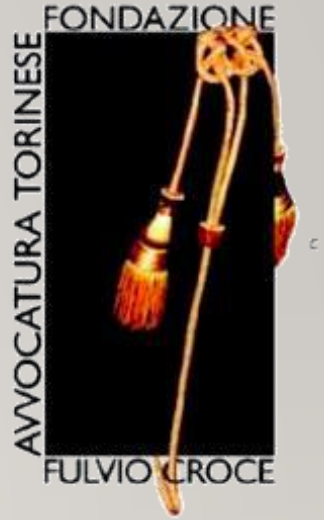
Ordine Avvocati di Torino, Commissione Informatica
In Collaborazione con Fondazione Fulvio Croce



LA PROVA INFORMATICA NEI PROCESSI CIVILI E PENALI RIFORMATI, IL DOVERE DI VERITA' DELL'AVVOCATO

10 ERRORI INFORMATICI FORENSI DA CUI IMPARARE

Paolo Dal Checco, Consulente Informatico Forense
Forenser Srl

Forenser Digital Investigations

CHI SONO

- Laurea e Ph.D. in Informatica, Università di Torino
- Consulente Informatico Forense (10+ anni, 2k+ casi)
- CTP, CTU, Esperto, Perito del Giudice, CT del PM, Ausiliario di PG
- Collaborazioni con UniTO (Docente a Contratto corso Sicurezza Informatica @SUISS), UniGE (Master), UniMI e PoliMI (Master e Corsi di Perfezionamento)
- Interessi in mobile forensics, OSINT, cryptocurrency forensics, web forensics…. in sostanza tutti gli aspetti della digital forensics

LA PROVA INFORMATICA

- Informatica Forense e Legge s'intrecciano quando si ha a che fare con le «prove»
- Informazione o dato che viene raccolto, conservato e presentato attraverso mezzi tecnologici o meno per essere utilizzato come evidenza in un procedimento legale
- Importante che legale e consulente riescano a dialogare e ognuno comprenda il linguaggio dell'altro
- Difficile creare un linguaggio comune, ma possiamo intanto partire dagli errori più frequenti per cercare di costruirne uno

1° ERRORE: NON RACCOGLIERE QUANTO UTILE ALLA CAUSA

- Dedicare tempo alla fase d'identificazione («abbiamo raccolto e documentato tutto ciò che serve o potrà servire?»)
- Potrebbe essere troppo tardi farlo dopo
  - Chat o file cancellati
  - Pagine/post/tweet rimossi dal web
  - Dischi persi, danneggiati, sistemi reinstallati
  - Log sovrascritti o retention superata (es. log posta MS. 365, 2 anni per tabulati voce, etc…)
  - Servizi (es. server, hosting, cloud, etc…) o domini chiusi o non rinnovati

2° ERRORE: NON DEPOSITARE QUANTO UTILE ALLA CAUSA

- In particolare in ambito di cause civili, anche se osservo cambiamenti nella giurisprudenza (Cassazione civile sez. un. - 01/02/2022, n. 3086) ma è meglio non fidarsi…
- Se l'acquisizione non è stata fatta «bene» (hash che non quadra, mancata data certa, etc…) potrebbe essere contestata in seguito a un deposito tardivo
  - es. hard disk di dipendente acquisito il giorno della fuoriuscita ma depositato anni dopo
- I dati o le copie possono andare perse se non depositate subito
- Attenzione agli **allegati digitali alle relazioni** («non li ho depositati perché **non rientravano come dimensione nel deposito PCT**»
- Se per scelta **si decide volontariamente** di non produrre qualcosa, valutare se produrlo comunque cifrato, secretato (es. ex Art. 121 ter CPI), etc…

3° ERRORE: UTILIZZARE SUPPORTI NON DUREVOLI

- Pendrive, CDROM, DVD non vanno bene
- Hard disk ok, meglio **due copie**
  - Prima copia: USB 2.5 pollici
  - Seconda copia: naked Sata 2.5 pollici

3° ERRORE: UTILIZZARE SUPPORTI NON DUREVOLI

Processo Eternit, la chiavetta usb è vuota: la sentenza è rimandata

Nel device era custodito il novanta per cento degli atti. I giudici: "Siamo mortificati"

Una società di archiviazione dati avverte: 'salvataggio su HDD degli anni '90? I dati potrebbero essere persi'

La società specializzata nell'archiviazione dati Iron Mountain ha spiegato che gli hard disk obsoleti non sono affidabili, anche se lasciati inutilizzati in un ambiente controllato. Alcune registrazioni originali dell'industria musicale sono perse per sempre.

di Vittorio Rienzo pubblicata il **16 Settembre 2024**, alle **17:52** nel canale STORAGE

Era l'inizio degli **anni '90** quando numerose etichette discografiche decisero di passare dal tradizionale e storico nastro magnetico agli **hard disk più compatti e rapidi da consultare**. Tuttavia, la società di archiviazione dati **Iron Mountain ha l'anciato l'allarme sull'inaffidabilità delle unità più vecchie**.

