

CScorza

BEST PRACTICES DI DIGITAL FORENSICS

Trattamento della prova digitale durante
l'Identificazione e il Repertamento

BEST PRACTICES DI DIGITAL FORENSICS

Testo scritto e prodotto da **CScorza**

Anno di pubblicazione 2023

Contatti

Linkedin - <https://www.linkedin.com/in/cscorza/>

Telegram – https://t.me/+kP_uYlc6-345Njc8

👤 CScorza - Indagini Telematiche "Canale Pubblico"

Github - <https://github.com/CScorza>

Gli articoli di questo libro sono ad accesso aperto e distribuiti sotto Creative Licenza Commons Attribution (CC BY), che consente agli utenti di scaricare, copiare e sviluppare articoli pubblicati, purché l'autore e l'editore siano adeguatamente accreditati, il che garantisce il massimo diffusione e un più ampio impatto delle nostre pubblicazioni



INDICE

- INTRODUZIONE
- LA DIGITAL EVIDENCE
- PASSI OPERATIVI
 - IDENTIFICAZIONE E REPERTAMENTO
 - REPERTAMENTO POST MORTEM
 - REPERTAMENTO LIVE
 - CATENA DI CUSTODIA
 - ANALISI
 - DATA CARVING
 - ACQUISIZIONE PAGINA WEB
 - FIRMA DIGITALE – “HASH”
- L'ACQUISIZIONE DELLA PROVA
LA POLIZIA GIUDIZIARIA CODICE DI PROCEDURA PENALE ED ALTRE LEGGI
- STRUMENTI OPEN SOURCE PER LA DIGITAL FORENSICS
- MOBILE FORENSICS
- LINEE GUIDA
- ALLEGATI
(VERBALE DI REPERTAMENTO E PERQUISIZIONE DI MATERIALE INFORMATICO)
- BIBLIOGRAFIA

INTRODUZIONE

Questo testo, non vuole essere un manuale di Digital Forensics, ma una linea guida per tutte quelle persone che si stanno affacciando per motivi di lavoro o di studio, alla materia. Ma anche un supporto per i più esperti e navigati del settore.

Questo testo fa parte di una più grande raccolta di strumenti da me raccolti e presenti nel profilo GitHub CScorza¹.

Il mondo digitale ci accompagna in ogni settore della nostra vita, dagli smartphone, ai pc, alla domotica in casa o negli uffici. Tutti questi strumenti sono ricchi di informazioni che possono essere utili ed usati per ricostruire eventi che interessano la sfera giudiziale. Per questo è importante conoscere le linee guida essenziali, ai fini del mantenimento dell'indizio che poi diventa prova in sede dibattimentale.

Ma iniziamo con le prime due domande:

Cos'è la Digital Forensics (Informatica Forense)

La Digital Forensics, anche conosciuta come Informatica Forense, è la pratica di analizzare, identificare, raccogliere, preservare e analizzare le prove digitali (ad esempio file, registri, e-mail, chat, foto, video) per risolvere crimini informatici o altri problemi legali e di sicurezza.

Questo campo è particolarmente importante in un'epoca in cui la tecnologia digitale è sempre più presente nella vita quotidiana e spesso costituisce una parte essenziale delle prove in casi di reati informatici, frodi informatiche, violazioni della sicurezza informatica, diffamazione online, stalking, e altri reati.

La Digital Forensics può essere utilizzata anche per recuperare dati persi o danneggiati e per effettuare controlli interni in un'organizzazione per individuare comportamenti fraudolenti o impropri da parte di dipendenti. Gli specialisti di Digital Forensics utilizzano strumenti software specializzati nel raccogliere e analizzare le prove digitali in modo da preservare l'integrità delle prove e assicurarsi che le informazioni raccolte siano valide dal punto di vista legale

La Digital Evidence

La Digital Evidence (o prova digitale) si riferisce alle informazioni e ai dati di natura digitale che possono essere utilizzati come prove in un procedimento legale. Questo tipo di prove possono includere file, documenti, e-mail, chat, foto, video, messaggi di testo, registri delle attività, dati di navigazione e altri dati elettronici.

La Digital Evidence è diventata sempre più importante negli ultimi anni, in quanto sempre più informazioni sono create e conservate in formato digitale, rendendo le prove digitali sempre più comuni nei procedimenti giudiziari.

La Digital Evidence può essere raccolta attraverso tecniche di Digital Forensics, che utilizzano strumenti software specializzati per raccogliere e analizzare le prove digitali in modo che siano valide dal punto di vista legale.

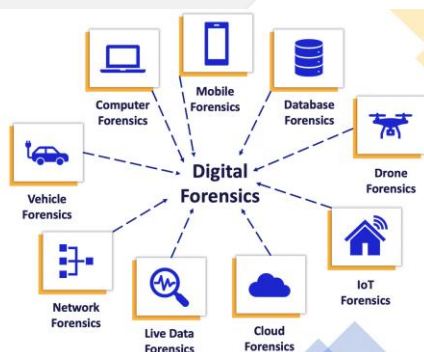
È importante notare che la Digital Evidence può essere facilmente manipolata o alterata, il che rende fondamentale la preservazione dell'integrità delle prove digitali durante la raccolta e l'analisi, così da assicurarsi che siano accettabili dal punto di vista legale. Inoltre, la Digital Evidence deve essere gestita in modo da rispettare le leggi sulla privacy e le normative sulla protezione dei dati personali.

¹ <https://github.com/CScorza/>

LA DIGITAL EVIDENCE

Si divide in:

- **Digital Device Evidence:** questa categoria include le prove digitali provenienti dai dispositivi elettronici, come computer, smartphone, tablet, dispositivi di archiviazione, telecamere di sicurezza, ecc.
- **Digital Communications Evidence:** questa categoria include le prove digitali provenienti dalle comunicazioni digitali, come e-mail, chat, messaggi di testo, social media, applicazioni di messaggistica istantanea, ecc.
- **Digital Media Evidence:** questa categoria include le prove digitali provenienti da diversi tipi di media digitali, come foto, video, audio, presentazioni, documenti, file PDF, ecc.
- **Network Evidence:** questa categoria include le prove digitali provenienti dalle attività di rete, come i registri degli accessi, le attività di navigazione, le attività di download, le attività di upload, ecc.
- **Cloud Evidence:** questa categoria include le prove digitali provenienti dai servizi cloud, come le attività di archiviazione, le attività di condivisione, le attività di sincronizzazione, ecc.
- **App Evidence:** questa categoria include le prove digitali provenienti dalle applicazioni software, come i registri delle attività dell'applicazione, le conversazioni, le attività di geolocalizzazione, ecc.
- **Internet of Things (IoT) Evidence:** questa categoria include le prove digitali provenienti da dispositivi IoT, come i dispositivi di monitoraggio della salute, le telecamere intelligenti, i dispositivi di casa intelligente, ecc.



FORMOBILE Mobile Forensics Fundamentals and Best Practices Training

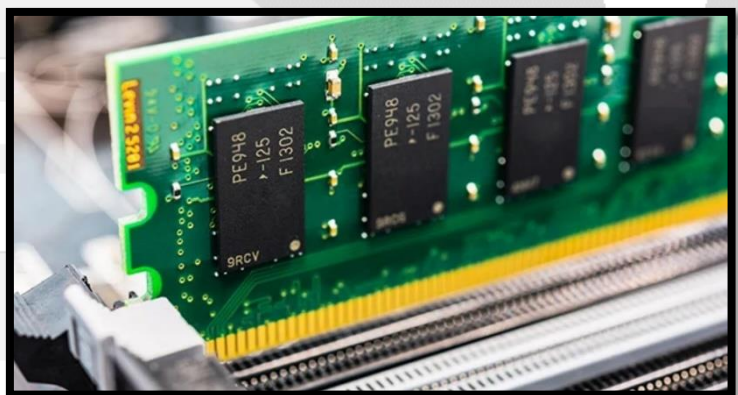
Una Digital Evidence è fragile per natura, perché è facilmente modificabile, manipolabile e distruttibile rispetto alle prove fisiche. Le prove digitali possono essere alterate involontariamente o intenzionalmente da vari fattori, come l'hardware o il software utilizzati, la configurazione del sistema, le attività di hacking o malware, e così via. Inoltre, le prove digitali sono altamente sensibili alle interferenze ambientali come la temperatura, l'umidità, le vibrazioni elettromagnetiche e i campi magnetici, che possono causare la perdita di dati. Inoltre:

- Quando il dispositivo che contiene le informazioni di interesse viene spento, i dati che non sono stati salvati possono andare persi definitivamente.
- Quando il dispositivo viene rivenuto spento, l'accensione comporta modifiche al sistema e/o ai dati in esso contenuti.
- Quando il dispositivo è connesso ad Internet o ad una rete aziendale, possono avvenire accessi dall'esterno con l'obiettivo di cancellare le informazioni.
- Quando la Digital Evidence si trova su Internet (sito web, profilo di social network, ecc.), può essere modificata e/o rimossa dall'OWNER della pagina.

