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

LE INVESTIGAZIONI DIGITALI

GLI STRUMENTI DI CUI PUÒ DISPORRE IL DIFENSORE E IL LORO UTILIZZO

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

ARGOMENTI DELLA PRIMA PARTE DEL CORSO

- Princìpi e metodologie dell'informatica forense
- L'accesso ai dati contenuti su pendrive e hard disk senza compromettere l'integrità del mezzo di prova
- La copia forense di PC, pendrive, dischi: come produrla, verificarne l'integrità e visionarne il contenuto

PRINCIPI D'INFORMATICA FORENSE

Convenzione di Budapest

- La Convenzione, che risale al 23 novembre 2001, suggerisce agli stati membri del Council of Europe alcuni princìpi cui ispirarsi nella disciplina sanzionatoria del fenomeno dei reati informatici

- L'idea è di uniformarsi introducendo un minimum target di tutela dei beni giuridici offesi dai cybercrimes e un livello minimo essenziale comune di strategie di contrasto a tali illeciti, adottando legislazioni appropriate e promuovendo la cooperazione internazionale.

- Gli stati membri hanno firmato e ratificato in momenti diversi, il fine è armonizzare e uniformare le normative

PRINCIPI D'INFORMATICA FORENSE

Convenzione di Budapest

- 23 novembre 2001, suggerisce agli stati membri del Council of Europe alcuni **prinicìpi cui ispirarsi nella disciplina sanzionatoria del fenomeno dei reati informatici**
- L'idea è di uniformarsi introducendo un **linguaggio comune per la tutela dei beni giuridici offesi dai cybercrimes** e un livello minimo essenziale comune di strategie di contrasto a tali illeciti, adottando legislazioni appropriate e promuovendo la **cooperazione internazionale**
- Gli stati membri hanno **firmato e ratificato** in momenti diversi

Titolo	**Convenzione sulla criminalità informatica (STE no. 185)**
Riferimento	**STE n° 185**
Apertura del trattato	**Budapest 23/11/2001 - Trattato aperto alla firma degli Stati membri e degli Stati non membri i quali hanno participato alla sua elaborazione e all'adesione degli altri Stati non membri**
Entrata in vigore	**01/07/2004 (5 Ratifiche inclusi almeno 3 Stati membri del Consiglio d'Europa.)**
Riassunto	La Convenzione è il primo trattato internazionale sulle infrazioni penali commesse via internet e su altre reti informatiche, e tratta in particolare le violazioni dei diritti d'autore, la frode informatica, la pornografia infantile e le violazioni della sicurezza della rete. Contiene inoltre una serie di misure e procedure appropriate, quali la perquisizione dei sistemi di reti informatiche e l'intercettazione dei dati. Il suo obiettivo principale, enunciato nel preambolo, è perseguire una politica penale comune per la protezione della società contro la cibercriminalità, in special modo adottando legislazioni appropriate e promuovendo la cooperazione internazionale.
Testi ufficiali	English Français
Testi DE, IT, RU	Tedesco Russo
Link correlati	• Firme e ratifiche • Riserve et Dichiarazioni • Protocolli

https://www.coe.int/it/web/conventions/full-list?module=treaty-detail&treatynum=185

PRINCIPI D'INFORMATICA FORENSE

Convenzione di Budapest

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

European Treaty Series - No. 185

Convention on Cybercrime

Budapest, 23.XI.2001

Article 16 – Expedited preservation of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

https://rm.coe.int/1680081561

PRINCIPI D'INFORMATICA FORENSE

Legge 48 del 2008

- 18 marzo 2008, quasi 7 anni dopo la convenzione di Budapest
- "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"
- Importante per le modifiche introdotte nel Codice di Procedura Penale
- Causa l'introduzione dell'Art. 24 bis nel D.lgs 231/2001
- Causa a sua volta aggiornamento del MOG introducendo una nuova Parte Speciale

