pendrive, smartphone, caselle di posta, cloud
2. IDS/IPS, Proxy, VPN, Router, Firewall, Antivirus
3. Log applicativi, Log di Sistema (PC e Server)
4. Server/relay DNS e DHCP
5. Server di posta
6. Directory Server
7. Sistema gestione log (SIEM)
   - Raccolta
   - Parsing
   - Correlazione
   - Analisi Allarme
   - Storicizzazione Tamper Proof

Modalità operative

- Acquisizione (con firma digitale, hash e documentazione continua)
  - Identificazione del perimetro e isolamento dei sistemi
  - Copia forense dei sistemi
  - Eventuale Dump di rete
  - Live Forensics, Data Recovery, eDiscovery
  - Avvio procedure per recupero log da SIEM
- Analisi:
  - Log
  - Copie forensi
  - Dati live
- Obiettivi da identificare con ricostruzione temporale:
  - Modalità di esecuzione del reato
  - Informazioni temporali (inizio, fine, etc…)
  - Entità dell'utilizzo dei sistemi informatici

Modalità operative

- Strumenti hardware
  - Write Blocker
  - Copiatori forensi
- Strumenti software
  - TSURUGI, DEFT, CAINE, PALADIN, Raptor, SIFT
  - FTK, X-Ways, Axiom
  - Risorse varie
- Servizi
  - Timestamp digitale
  - AWS, Cloud
  - Decryption, Rainbow Table

Grazie per l'attenzione!

Per eventuali domande o riferimenti:

Paolo Dal Checco, Consulente Informatico Forense

www.dalchecco.it / paolo@dalchecco.it