I dati digitali possono essere divisi in due categorie:

1. Dati volatili: sono quei dati che possono essere persi o alterati quando il sistema informatico viene spento o si verifica un'interruzione di corrente. Questi includono:

- **Memoria RAM (Random Access Memory):** la memoria RAM è una memoria temporanea in cui i dati vengono elaborati e temporaneamente memorizzati mentre il sistema è in funzione. La memoria RAM è volatile, perché i dati in essa contenuti vengono persi quando il sistema viene spento.
- **Cache di dati e file temporanei:** molti software e sistemi operativi memorizzano temporaneamente i dati e i file in cache per accelerare il caricamento delle pagine web o delle applicazioni. Questi dati sono volatili, perché possono essere cancellati quando il sistema viene spento o quando viene svuotata la cache.
- **File di swap:** i file di swap sono utilizzati dal sistema operativo per gestire la memoria virtuale. Questi file sono volatili, perché vengono creati durante l'esecuzione del sistema operativo e possono essere cancellati quando il sistema viene spento.
- **Sessioni di accesso:** le sessioni di accesso sono i dati relativi alla connessione di un utente al sistema informatico, come ad esempio le credenziali di accesso e le attività svolte durante la sessione. Questi dati sono volatili, perché vengono persi quando l'utente termina la sessione o quando il sistema viene spento.
- **Informazioni di rete:** le informazioni relative alla configurazione della rete, come gli indirizzi IP, i log di connessione e i pacchetti di dati trasmessi, sono volatili, perché possono essere persi o sovrascritti quando il sistema viene spento o quando viene modificata la configurazione di rete.
- **Applicazioni aperte in uno Smartphone** (Come social network, app di hacking o altro)
- **Contenuto di una chat attiva.**

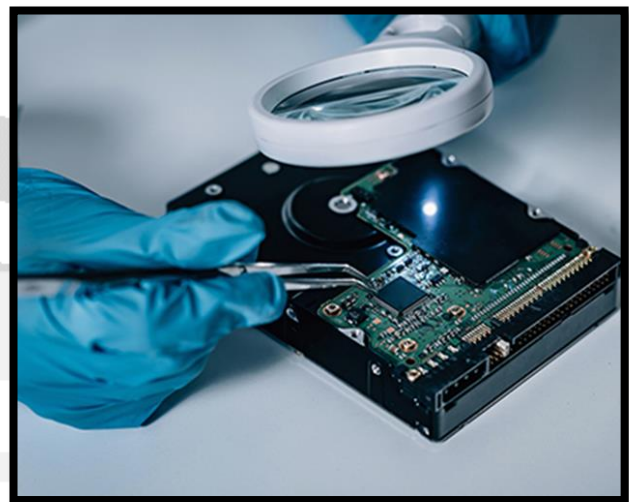


2. Dati non volatili: sono quei dati che possono essere recuperati anche dopo lo spegnimento del sistema informatico o la perdita di corrente elettrica. Questi dati includono:

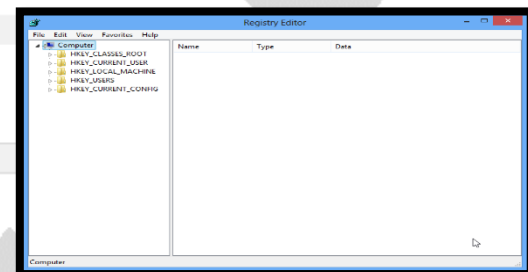
- **Disco rigido (Hard Disk Drive, HDD):** il disco rigido è il dispositivo di memorizzazione permanente più comune utilizzato nei computer. Contiene i dati del sistema operativo, dei programmi e dei file memorizzati dall'utente. I dati sul disco rigido sono non volatili, perché rimangono memorizzati anche dopo lo spegnimento del sistema.
- **Dispositivi di memorizzazione esterni:** i dispositivi di memorizzazione esterni, come le chiavi USB, le schede di memoria e i dischi ottici, sono utilizzati per memorizzare i dati in modo portatile e possono essere rimossi dal sistema informatico. I dati su questi dispositivi sono non volatili, perché rimangono memorizzati anche quando il dispositivo viene scollegato dal sistema.
- **Archivi di backup:** gli archivi di backup sono copie dei dati del sistema informatico utilizzati per il ripristino in caso di perdita o danneggiamento dei dati originali. Questi dati sono non volatili, perché rimangono memorizzati anche dopo lo spegnimento del sistema.

- **Registri di sistema:** i registri di sistema sono file di log utilizzati per registrare le attività del sistema operativo e delle applicazioni. Questi dati sono non volatili, perché rimangono memorizzati anche dopo lo spegnimento del sistema.
- **Metadati:** i metadati sono informazioni aggiuntive sui file, come ad esempio la data di creazione, la data di modifica, l'autore e le informazioni di formato. Questi dati sono non volatili, perché sono memorizzati nel file stesso e rimangono disponibili anche dopo lo spegnimento del sistema.

Ma anche:



- File di registro di eventi di sistema (system event logs)
- File di registro di sicurezza (security logs)
- File di registro di applicazioni (application logs)
- Archivi di posta elettronica
- File di configurazione di sistema e di applicazioni
- Immagini di sistema e di applicazioni
- Snapshot di sistema
- File di configurazione di rete
- File di configurazione di firewall
- File di configurazione di proxy
- File di configurazione di router e switch di rete
- File di configurazione di server web e applicazioni web
- File di registro di accesso di server web e applicazioni web
- File di backup di server web e applicazioni web
- File di registro di accesso al database
- File di backup del database
- Registro di attività di accesso ai file
- File di registro di attività di stampa
- File di configurazione del sistema operativo
- File di configurazione di applicazioni di terze parti.
- File personali dell'utente (documenti, fogli di calcolo, archivi di posta, ecc.)
- File di configurazione del sistema operativo
- File dei software applicativi
- Spazio non allocato
- Slack Space



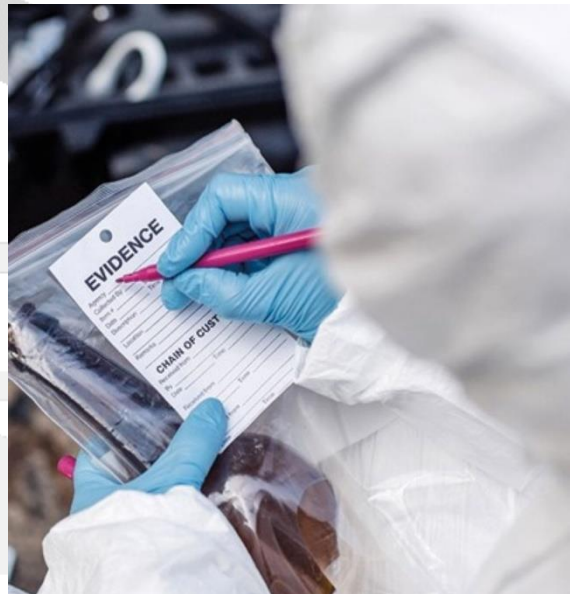
PASSI OPERATIVI

IDENTIFICAZIONE E REPERTAMENTO

- Computer Spento
- Computer Acceso

L'IDENTIFICAZIONE

- La fase di identificazione avviene in corrispondenza dell'analisi della scena del crimine
- Il processo di identificazione deve seguire le cosiddette *"best practices"*
- Può sembrare la fase più semplice, perché si tratta «unicamente» di individuare e catalogare il potenziale contenitore delle informazioni ricercate
- Tuttavia, vista l'enorme quantità di strumenti atti a conservare dati che si possiedono, è fondamentale individuare tutto quello che può essere utile
- Per esempio....
 - Quanto ci vuole per occultare una scheda microSD?
 - È sempre facile individuare un Pen Drive?
 - Il pc è collegato alla rete?
 - Ha un sistema di crittografia?
 - Mi serve tutto il "case" o porto solo la memoria?