Titolo	**Convenzione sulla criminalità informatica (STE no. 185)**
Riferimento	**STE n° 185**
Apertura del trattato	**Budapest 23/11/2001 - Trattato aperto alla firma degli Stati membri e degli Stati non membri i quali hanno participato alla sua elaborazione e all'adesione degli altri Stati non membri**
Entrata in vigore	**01/07/2004 (5 Ratifiche inclusi almeno 3 Stati membri del Consiglio d'Europa.)**
Riassunto	La Convenzione è il primo trattato internazionale sulle infrazioni penali commesse via internet e su altre reti informatiche, e tratta in particolare le violazioni dei diritti d'autore, la frode informatica, la pornografia infantile e le violazioni della sicurezza della rete. Contiene inoltre una serie di misure e procedure appropriate, quali la perquisizione dei sistemi di reti informatiche e l'intercettazione dei dati. Il suo obiettivo principale, enunciato nel preambolo, è perseguire una politica penale comune per la protezione della società contro la cibercriminalità, in special modo adottando legislazioni appropriate e promuovendo la cooperazione internazionale.
Testi ufficiali	English Français
Testi DE, IT, RU	Tedesco Russo
Link correlati	• Firme e ratifiche • Riserve et Dichiarazioni • Protocolli

https://www.coe.int/it/web/conventions/full-list?module=treaty-detail&treatynum=185

PRINCIPI D'INFORMATICA FORENSE

Legge 48 del 2008

- La legge pone forte accezione sull'adottare "*misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione*", eseguire acquisizioni che avvengano "*mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità*" e "*custodire i reperti con l'obbligo di impedirne l'alterazione o l'accesso da parte di terzi, salva, in quest'ultimo caso, diversa disposizione dell'autorità giudiziaria*".
- Modifiche di rilievo:
  - Art. 244 CPP "Casi e forme delle ispezioni"
  - Art. 247 CPP "Casi e forme delle perquisizioni"
  - Art. 254-bis: Sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni
  - Art. 259 CPP "Custodia delle cose sequestrate" Art. 260 "Apposizione dei sigilli alle cose sequestrate. Cose deperibili"
  - Art. 352 Perquisizioni
  - Art. 354 - Accertamenti urgenti sui luoghi, sulle cose e sulle persone. Sequestro

PRINCIPI D'INFORMATICA FORENSE

Legge 48 del 2008

- I tre punti chiave per l'informatica forense che emergono dalla Legge 48/2008 sono:

1. Lasciare inalterato l'originale (→ write blocker, copia forense) [attenzione a Mac OS e USB]
2. Copia identica all'originale (→ valori hash)
3. Copia inalterabile nel tempo (→ supporti, valori hash, marca temporale, firma digitale)

PRINCIPI D'INFORMATICA FORENSE

ISO 27037

- "Guidelines for identification, collection, acquisition and preservation of digital evidence"
- La ISO/IEC 27037:2012 si limita alle fasi iniziali del processo di gestione della prova informatica, non arriva all'analisi, non si occupa di aspetti legali, strumenti, reportistica, trattamento dei dati
- Integrità della prova informatica e metodologia al fine di rendere ammissibile la prova in Giudizio
- Si occupa di trattamento del reperto informatico e identifica 4 fasi:

    - 1) Identificazione (ispezione),
    - 2) Raccolta (sequestro)
    - 3) Acquisizione (copia o sequestro virtuale)
    - 4) Conservazione (conservazione e sigillo)

PRINCIPI D'INFORMATICA FORENSE

Catena di Custodia

- Descrivere il **ciclo di vita** del reperto fino a diventare copia forense;
- Valori **Hash**: identificano il contenuto
  - MD5, SHA1, SHA256, etc… se possible calcolarne due, ma anche uno solo basta
  - Nirsoft HashMyFiles: https://www.nirsoft.net/utils/hash_my_files.html
- **Marca Temporale**: identifica il tempo (e il contenuto)
  - Marca Temporale del Certificatore: pdf, m7m, tsd, tsr, tst
  - Blockchain (https//opentimestamps.org)
  - PEC
- **Firma Digitale**: identifica l'autore
  - Facoltativa, può aggiungere un riferimento a chi ha eseguito le attività o quantomeno l'ultima

