

La Copia Forense

DOTT. ROBERTO ROCCHETTI
ROCCHETTI@ALICEGROUP.COM

Articolo 360 c.p.p ed il concetto di irripetibilità

L'art. 360 c.p.p. precisa invece che “quando gli accertamenti previsti dall'art. 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”.

Nota: non tutte le copie forensi avvengono nel contesto dell'articolo 360 c.p.p. e sono caratterizzate da tale vincolo vincolo

La copia Forense secondo la Cassazione

Secondo giurisprudenza consolidata la copia forense digitale **non può considerarsi atto irripetibile** (sez. I 25.2.2009 n. 11503, sez. I 5.3.2009 n. 14511).

La Cassazione ha affermato che una attività di questo tipo non comporta alcuna attività di carattere valutativo su base tecnico scientifica né determina alcuna alterazione dello stato delle cose.

- Nell'eseguire la copia dei dati sarà tuttavia necessario adottare delle precauzioni, cioè misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immutabilità" (come prescritto dalla Legge 48/2008, ratifica convenzione Budapest 23/11/2001).

Terminologia

Copia Forense o Immagine Forense?

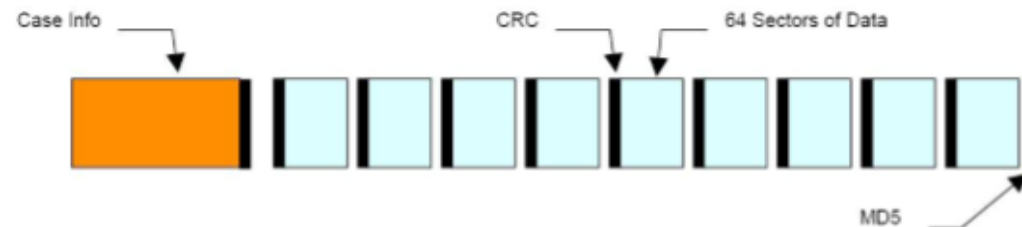
La Copia forense è il risultato della duplicazione di una memoria digitale avvenuto nel rispetto della normativa vigente e delle buone pratiche scientifiche

- Copia orientata al device Fisico (orientata alla copia sequenziale di aree fisiche, (Settori HDD, SSD, ecct)
- Copia orientata alle partizioni Logiche (File System)

Formati comuni

AD1 (folder forensics copy)

E01 (Guidance Software's EnCase Forensic File Format, proprietary, standard de facto, .E0nn, compression, Case Metadata, based on ASR Data's Expert Witness Compression Format)



RAW (DD; bit per bit, .dd, No compression, no forensics case metadata)

SMART (by ASR data)

AFF (advance forensic image, Harvard University, open, extensible, Case metadata, consume less)

Ilook, ProDiscover, RAID, SafeBAck, Sdi32...

Legge 48-2008

Capo III. MODIFICHE AL CODICE DI PROCEDURA PENALE E AL CODICE DI I CUI AL DECRETO LEGISLATIVO 30 GIUGNO 2003, N. 196.

articolo 8

...omissis...

7. All'articolo 259, comma 2, del codice di procedura penale, dopo il primo periodo è inserito il seguente: «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».

8. All'articolo 260 del codice di procedura penale sono apportate le seguenti modificazioni:

a) al comma 1, dopo le parole: «con altro mezzo» sono inserite le seguenti: «, anche di carattere elettronico o informatico,»;

b) al comma 2 è aggiunto, in fine, il seguente periodo: «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**; in tali casi, la custodia degli originali può essere disposta anche in luoghi diversi dalla cancelleria o dalla segreteria».

Software per copie forensi

Per HDD, dvd, cd, flash drive, Sd card

- Ftk imager
- X-Ways Forensics
- Encase
- Linus CAINE / Guymager

Per Smartphone, tablet, cellulari tradizionali

- UFED
- MobilEdit
- Oxygen
- Lantern
- XRY

FTK IMAGER

Accessdata Group LLC

File Systems

The following table lists AccessData Imager-identified and analyzed file systems:

TABLE A-1 Identified and Analyzed File Systems

• FAT 12, FAT 16, FAT 32	• NTFS
• Ext2FS	• HFS
• Ext3FS	• HFS+
• Ext4FS	• CDFS
• ReiserFS3	• VXFS
• exFAT	

GUYMAGER

Imager tool in Linux CAINE. CAINE (Computer Aided INvestigative Environment) is an Italian GNU/Linux live distribution created as a Digital Forensics project. Currently the project manager is Nanni Bassetti (Bari - Italy).

Boot da usb flash drive, Si può installare in RAM

“The important news is that CAINE 8.0 and 7.0 block all the block devices (e.g. /dev/sda), in Read-Only mode. You can use a tool with a GUI named BlockON/OFF present on Caine's Desktop. This new write-blocking method assures all disks are really **preserved from accidentally writing** operations, because they are locked in Read-Only mode. If you need to write a disk, you can unlock it with BlockOn/Off or using "Mounter" changing the policy in writable mode. “ <https://www.caine-live.net/page8/page8.html>

Hardware write block

Write Block Tool - T4 Forensic **SCSI** Bridge (USB Interface)

Write Block Tool - Tableau T8 Forensic **USB** Bridge (FireWire Interface)

Write Block Tool - FastBloc **FE** (FireWire Interface)

Write Block Tool - Tableau T5 Forensic **IDE** Bridge (FireWire Interface)

Write Block Tool - Tableau Forensic **SATA** Bridge T3u

ALTRI

Software Write Block

Windows Registry Regedit

CAINE (block tools)

Apple Thunderbolt Cable + target disk mode boot

Impronta digitale (Hash value)

Requisiti della copia forense

- **conformità della copia all'originale:** uguaglianza tra i dati del dispositivo originale e della copia forense
- **Immodificabilità:** Deve essere possibile verificare nel tempo se sono state effettuate modifiche o sopraggiunte alterazioni ai dati della copia forense.
- **Conformità all'originale + Immodificabilità-> Ammissibilità in Tribunale**

Soluzione:

- Calcolo della impronta digitale (una o due) con tecnica matematica Hash
- Il valore Hash permette di verificare in qualsiasi momento se una evidenza digitale è la copia esatta dell'originale da cui è stata estratta
- SHA1 o SHA256
- I principali tool di imaging attivano la funzione di Hash per default

HASH VALUE DISCORDANTI

COSA SUCCEDE SE IL MEDIA SI DETERIORA E LA RIPETIZIONE DELLA COPIA FORNISCE UN HASH DIFFERENTE DA QUELLO INDICATO DAL CONSULENTE TECNICO NELLA PERIZIA?

QUALI CONTROMISURE?

DEMO IMMAGINE FORENSE

FTK IMAGER+FLASH DRIVE

DISCO DI DESTINAZIONE

USB SW WRITE LOCK

E01

HASH

FILE LIST

DEMO MOBILEEDIT

Copia forense di uno smartphone in tecnica classica

- Sblocco
- Configurazione apparato
- Connessione
- Identificazione
- Autorizzazione
- Estrazione (inserimento metadati e opzioni)
- Produzione Report
- Analisi Log, RIPETIZIONE?
- DUPLICAZIONE (ERROR LONG PATHNAME...)

FINE

GRAZIE PER IL GENTILE ASCOLTO.

_

ROBERTO ROCCHETTI

rocchetti@alicegroup.com