REPERTAMENTO

- A seconda della tipologia di dispositivo e/o localizzazione, si possono identificare delle *"best practices"* per il repertamento.
- Analizziamo 2 casi:
 1. **Computer spento (Post Mortem Forensics)**
 2. **Computer acceso (Live Forensics)**



REPERTAMENTO DI UN COMPUTER SPENTO (POST MORTEM FORENSICS)

Le varie fasi da compiere sono:

1. Mettere in sicurezza la scena
2. Allontanare le persone presenti dai dispositivi digitali
3. Fotografare o fare una ripresa video della scena del crimine
4. Assicurarci che il computer sia effettivamente spento
5. NON ACCENDERE IL COMPUTER PER NESSUN MOTIVO
6. Rimuovere la batteria
7. Scollegare l'alimentazione
8. Etichettare le porte e i cavi
9. Assicurarci che tutti gli oggetti siano stati sigillati e siglati
10. Identificare eventuali indicazioni del modello e del numero di serie presenti
11. Compilare un report di sequestro per ogni oggetto
12. Cercare diari, appunti o pezzi di carta con password
13. Prendere nota dettagliata di tutte le operazioni compiute in relazione ai dispositivi informatici



REPERTAMENTO DI UN COMPUTER ACCESO (LIVE FORENSICS)

Quando ci si trova davanti a un computer acceso si deve effettuare una scelta:

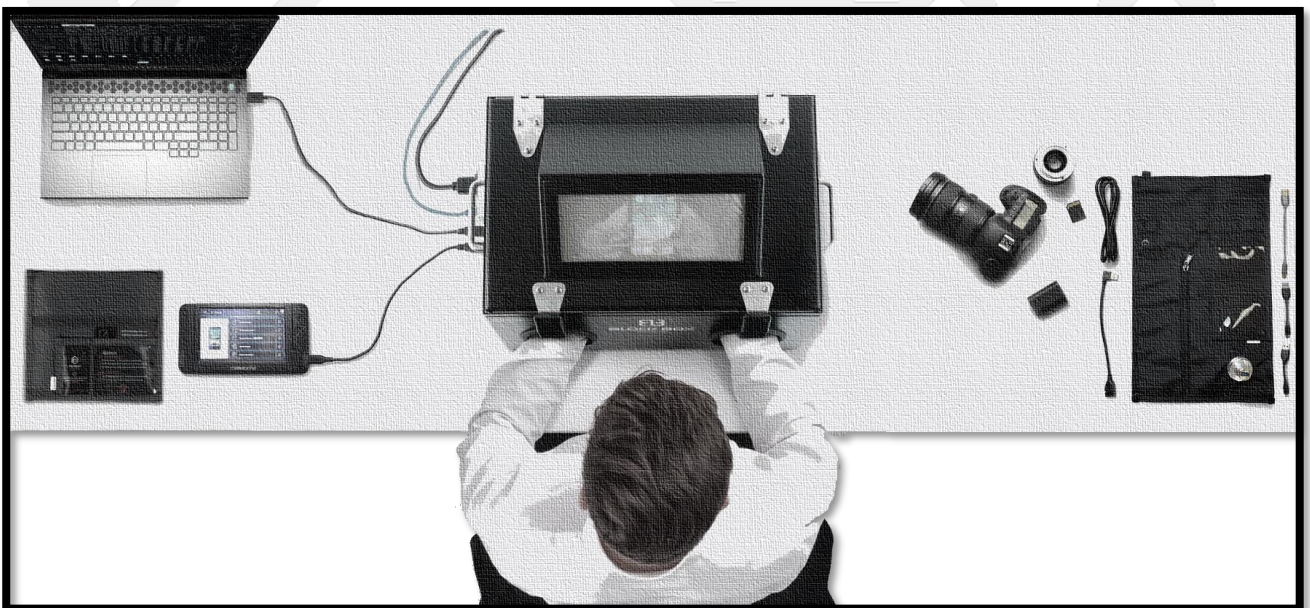
1. Spegnerlo subito per effettuare una copia forense.
2. Esaminarlo mentre è in esecuzione.

La scelta dipende da diversi fattori:

- Competenza e/o conoscenza dello specifico sistema
- Strumenti disponibili
- Rilevanza dei dati rispetto all'indagine

Un intervento di Live Forensics si rende necessario (o molto utile) quando:

1. Il sistema non è fisicamente rimovibile.
2. Il sistema non può essere spento perché è un sistema:
 - Militare
 - Di videosorveglianza
 - Di strumenti medici
 - Un database server in condivisione
 - Un Server in hosting/housing
3. Il sistema non può essere acquisito nella sua interezza (problema di memoria o altro).
4. Le informazioni "volatili" sono rilevanti rispetto alle indagini (es. stato della rete, chat/download in corso, memorie volatili, ecc.)
5. Siamo in presenza di volumi cifrati (BitLocker, FileVault, TrueCrypt, LUKS, ecc.)



Ecco una panoramica dei passi principali coinvolti nel repertamento di un computer acceso:

- **Identificazione dell'obiettivo:**
 - L'analista di Digital Forensics deve identificare il sistema informatico da analizzare e le informazioni specifiche che devono essere acquisite.
- **Accesso al sistema:**
 - L'analista deve ottenere l'accesso al sistema in questione, ad esempio attraverso un account di amministratore o una connessione remota.
- **Raccolta di informazioni:**
 - Una volta che l'analista ha accesso al sistema, può iniziare a raccogliere informazioni utilizzando una serie di strumenti di analisi. Questi strumenti possono includere software di monitoraggio del traffico di rete, strumenti di analisi del registro di sistema, strumenti di analisi del traffico del disco e così via.
- **Analisi delle informazioni raccolte:**
 - Una volta raccolte le informazioni, l'analista deve analizzarle per identificare eventuali attività sospette, comportamenti anomali, malware o altri elementi di prova.
- **Preservazione delle prove:**
 - Durante il processo di repertamento del sistema in funzione, l'analista deve assicurarsi che le prove siano preservate in modo accurato e affidabile. Ciò significa che le informazioni raccolte devono essere documentate, registrate e archiviate in modo sicuro per garantire l'integrità delle prove.

Per contro utilizzando tecniche di Live Forensics:

- Il sistema viene sicuramente perturbato:
 - Le modifiche apportate sono note?
 - Le modifiche apportate sono documentabili?
 - Le modifiche apportate intaccano significativamente il risultato dell'analisi?
 - Ogni modifica apportata può distruggere un altro dato.
- Gli accertamenti svolti su sistemi accesi non saranno ripetibili.

CATENA DI CUSTODIA

La Digital Evidence deve essere trattata e conservata molto attentamente per evitare contaminazioni, danni e qualsiasi azione che potrebbe renderla inutilizzabile.

Si deve predisporre una catena di custodia che identifichi tutte le persone che hanno avuto accesso al supporto originale.

La catena di custodia deve contenere alcune informazioni fondamentali, come:

1. **Identificazione e raccolta delle prove digitali:** inizia con l'identificazione delle prove digitali pertinenti al caso. Le prove digitali possono essere recuperate da diversi dispositivi, come computer, smartphone, dispositivi di storage, server, etc. La raccolta delle prove digitali deve essere effettuata con tecniche e strumenti forensi specifici per evitare di alterare i dati.
2. **Documentazione della raccolta delle prove digitali:** una volta che le prove digitali sono state raccolte, è importante documentare l'intero processo. È necessario annotare tutte le attività svolte, i dispositivi coinvolti e le tecniche utilizzate.
3. **Conservazione delle prove digitali:** le prove digitali devono essere conservate in modo sicuro e affidabile per garantirne l'integrità. È importante utilizzare dispositivi di archiviazione specifici per le prove digitali, come hard disk esterni o dispositivi di archiviazione cloud.
4. **Trasferimento delle prove digitali:** se le prove digitali devono essere trasferite da un luogo all'altro, è importante farlo con metodi sicuri e affidabili, come l'uso di crittografia e firme digitali.
5. **Analisi delle prove digitali:** le prove digitali devono essere analizzate da esperti forensi digitali per ricavare informazioni utili alla risoluzione del caso.
6. **Documentazione dell'analisi delle prove digitali:** tutte le attività svolte durante l'analisi delle prove digitali devono essere documentate in modo dettagliato, compreso il tipo di attività svolta, gli strumenti utilizzati e i risultati ottenuti.
7. **Presentazione delle prove digitali in tribunale:** infine, le prove digitali devono essere presentate in tribunale in modo da garantirne l'affidabilità e l'integrità come prova legale. La documentazione completa della catena di custodia è essenziale per dimostrare la validità delle prove digitali e garantire che siano ammissibili come prove in tribunale.