ACCESSO AI CONTENUTI DEI SUPPORTI

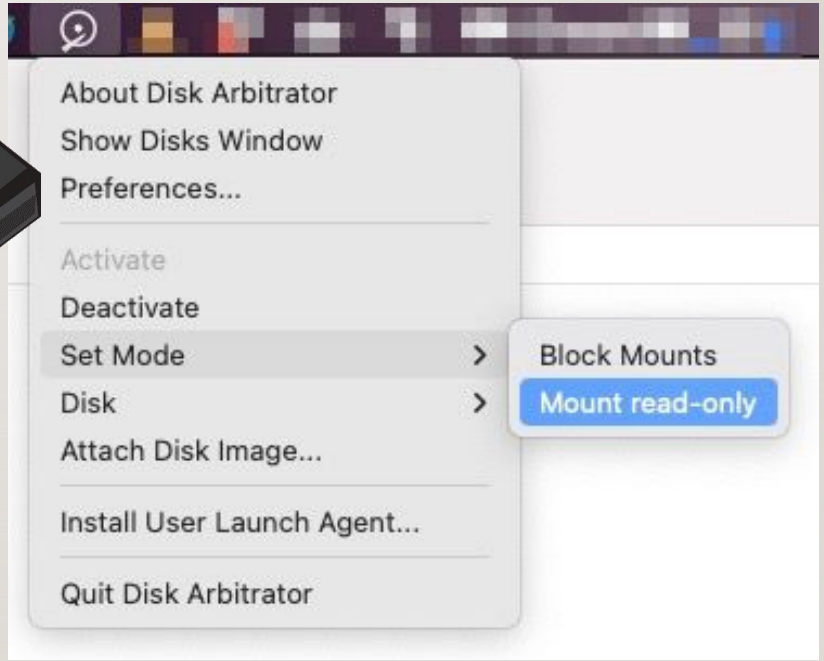
- Importante non alterare l'evidenza digitale durante la visione/triage (es. quando il cliente è dal legale)
- Non sempre possibile (es. dischi non rimovibili) ma su pendrive e hard disk in genere è fattibile
- Diverse soluzioni: write blocker hardware (€ 300-600) Vs write blocker software (gratis)

ACCESSO AI CONTENUTI DEI SUPPORTI: HANDS ON

- Utilizziamo il software «USB Write Protector» o «Disk Arbitrator» su Mac OS per mettere in blocco scrittura le porte USB (**verificare sempre con un altro dispositivo se possibile identico che il blocco sia attivo**)

ACCESSO AI CONTENUTI DEI SUPPORTI: HANDS ON

- Windows: **GaiJin USB WriteProtector** (https://www.gaijin.at/en/software/usbwriteprotector)
- Mac OS: **Disk Arbitrator** (https://github.com/aburgh/Disk-Arbitrator/releases)

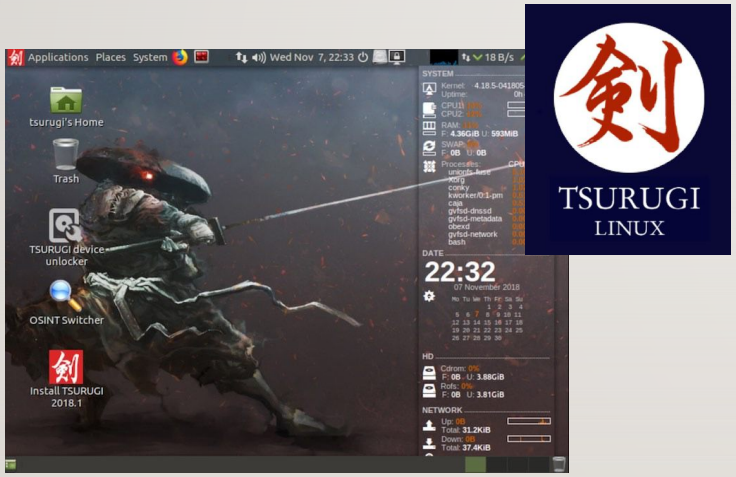


COPIA FORENSE PENDRIVE O HARD DISK

- Il punto è eseguire una copia che rispetti i princìpi derivati dalla Legge 48/2008 e dalla ISO 27037
- Diverse soluzioni per copiare hard disk o pendrive: Copiatore forense (€ 1000-5000), Write blocker hardware + software (€ 300-600) oppure Write blocker software + applicativo (gratis)