L'azienda ha pubblicato un resoconto sui suoi backup delle tracce registrate dagli studi musicali e, secondo quanto emerso, **il tasso di guasti raggiunge il 20%**. Tra i file archiviati non vi erano solo copie, ma **anche registrazioni originali che, inevitabilmente, sono state perse per sempre**.

4° ACQUISIZIONE NON (COMPLETAMENTE) FORENSE

- Un'acquisizione non forense, o anche parzialmente forense (es. acquisizione di una parte del tutto) potrebbe non consentire di provare l'autenticità dell'evidenza digitale
  - Es. file audio, foto, video estrapolato dall'ambiente in cui è stato prodotto
- Sempre acquisire il perimetro massimo possibile
  - Verbalizzare quanto viene svolto durante l'acquisizione
  - Se **il perimetro è eccessivo**, si può sempre non depositare il contenitore ma solo il contenuto

4° ACQUISIZIONE NON (COMPLETAMENTE) FORENSE

- Evitare stampe cartacee o pdf, di pagine web piuttosto utilizzare servizi web come:
    - Internet Web Archive (attenzione, i siti si possono rimuovere)
    - Perma.cc (10 snapshot gratuite)
    - Archive.is (gratuito ma pubblico)
    - Kopjra Web Forensics Instant (nato da poco ma promettente)
- Evitare stampa email o PEC in pdf, piuttosto:
    - Esportare file in formato EML/MSG (per le PEC, esportare EML esterno e non solo postacert.eml + daticert.eml)
    - Lasciare le mail sul server, non cancellarle né spostarle, se possibile

5° ERRORE: ACCORPARE LE EVIDENZE DIGITALI ACQUISITE

- Es. calcolo marca temporale di tutte le evidenze insieme
- Non sarà poi possibile scorporarle in base alla strategia difensiva

6° ERRORI NELLA CATENA DI CUSTODIA

- Catena di custodia: insieme della documentazione che traccia un reperto dal momento in cui viene identificato alla sua acquisizione e poi analisi
- Tutto deve essere lineare e collegato, ogni reperto va correttamente identificato e delineato all'interno del perimetro, non devono esserci «salti»
- Es: copia forense eseguita correttamente + analisi eseguita su dati non acquisiti in maniera forense o ricevuti direttamente dal cliente (si può fare ma va comunque verificato che siano derivati dalla copia forense)

7° ALTERAZIONE DELLE PROVE

- **Involontaria** (almeno si spera) modifica delle evidenze digitali prima dell'acquisizione o del deposito
- Alcuni esempi:
  - collegare pendrive e aprire file
  - cancellare o spostare email
  - salvare l'interno della PEC e non il contenitore
  - Il consulente accede a un disco prima di farne copia forense
  - copie forensi eseguite ex art 359 ma con alterazione dati
  - inserimento o modifica di email in una mailbox

8° TROPPA FIDUCIA NEL CLIENTE

- Verificare sempre, per quanto possibile, i dati ricevuti dai clienti
- Verificare se esistono su web, smartphone, social, etc..
- Se non esistono, verificare se vi sono tracce (es. Internet Archive) o acquisizioni forensi
- Se sono stati appena rimossi, si può fare in tempo a recuperarli (es. Internet Archive, Cache dei motori di ricerca, Sitemap, etc…)

9° ERRATA INTERPRETAZIONE DEI DATI

- Dati acquisiti correttamente ma interpretati in maniera errata
- Consigliabile utilizzare più strumenti, alcuni danno **falsi positivi** o **falsi negativi**
- Non arrivare a conclusioni errate: es. consulente che riferisce che un file è criptato perché non legge il contenuto
- Valutare con il consulente l'entità delle conclusioni tratte: es. «è stata inserita dall'ex dipendente una pendrive USB» può diventare «l'ex dipendente ha sottratto i dati»

10° FUORIUSCITA DAL PERIMETRO DI ATTIVITÀ FORENSE

- Evitare – soprattutto per i consulenti tecnici – di uscire dal perimetro del conferimento incarico
- Es. incarico acquisire contenuti smartphone, il consulente acquisisce il cloud
- Es. mancata verifica della titolarità del dispositivo acquisito, etc…
- Particolarmente grave (o utile per la difesa) quando il CT è del PM, Giudice

GRAZIE PER L'ATTENZIONE

Per domande o chiarimenti mi trovate online! ☺