Ogni volta che i supporti oggetto di indagini sono affidati a un nuovo investigatore, nella catena di custodia dovrà essere aggiunta un'informazione contenente:

- Nome della persona che ha preso in carico il supporto
- Data e ora di consegna e data e ora di restituzione

Description of Evidence		
Item #	Quantity	Description of Item (Model, Serial #, Condition, Marks, Scratches)

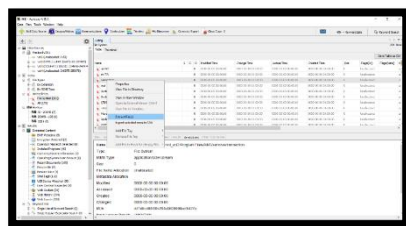
Chain of Custody				
Item #	Date/Time	Released by (Signature & ID#)	Received by (Signature & ID#)	Comments/Location



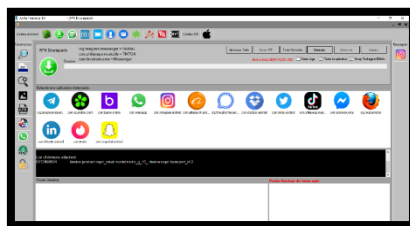
ANALISI

La Digital Forensics utilizza diverse modalità di analisi² per esaminare le prove digitali e ricavare informazioni utili alla risoluzione di un caso. Ecco alcune delle modalità di analisi più comuni:

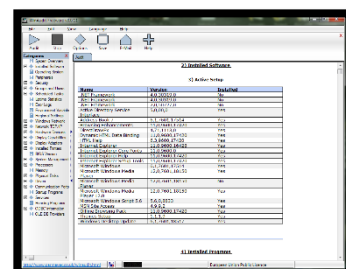
- **Analisi logica:**
 - È una modalità di analisi che si concentra sulla ricerca di informazioni nei file di sistema, nei registri di sistema, nei file di registro di applicazioni, nei file di configurazione di sistema e di applicazioni, nei metadati e in altri elementi di prova digitali non criptati. L'analisi logica viene utilizzata per identificare gli eventi che hanno portato alla creazione, modifica o eliminazione di determinati file e per identificare i programmi o le applicazioni utilizzate per accedere ai file.
- **Analisi file carving:**
 - È una modalità di analisi che si concentra sulla ricerca di informazioni nei file eliminati o corrotti. L'analisi file carving utilizza tecniche speciali per recuperare i dati dai cluster di file cancellati o danneggiati.
- **Analisi di rete:**
 - È una modalità di analisi che si concentra sulla ricerca di informazioni nei dati di traffico di rete, nei log di rete e nei file di configurazione di rete. L'analisi di rete viene utilizzata per identificare le connessioni di rete tra i dispositivi, le attività di rete sospette, le intrusioni di rete e le attività di hacking.
- **Analisi delle password:**
 - È una modalità di analisi che si concentra sulla ricerca di informazioni relative alle password. L'analisi delle password viene utilizzata per identificare le password utilizzate per accedere ai sistemi, le password che sono state modificate o cancellate, le password criptate e le password che sono state dimenticate.
- **Analisi del sistema operativo:**
 - È una modalità di analisi che si concentra sulla ricerca di informazioni nel sistema operativo del dispositivo. L'analisi del sistema operativo viene utilizzata per identificare le attività dell'utente, le applicazioni installate, le modifiche al sistema operativo e le impostazioni di sistema.
- **Analisi del browser web:**
 - È una modalità di analisi che si concentra sulla ricerca di informazioni nel browser web del dispositivo. L'analisi del browser web viene utilizzata per identificare la cronologia di navigazione dell'utente, le informazioni di login, i cookie e le impostazioni del browser.
- **Analisi dei metadati:**
 - È una modalità di analisi che si concentra sulla ricerca di informazioni nei metadati associati ai file digitali. L'analisi dei metadati viene utilizzata per identificare le informazioni sulle date e gli orari di creazione, modifica e accesso dei file, le informazioni sul dispositivo utilizzato per creare o modificare i file e le informazioni sulla posizione geografica dei file.



Autopsy



Avilla Forensics



WinAudit

² <https://github.com/CScorza/Analisi-Digital-Forensics>

(Nel seguente link, ci sono diversi strumenti di Analisi Digital Forensics)

DATA CARVING

Il data carving³, (noto anche come file carving), è una tecnica di recupero dati digitale che consiste nel recuperare file dallo spazio non allocato di un supporto di memorizzazione di dati digitali (ad esempio un hard disk o una chiavetta USB) anche quando non vi è più traccia di quel file nella tabella di allocazione. utilizzando la firma binaria di un file o la sua struttura logica.

Quando noi cancelliamo un file da un supporto di memoria, realmente il file viene marcato come “eliminato”, ma continua a rimanere memorizzato sul supporto informatico. Molte delle volte del file cancellato, rimane traccia nel file system, pertanto, il suo recupero è anche più tosto semplice con un programma di recupero file (Per esempio *RECUVA*). Quando non è possibile perché si perde il riferimento dei file, l'unica strada da fare è quella del Carving.

Ecco alcuni esempi di utilizzo del data carving:

1. **Recupero di file cancellati accidentalmente:** se un file viene eliminato accidentalmente da una scheda di memoria o da un'unità disco rigido, il data carving può essere utilizzato per recuperare il file, anche se è stato rimosso dalla cartella originale e dal cestino.
2. **Individuazione di file nascosti:** il data carving può essere utilizzato per trovare file nascosti all'interno di un'unità disco rigido. Ad esempio, se un file viene nascosto all'interno di un altro file o di una cartella, il data carving può essere utilizzato per individuare la sua firma binaria e recuperarlo.
3. **Recupero di file da una scheda di memoria danneggiata:** se una scheda di memoria viene danneggiata e non è possibile accedervi normalmente, il data carving può essere utilizzato per recuperare i file dalla memoria danneggiata.

I motivi per cui non si può effettuare questa tecnica, sono tanti, tra cui:

- **La Sovrascrittura dei dati.**
 - Dati Sovrascritti con altre informazioni.
- **Corruzione dei dati**
 - Dati corrotti o danneggiati
- **Frammentazione dei dati**
 - Dati danneggiati e suddivisi in più parti
- **Crittografia**
 - Dati Crittografati (mancanza della chiave di decrittazione)
- **Compressione**
 - Dati compressi (bisognerebbe decomprimerli prima)
- **Dispositivi fisicamente danneggiati e non recuperabili.**
 - Unità di memoria fisicamente danneggiati.

Gli strumenti che effettuano questo tipo di tecnica sono:

Strumenti Base

- [TestDisk](#)
- [PhotoRec](#)
- [Recuva](#)
- [R-Studio](#)

Strumenti Forensi

- [Encase Forensics](#)
- [Forensic Toolkit \(FTK\)](#)
- [Oxygen Forensic Detective](#)
- [X-Ways Forensics](#)
- [Autopsy](#)

³ <https://www.bit4law.com/data-carving/>

ACQUISIZIONE PAGINA WEB

L' Acquisizione Forense siti o Pagine Web⁴ è finalizzata a cristallizzare le prove contenute su siti web, profili o pagine Facebook, Instagram, Twitter, LinkedIn, testate giornalistiche online, forum, gruppi, video su YouTube o TikTok o su chat di messaggistica come WhatsApp, Telegram, Signal, piattaforme di streaming, software, piattaforme di file sharing, Torrent, Emule, audio e qualunque tipo di contenuto sia accessibile tramite la rete Internet.

Diverse sono le sentenze della Cassazione⁵, dicono che, sono da ritenersi pienamente utilizzabili, in quanto legittima ne è l'acquisizione come documento, i messaggi SMS fotografati dallo schermo di un telefono cellulare. Ma molte volte non è necessario è sufficiente la stampa cartacea o in PDF, dello screenshot o il salvataggio dello schermo di una pagina web, per garantire il suo valore probatorio. Questo perché lo stesso può essere facilmente manipolato, privando così il suo valore di prova.

L'acquisizione della pagina web è molto utili per quei reati come diffamazione (Art. 595 c.p.), ingiuria o calunnia (Art.594), stalking (Art. 612 bis c.p.) o minacce (Art.612 c.p.), specie per quanto riguarda forum, social media e chat di messaggistica), oppure reati a sfondo sessuale come la pedopornografia (Art. 600 - ter/quarter/quarter 1 c.p.) e Revenge Porn (Art. 612-ter c.p.).

Strumenti per effettuare l'acquisizione:

- **HTTTrack**
 - È uno strumento gratuito e open source che consente di scaricare un sito web completo, comprese le pagine web, le immagini, gli script e altro ancora. È disponibile per Windows, Linux e iOS.
- **WebForensics**
 - Ambiente forense composto da un browser web, diverse console di log e un'applicazione per cristallizzare le prove digitali e archivarle in cloud.
- **Forensic Browser (FoBro)** *thefreetoolproject.eu (tool LAW di EUROPOL)*
 - Raccogliere e conservare prove online, come si vede, durante le indagini online
- **MAGNET Web Page Saver**
 - È uno strumento perfetto per catturare l'aspetto delle pagine Web in un momento specifico.