COPIA FORENSE PENDRIVE O HARD DISK: HANDS ON

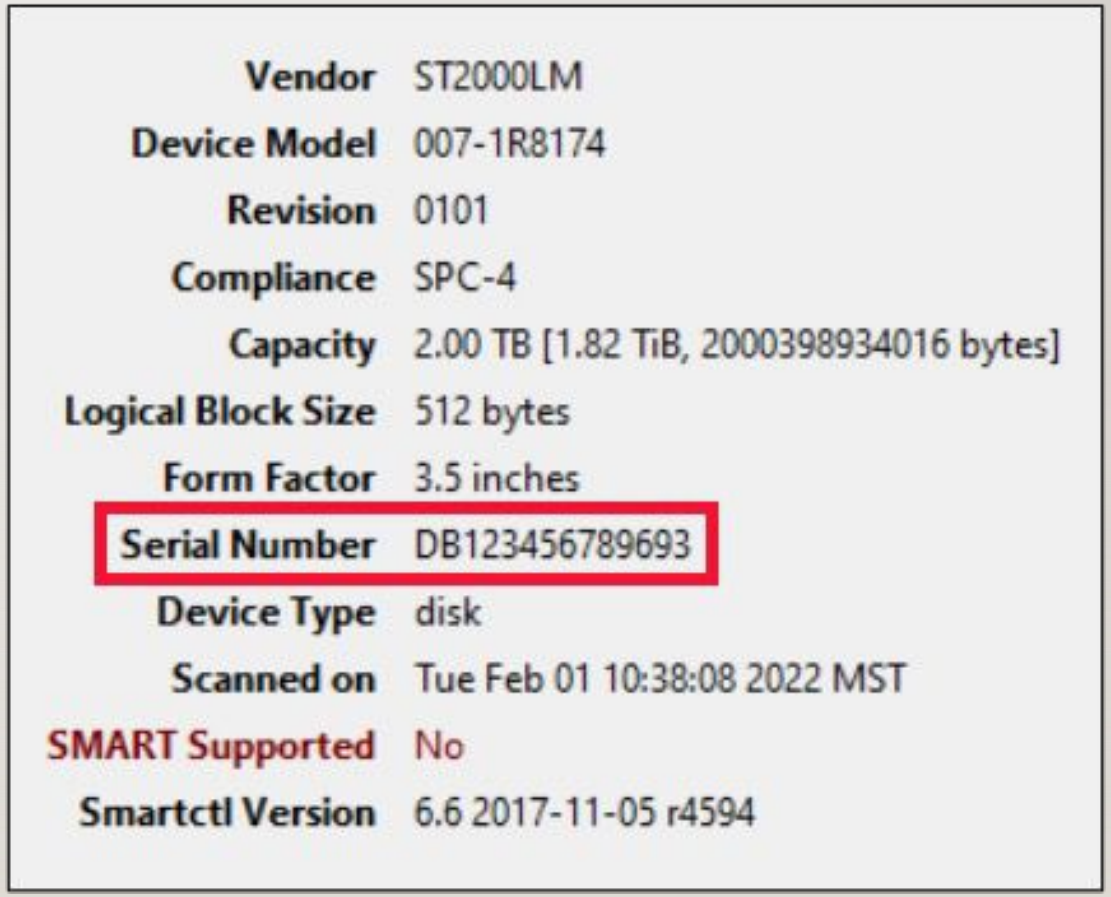
- Copia tramite software di blocco da scrittura gratuito e software di copia gratuito
- Due alternative: sistema Linux live (ottimo ma complicato) oppure applicativo per Windows/MacOS