⁴ <https://dalchecco.it/servizi/perizie/perizie-reti-internet/acquisizione-forense-pagine-siti-web/>

⁵ <https://canestrinilex.com/risorse/screenshot-e-prova-cass-2460022/>

FIRMA DIGITALE DI UN' IMMAGINE FORENSE

L'HASH

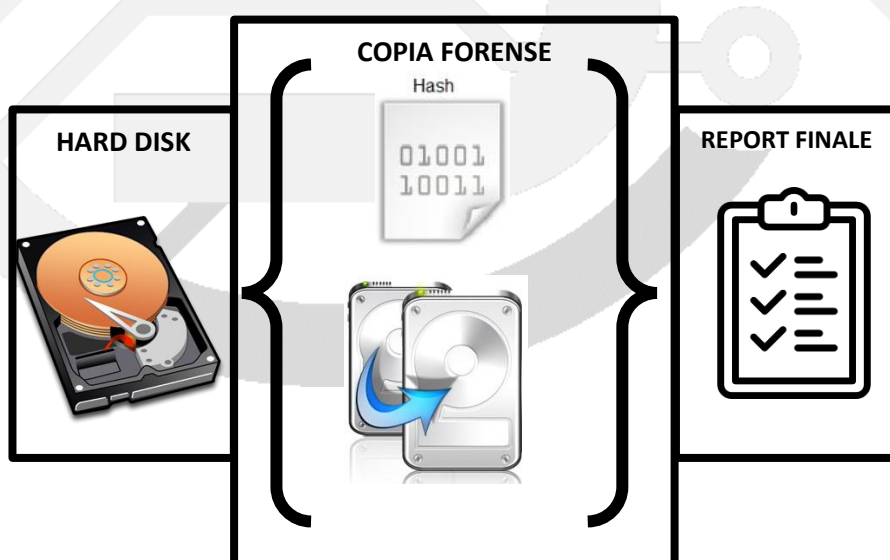
La funzione di hash è spesso utilizzata nella Digital Forensics per firmare digitalmente e codificare un'immagine forense.

L'Hashing è un processo crittografico che consente di creare un valore univoco di lunghezza fissa, noto come "hash", a partire da un insieme di dati di input. L'Hashing è utilizzato per garantire l'integrità dei dati e verificare che un file non sia stato modificato o corrotto. Spesso si utilizzano più funzioni hash per garantire la solidità del dato.

Per firmare digitalmente un'immagine forense utilizzando una funzione di hash, è necessario eseguire i seguenti passaggi:

1. **Calcolo dell'hash:** utilizzare una funzione di hash (come MD5, SHA-1, SHA-256 etc.) per calcolare l'hash dell'immagine forense. Questo creerà un valore univoco che può essere utilizzato per verificare l'integrità dell'immagine.
2. **Firma dell'hash:** utilizzare un algoritmo di firma digitale (come RSA o DSA) per firmare l'hash calcolato. La firma digitale viene generata utilizzando una chiave privata e può essere verificata utilizzando una chiave pubblica.
3. **Salvataggio dell'hash firmato:** salvare l'hash firmato insieme all'immagine forense. Questo consente di verificare l'integrità dell'immagine in futuro utilizzando la chiave pubblica corrispondente alla chiave privata utilizzata per firmare l'hash.

Il tutto deve essere poi riportato nei vari report, in modo da effettuare le opportune verifiche di integrità.



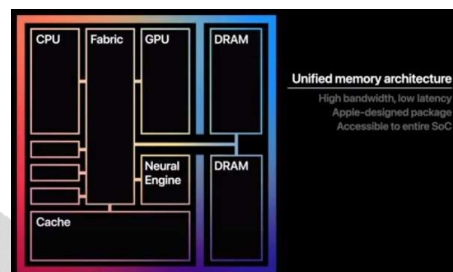
TIPI DI MEMORIE

Le Memorie Informatiche possono anche essere classificate in base alla loro volatilità, ovvero la loro capacità di mantenere i dati anche in assenza di energia elettrica. In base a questo criterio, si distinguono le memorie fisiche e le memorie volatili.

Le Memorie Volatili, invece, sono quelle che richiedono di energia elettrica per conservare i dati, come ad esempio la memoria RAM e la cache. Quando il computer si spegne, i dati memorizzati in queste memorie vengono persi.

In dettaglio:

- **Memoria RAM (Random Access Memory):** È la memoria principale del computer e viene utilizzata per archiviare temporaneamente i dati che il processore sta elaborando in quel momento.



Struttura di una RAM

Le Memorie Fisiche non volatili sono quelle che conservano i dati anche in assenza di alimentazione elettrica, come ad esempio i dischi rigidi, le unità flash USB e le memorie CD/DVD.

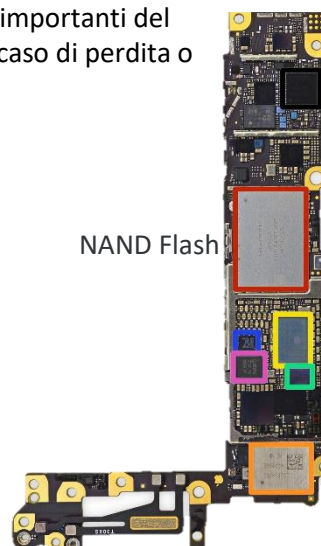
In dettaglio:

- **Memoria ROM (Read-Only Memory):** è una memoria di sola lettura, utilizzata per archiviare il firmware e il BIOS del computer.
- **Memoria cache:** è una memoria molto veloce utilizzata per conservare temporaneamente i dati che il processore usa più frequentemente.
- **Disco rigido:** è una memoria di archiviazione permanente, utilizzata per memorizzare i file e i programmi del computer.
- **Memoria flash:** è una memoria non volatile utilizzata per l'archiviazione di dati come file, foto e musica.
- **Memoria virtuale:** è una parte dello spazio su disco rigido utilizzata dal sistema operativo come una sorta di estensione della memoria RAM.
- **Memoria di massa:** è una memoria di archiviazione permanente, come un disco rigido o un'unità flash USB, utilizzata per memorizzare grandi quantità di dati.
- **Memoria video:** è una memoria utilizzata dalle schede grafiche per archiviare i dati relativi alle immagini e ai video.
- **Memoria di backup:** è una memoria utilizzata per effettuare il backup dei dati importanti del computer, come documenti e file di sistema, in modo da poterli recuperare in caso di perdita o danneggiamento.

USB



NAND Flash



MEMORIE SSD








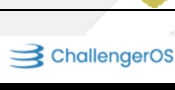
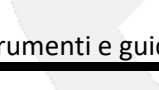


HARDISK



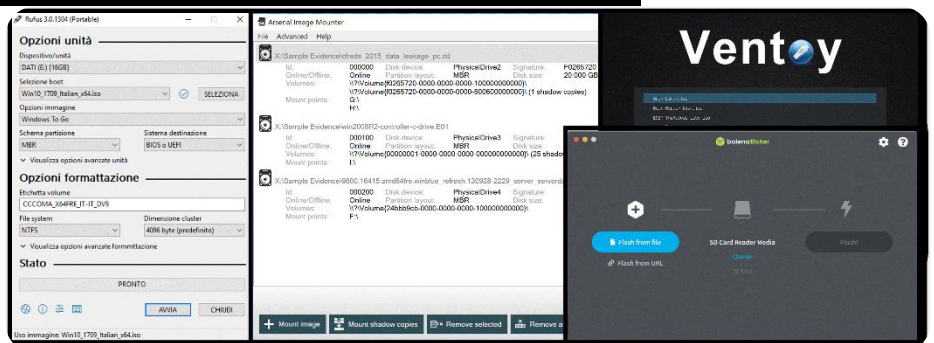
STRUMENTI OPEN SOURCE PER LA DIGITAL FORENSICS

Distro Linux⁶ che hanno la possibilità di analisi in Live o “Post Mortem”:

	Caine
	Kali Linux
	Tsurugi
	Tails
	Parrot Security OS
	CSI Linux
	Athena OS
	Forlex
	Paladin EDGE
	ChallengerOS

Strumenti e guide per avviare una Distro in modalità Live Forensics

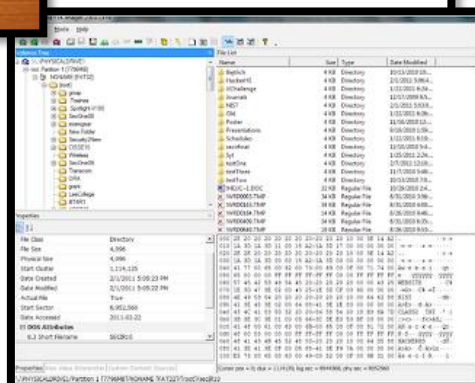
Rufus	Arsenal Recon - Image Mounter	Ventoy	Balena Etcher	Easy2Boot
GUIDA	GUIDA	GUIDA Ventoy - Megazine Computer Idea	GUIDA	GUIDA



⁶ <https://github.com/CScorza/DistroForensics>

Strumenti per la copia delle immagini ISO

Open-Source	
dd	<i>Un comando di copia del disco di base disponibile su molte distribuzioni Linux.</i>
dc3dd	<i>Una versione avanzata di dd con alcune funzionalità aggiuntive.</i>
FTK Imager	<i>Un'applicazione di copia forense gratuita che supporta una vasta gamma di formati di immagini.</i>
Guymager	<i>Un'applicazione open source che supporta la copia di immagini di dischi rigidi, USB, CD/DVD e altre unità di archiviazione.</i>
OSFClone	<i>Un'applicazione gratuita per creare immagini di dischi rigidi e partizioni.</i>
Arsenal Recon	<i>Strumenti di digital forensics sviluppati per creare immagini e copie forensi</i>
MAGNET RAM Capture	<i>è uno strumento di imaging gratuito progettato per acquisire la memoria fisica del computer di un sospetto</i>
A Pagamento	
EnCase	<i>Un'applicazione completa per la copia forense di dischi rigidi, dispositivi mobili e altri dispositivi di archiviazione.</i>
X-Ways Forensics	<i>Un'applicazione avanzata per la copia forense di dischi rigidi, unità flash USB e altri dispositivi di memorizzazione.</i>
Magnet Acquire	<i>Un'applicazione per la copia forense di dischi rigidi, telefoni cellulari e altri dispositivi mobili.</i>
AccessData FTK	<i>Un'applicazione per la copia forense e l'analisi dei dati di dischi rigidi, dispositivi mobili e altri dispositivi di archiviazione.</i>
Forensic Explorer	<i>Un'applicazione per la copia forense e l'analisi dei dati di dischi rigidi e altri dispositivi di archiviazione</i>
Oxygen Forensic Detective	<i>Un'applicazione per la copia forense e l'analisi di smartphone, tablet, dispositivi GPS e altri dispositivi mobili.</i>
Cellebrite UFED	<i>Un'applicazione per la copia forense di smartphone, tablet e altri dispositivi mobili.</i>
MSAB XRY	<i>Un'applicazione copia forense dei dati, la decodifica dei file e la visualizzazione dei risultati.</i>



L'ACQUISIZIONE DELLA PROVA LA POLIZIA GIUDIZIARIA CODICE DI PROCEDURA PENALE ED ALTRE LEGGI⁷

Di seguito sono riportati gli articoli⁸ più rilevanti:

- **Art. 234 Cpp Prova documentale.**
 - *È consentita l'acquisizione di scritti o di altri documenti che rappresentano fatti, persone o cose mediante la fotografia, la cinematografia, la fonografia o qualsiasi altro mezzo.*
- **Art. 244. Co.2 Casi e forme delle Ispezioni.**
 - *[...] 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.*
- **Art. 247 Cpp Casi e forme delle perquisizioni.**
 - *[...] 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 bis Cpp Sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni**
 - *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.*
- **Art. 256 Cpp – Dovere di esibizione e segreti**
 - *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, e ogni altra cosa esistente presso di esse per ragioni del loro ufficio, incarico, ministero, professione o arte, salvo che dichiarino per iscritto che si tratti di segreto di Stato ovvero di segreto inerente al loro ufficio o professione.*
- **Art. 350 Cpp Sommarie informazioni dalla persona nei cui confronti vengono svolte le indagini**
 - *(Per l'acquisizione di password)*
- **Art. 352 Cpp – Perquisizioni**
- **Art. 354 Cpp – Accertamenti urgenti sui luoghi, sulle cose e sulle persone. Sequestro.**
 - *Gli ufficiali e gli agenti di polizia giudiziaria curano che le tracce e le cose pertinenti al reato siano conservate e che lo stato dei luoghi e delle cose non venga mutato prima dell'intervento del pubblico ministero.*
- **Art. 359 Cpp Consulenti tecnici del pubblico ministero**
- **Art. 360 Cpp Accertamenti tecnici non ripetibili**
- **D.lgs. 7 marzo 2005, n. 82**
 - **Art. 1 lett. p** - *I file di log sono dei veri e propri documenti informatici*
 - **Art. 23 bis** - *Duplicato Informatico e copia Informatica*

⁷ <https://www.rivistaildirittovivente.it/lacquisizione-della-prova-digitale.htm>

⁸ <https://www.brocardi.it/>

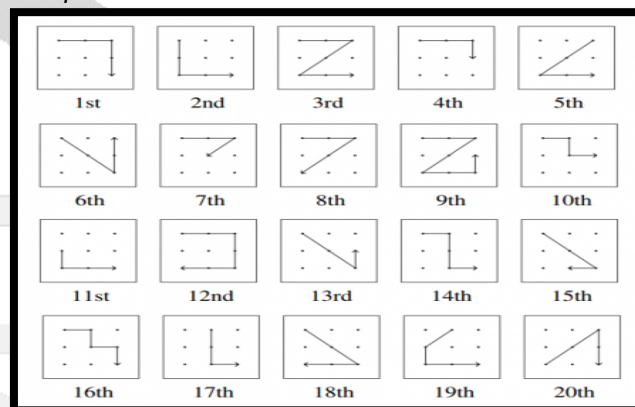
MOBILE FORENSICS

La mobile forensics⁹ (o informatica forense mobile) è la pratica di acquisire, analizzare e interpretare le prove digitali su dispositivi mobili, come smartphone, tablet e altri dispositivi portatili. Le prove digitali possono includere dati come messaggi di testo, e-mail, immagini, video, cronologia di navigazione, registri delle chiamate e molto altro.

Buone norme:

1. Evita di maneggiare o toccare il dispositivo il più possibile, per evitare di contaminare o modificare le prove digitali. Indossare guanti in lattice può essere utile.
2. Controllare tramite il sistema controllo, la sequenza della password utilizzata per sbloccare il dispositivo
3. Isola il dispositivo dal Wi-Fi e dalla rete cellulare (Modalità Aereo o Busta di Faraday¹⁰) per impedire la connessione e la modifica a distanza dei dati contenuti all'interno (più comunemente serve ad impedire la sottrazione dei dati o la formattazione a distanza)
4. Esegui una copia forense del dispositivo il più presto possibile. Questo consentirà di lavorare su una copia del dispositivo senza modificare o compromettere l'originale.
5. Identifica il tipo di sistema operativo e la versione del dispositivo per determinare il metodo migliore per acquisire i dati. Ad esempio, su dispositivi iOS, la sincronizzazione tramite iTunes può essere utilizzata per acquisire i dati, mentre su dispositivi Android potrebbe essere necessario sbloccare il "bootloader".
6. Esamina i dati acquisiti con attenzione e analizza le informazioni in modo approfondito per identificare le prove rilevanti.
7. Documenta tutte le attività eseguite durante il processo di analisi delle prove digitali, comprese le procedure utilizzate e le attività eseguite.

Sequenze di sblocco comuni



Buste di Faraday



Consigli:

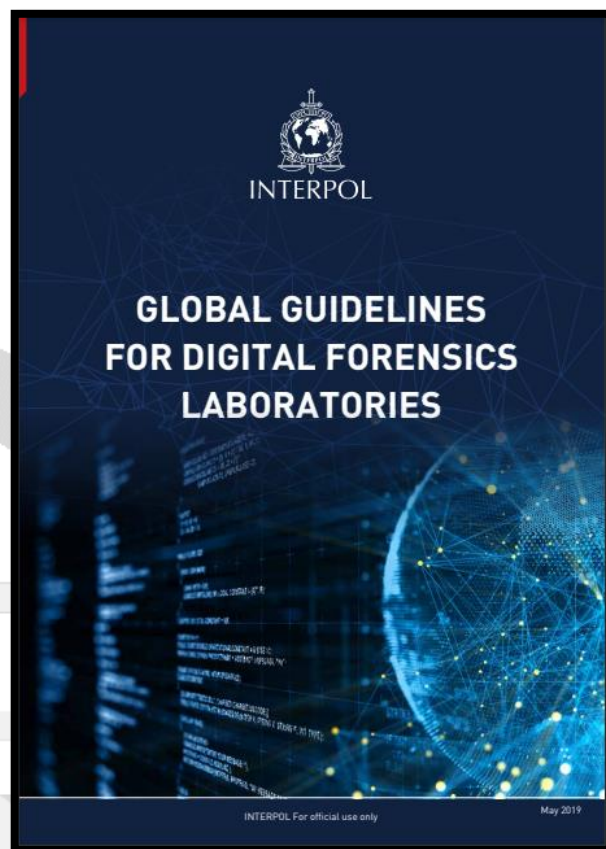
- best practices per iOS [Le mie best practices per iPhone e iDevice](#) Scritto da "Rebus".
- Vedi file in allegato su Repertamento e Perquisizione Informatica