- GaiJin USB WriteProtector: https://www.gaijin.at/en/software/usbwriteprotector [**FARE PRIMA PROVA**]
- Exterro FTK Imager: https://www.exterro.com/ftk-imager

COPIA FORENSE PENDRIVE O HARD DISK: HANDS ON

- Attenzione a identificare sempre in maniera fotografica e tramite documentazione dei seriali ciò che si acquisisce (pendrive, hard disk, etc…) che **devono corrispondere con quelli ricavati via software**
- Ricordare che pendrive e hard disk hanno due seriali: HW Serial Number (fisso) e Volume ID (variabile)
- Verbalizzare anche seriali di container (enclosure, PC, etc…)
- Con FTK Imamger si esegue una copia forense di una pendrive, scegliendo il formato EWF oppure RAW che andrà a finire nel file «pendrive.ad1»
- Il software produce un report «pendrive.ad1.txt» contenente i dati di copia e i valori hash



Vendor	ST2000LM
Device Model	007-1R8174
Revision	0101
Compliance	SPC-4
Capacity	2.00 TB [1.82 TiB, 2000398934016 bytes]
Logical Block Size	512 bytes
Form Factor	3.5 inches
Serial Number	DB123456789693
Device Type	disk
Scanned on	Tue Feb 01 10:38:08 2022 MST
SMART Supported	No
Smartctl Version	6.6 2017-11-05 r4594

COPIA FORENSE PENDRIVE O HARD DISK: HANDS ON

- Calcolare hash del report di copia
- Applicare marca temporale (eventualmente anche firma digitale) al report di copia (attenzione poi a non modificarlo)
  - File Protector/Dike (https://www.card.infocamere.it/infocard/pub/download-software_5543)
  - https://opentimestamps.org/
  - Invio via PEC del report/hash
- Riportare marca temporale sul verbale o cmq insieme alla copia

```
Created By AccessData® FTK® Imager 3.1.1.8

Case Information:
Acquired using: ADI3.1.1.8
Case Number: OdA Test
Evidence Number: Test prodotto durante la lezione per OdA Torino
Unique Description: Pendrive di Prova
Examiner: Paolo Dal Checco
Notes: Dispositivo cquisito durante la lezione

---------------------------------------------------------------

Information for C:\Users\Administrator\Desktop\pendrive.ad1:
[Custom Content Sources]
 \\.\PHYSICALDRIVE0:Partition 2 [238338MB]:NONAME [NTFS]|[root]|
[Computed Hashes]
 MD5 checksum:    02debcd6f96c15532e5a72975437017b
 SHA1 checksum:   5376f35cbca2b5f190c7eebdf15aa03ce5908643

Image information:
 Acquisition started:   Wed Feb 06 14:42:36 2023
 Acquisition finished:  Wed Feb 06 14:44:22 2023
 Segment list:
  C:\Users\Administrator\Desktop\pendrive.ad1

Image Verification Results:
 Verification started:  Wed Feb 06 14:44:22 2023
 Verification finished: Wed Feb 06 14:44:30 2023
 MD5 checksum:    02debcd6f96c15532e5a72975437017b : verified
 SHA1 checksum:   5376f35cbca2b5f190c7eebdf15aa03ce5908643 : verified
```

CONCLUSIONI

- **Princìpi dell'informatica forense:** non alterare le prove, acquisire copia identica all'originale con catena di custodia documentata, produrre un'evidenza «cristallizzata» immodificabile e datata nel tempo
- **Accesso a dispositivi di memoria**: non sempre possibile, ove possibile va fatto senza alterare l'originale, con software appositi che permettano la visione senza l'alterazione del dato
- **Copie forensi**: produce una copia identica all'originale, che rispetti le indicazioni presenti nella Legge 48/2008 e nella ISO 27037 (in sostanza, i punti precedenti)