⁹ <https://github.com/CScorza/OSINT-FORENSICS-MOBILE>

¹⁰ Questo tipo di busta è progettato con un materiale conduttivo che blocca i segnali radio, come ad esempio il segnale Wi-Fi o di rete cellulare, impedendo che il dispositivo all'interno della busta possa essere rintracciato o intercettato

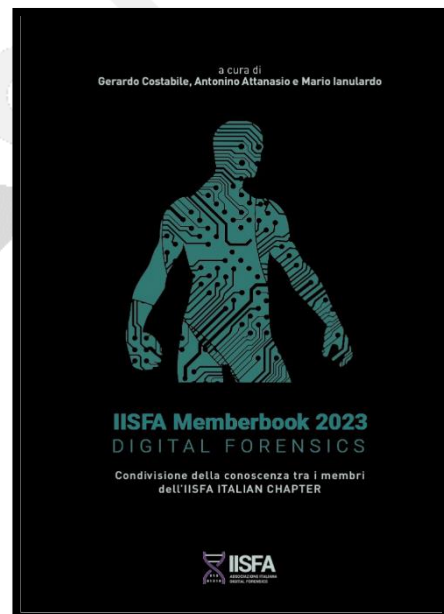
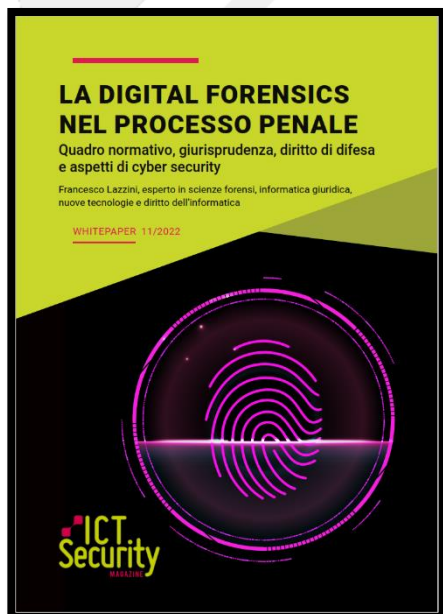
LINEE GUIDA PIÙ DIFFUSE

- [INTERPOL DFL GlobalGuidelinesDigitalForensicsLaboratory](#)
- [ENISA - Forensics Analysis](#)
- [ENFSI Best Practices Manuals](#)



PUBBLICAZIONI UTILI

- [LA DIGITAL FORENSICS NEL PROCESSO PENALE](#)
- [DIGITAL FORENSICS](#)
- [IISFA Memberbook 2023 DIGITAL FORENSICS](#)
Cyber-crime investigation, live-forensic & cloud.






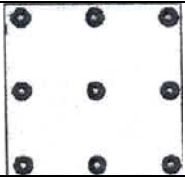
ALLEGATI

MODULO REPERTAMENTO E CATENA DI CUSTODIA

Data e ora _____

Dati Fascicolo	
Procedimento Penale	
Autorità Giudiziaria	
Verbalizzante/i	
Indagato	
Utilizzatore ¹	
Descrizione dispositivo MOBILE	
Tipologia apparato ²	<input type="checkbox"/> Cellulare/Smartphone <input type="checkbox"/> Tablet <input type="checkbox"/> Smart-watch <input type="checkbox"/> Smart-TV
Alimentatore/Cavi originali/Scatola di acquisto ³	
Marca	
Modello ⁴	
IMEI ⁵	
SIM ⁶	
Card e similari (SD, Micro-SD, CF, Memorystic) ⁷	
Stato ⁸	
Danneggiamenti e/o malfunzionamenti accertati "de visu"	
Eventuali video/fotografie eseguite al reperto che ne documentano lo stato/integrità all'atto della acquisizione/sequestro	<input type="checkbox"/> SI, se si dove sono state salvate ⁹ _____ <input type="checkbox"/> NO
Misure di sicurezza di protezione del cellulare/smartphone/tablet¹⁰	

- 1 Nel caso si proceda al sequestro di un dispositivo utilizzato da conviventi, familiari dell'indagato, in quanto si sospetta che possano celare evidenze informatiche, specificare appositamente l'utilizzatore del dispositivo.
- 2 Tipologia apparato: specificare se il sistema mobile (in grado di connettersi "over the air" a una rete cellulare) sia un cellulare senza la disponibilità di servizi internet come la messaggistica istantanea (Whatsapp etc.), oppure sia uno smartphone fornito di tali servizi.
- 3 Specificare se siano stati sequestrati i cavi originali e l'alimentatore, nonché la scatola originale. Cercare sempre di recuperare in particolari i cavi originali, considerato che alcuni smartphone/cellulari utilizzano delle tipologie con standard proprietario difficilmente reperibili in commercio e fondamentali per l'estrazione dati.
- 4 Il modello generalmente si trova nella scocca posteriore del dispositivo ed è contraddistinto da una sigla tipo SM-G960 (SAMSUNG) o A1337 (Apple)
- 5 E' possibile rinvenire l'IMEI nella scocca posteriore del dispositivo, oppure sulla scatola di acquisto. Se il dispositivo è acceso e sbloccato digitare la sequenza *#06#, annotando il codice IMEI rilevato.
- 6 Specificare l'ICCID stampato sulla SIM generalmente sotto il logo del gestore, oltre al numero telefonico associato, in quanto è l'ICCID che identifica una SIM. **In taluni casi impedire all'utente il riutilizzo dell'utenza associata alla SIM card potrebbe rivelarsi utile, per cui andrà richiesto all'A.G. apposito provvedimento d'inibizione da notificare al competente gestore.**
- 7 Specificare marca e capacità nominale.
- 8 Descrivere se il dispositivo sia stato rinvenuto acceso / spento.
- 9 Cercare sempre di documentare, mediante fotografie lo stato del dispositivo all'atto del sequestro e non di meno il luogo ove è stato ritrovato, con descrizione analitica della scena sul verbale di sequestro.
- 10 Se l'indagato si rifiuta di fornirle oppure afferma di averle dimenticate, potrà essere reso edotto della possibilità che il superamento della password potrebbe comportare un "blocco" del dispositivo di sua proprietà. Sul luogo o nell'immediatezza del fatto tali informazioni potranno essere acquisite anche senza la presenza del difensore, pure nei confronti di persona arrestata in flagranza o fermata ai sensi dell'art. 384alvo i casi di flagranza di reato nei quali la PG. Nei confronti di persona indagata dovranno invece essere acquisite alla necessaria presenza del difensore ai sensi dell'art. 350 c. 3 oppure potranno essere ricevute spontaneamente ai sensi del comma 7 dell'art. 350 c.p.p.

PIN ¹¹	
Password ¹²	
Pattern/Sequenza (da digitare come nell'esempio nel quadrato più piccolo, ossia con la freccia che indica il verso da seguire)	 
Face ID ¹³	
Touch ID ¹⁴	
PIN Sim Card ¹⁵	

Account cloud ¹⁶	
E-mail principale (iCloud, Google, Microsoft etc.)	User: _____; Password: _____; ¹⁷ Autenticazione a due fattori ¹⁸ : <input type="checkbox"/> SI (indicare su quale smartphone/servizio è abilitato ¹⁹ _____ <input type="checkbox"/> NO
E-mail secondaria (iCloud, Google, Microsoft etc.)	User: _____; Password: _____; Autenticazione a due fattori: <input type="checkbox"/> SI (indicare su quale smartphone/servizio è abilitato _____ <input type="checkbox"/> NO
E-mail nr. 3 (iCloud, Google, Microsoft etc.)	User: _____; Password: _____; Autenticazione a due fattori: <input type="checkbox"/> SI (indicare su quale smartphone/servizio è abilitato _____ <input type="checkbox"/> NO
Account nr. 1 (Facebook; Instagram etc.)	User: _____; Password: _____;

¹¹ Riportare la sequenza numerica, generalmente di quattro/sei cifre.

¹² Riportare l'intera sequenza di caratteri alfanumerici, avendo cura di annotare eventuali lettere maiuscole, minuscole e/o caratteri speciali.

¹³ In caso sia abilitato, segnare ABILITATO/NON ABILITATO, avendo cura di evitare di osservare direttamente la fotocamera del dispositivo e causare in tale maniera numerosi errori di riconoscimento, che comporterebbero il blocco del dispositivo.

¹⁴ In caso sia abilitato, segnare ABILITATO/NON ABILITATO, avendo cura di evitare di non toccare il tasto HOME e/o altro componente utilizzato dallo smartphone per il riconoscimento dell'impronta digitale.

¹⁵ Sequenza di quattro cifre, generalmente stampata sulla scheda descrittiva insieme al codice PUK.

¹⁶ L'acquisizione degli stessi va eseguita durante le perquisizioni senza soluzione di continuità, mediante una procedura che richiede quantomeno una connessione a internet nonché supporti di memoria ove salvare i dati acquisiti. Per tali complicazioni logistiche e tecniche si suggerisce sia eseguita da personale specializzato e/o consulenti tecnici

¹⁷ La password, se riferita dall'avente diritto, va cambiata temporaneamente in modo da impedirgli ulteriori accessi durante le attività di perquisizione e di conseguenza cancellare il contenuto dell'account. Alla fine delle operazioni l'indagato dovrà essere messo in condizione di accedere nuovamente al suo domicilio informatico, comunicandogli la password modificata e invitandolo a modificarla di proprio conto per ragioni di privacy e sicurezza.

¹⁸ Numerosi account supportano la possibilità di abilitare la ricezione di un sms sul telefono principale, che contiene un codice che va inserito per procedere all'accesso nell'account.

¹⁹ Nel caso in cui si sospetti sia attivo su un dispositivo ignoto, bisogna tentare di disattivare tale funzione, in modo che l'utente, una volta terminata la perquisizione e il seguente sequestro dell'account, proceda a un nuovo reset della password mediante l'autenticazione a due fattori attiva sull'altro dispositivo.

	Autenticazione a due fattori: <input type="checkbox"/> SI (indicare su quale smartphone/servizio è abilitato) <hr/> <input type="checkbox"/> NO
Account nr. 2 (Facebook; Instagram etc.)	User: _____; Password: _____; Autenticazione a due fattori: <input type="checkbox"/> SI (indicare su quale smartphone/servizio è abilitato) <hr/> <input type="checkbox"/> NO
Account nr. 3 (Facebook; Instagram etc.)	User: _____; Password: _____; Autenticazione a due fattori: <input type="checkbox"/> SI (indicare su quale smartphone/servizio è abilitato) <hr/> <input type="checkbox"/> NO
<p>N.B. Gli account cloud possono contenere sovente molte più informazioni degli stessi dispositivi fisici, per cui avere cura di annotare questi dati nel caso in cui l'indagato sia collaborativo e sia presente personale specializzato e/o consulenti tecnici. <u>I dati in questione tuttavia, salvo casi eccezionali come i reati di pedopornografia, non essendo cose fisiche (res) non potranno essere sottoposte a sequestro e/o qualsiasi forma di spossessamento dell'avente diritto salvo, ovviamente, diverso parere dell'A.G.. Questi andranno acquisiti mediante procedura di perquisizione telematica all'atto dell'ordinaria perquisizione da personale specializzato e/o consulenti tecnici.</u></p>	

Avvertenze / Cautele	
Smartphone Apple iOS	<p>In caso di smartphone ACCESO e bloccato, <u>NON SPEGNERLO</u> e provvedere all'isolamento dalla rete. Si può riuscire in ciò, abilitando la modalità "aereo" oppure rimuovendo la SIM card. Tenere presente che in alcune versioni del sistema operativo iOS, anche in modalità aereo è possibile abilitare il Wi-Fi, per cui procedere a disabilitarlo se possibile.</p> <p>Tenere bene a mente che, se il dispositivo sarà sequestrato bloccato, ossia senza disponibilità della relativa misura di sicurezza:</p> <ol style="list-style-type: none"> 1. Potrebbe esserci necessità di compiere l'accertamento entro una sola ora dal sequestro probatorio (ossia dall'ultima volta in cui si suppone che l'utente abbia sbloccato il dispositivo), in quanto potrebbe essere stata attivata la USB Restricted Mode (negli iPhone più recenti) che nell'ultima versione di iOS 13 disabilita la porta USB decorsa solo un'ora dall'ultimo sblocco del dispositivo. <u>In questo caso particolare il relativo accertamento tecnico assume una determinante urgenza, per cui all'atto del sequestro bisogna riferire tempestivamente la questione all'A.G. competente e al consulente / personale specializzato;</u> 2. Si dovrà procedere possibilmente all'individuazione e conseguente sequestro probatorio, del personal computer ove l'indagato eseguiva la sincronizzazione dei contenuti del suo dispositivo iOS, mediante noto

	<p>software iTunes. In questo particolare caso infatti la restrizione USB potrebbe essere allungata tenendo collegato l'iPhone al computer su cui veniva eseguito il backup mediante iTunes. Per cui andrà sequestrato anche questo dispositivo insieme all'iPhone.</p> <p>L'efficacia di tale operazione è strettamente legata al mantenere ACCESO (sempre isolato dalla rete) lo smartphone Apple iOS sequestrato, fino al conferimento al personale specializzato che sarà incaricato degli accertamenti tecnici, che tenterà, in parole povere, di recuperare una "chiave di sblocco" dal personal computer dell'indagato e da lì, sbloccare l'Apple iOS sequestrato ed estrarne i contenuti. Tale chiave ha una validità di 30 giorni dall'ultimo sblocco del dispositivo.</p> <p>Nel caso in cui l'indagato fornisca il codice di sblocco, <u>non bisogna procedere a disabilitarlo.</u> Infatti in caso contrario andrebbero persi dati fondamentali quali le informazioni del servizio iOS Health (che riporta le informazioni relative ai passi compiuti e alla frequenza cardiaca associata dell'utente); le password memorizzate e le reti Wi-Fi associate al dispositivo.</p> <p><u>Chiedere infine all'utente se ha settato una password per eseguire backup mediante iTunes e invitarlo a riferirla.</u></p> <p><u>AGGIORNAMENTO: Un epocale jailbreak recente [acquisizione di diritti elevati nei dispositivi iPhone - funziona da iPhone 5 fino a X (esclusi XS, XR e 11)] consente di eseguire acquisizioni dell'intero contenuto di memoria degli iOS a patto che sia conosciuta la password utente. Tuttavia anche se sconosciuta potranno essere recuperati dati quali le informazioni relative alle configurazioni di sistema, tuttavia senza avere accesso ai database criptati ad esempio di Whatsapp</u></p>
Smartphone Android	<p>Anche per gli smartphone Android (Samsung, Huawei, etc.) nel caso in cui siano rinvenuti ACCESSI, è raccomandabile procedere all'isolamento degli stessi dalla rete, mediante inserimento modalità AEREO e/o rimozione SIM card, nonché preservarli ACCESSI alimentandoli con il caricabatteria appositamente sequestrato, fino al conferimento al personale specializzato.</p>
Smartphone BQ Aquaris Encrochat ²⁰ e/o smartphone SKYECC ²¹	<p>Di recente, si è assistito ad un notevole incremento di sequestri di questa particolare tipologia di dispositivi. Nelle more dello sviluppo di un'efficace tecnologia di contrasto alle complesse misure di sicurezza dagli stessi utilizzati si prega di:</p> <ol style="list-style-type: none"> 1. recuperare l'IMEI rimuovendo, ove possibile la batteria, dato che utilizzano spesso tecniche di dissimulazione del numero IMEI (cambia ad ogni accensione / spegnimento); 2. sfruttare adeguatamente l'effetto sorpresa nei confronti dell'indagato, durante le esecuzioni di perquisizioni / OCC, in quanto tali dispositivi supportano funzioni cd. "WIPE PANIC", che al digitare di un semplice sequenza numerica, cancellano definitivamente tutto quanto in esso

²⁰ <http://encrochat.network/>

²¹ <https://www.skyecc.com/>

	<p>contenuto;</p> <ol style="list-style-type: none"> 3. nel caso in cui vengano rinvenuti accessi, procedere a documentare tutto quanto viene visualizzato a schermo, mediante foto / video, tenuto conto che se il dispositivo dovesse spegnersi, tutto quanto in esso presente potrebbe cancellarsi / non essere più accessibile. 4. considerato che dopo 7 giorni, generalmente tali dispositivi (come avviene negli Apple iOS più recenti), disabilitano la porta USB, nonché tendenzialmente eliminano automaticamente le sessioni di chat criptate, in caso di disponibilità della password di sblocco (che da accesso alla ROM Virtuale), l'estrazione dati va fatta immediatamente, notiziando l'A.G. di tale necessità e il competente reparto tecnico.
--	--

N.B. NON CONSEGNARE IL PRESENTE MODULO ALL'INDAGATO, VA COMPILATO SOLO PER IL REPERTAMENTO E CONSEGNATO A SEGUIRE AL CONSULENTE TECNICO NOMINATO E/O ALLA P.G. INCARICATA DEGLI ACCERTAMENTI TECNICI.



OGGETTO: Verbale di perquisizione informatica, disposta con Decreto emesso da _____, il _____ a firma del Sost. Procuratore della Repubblica di _____, Dott. _____, in relazione al Proc. Pen. nr. _____.-

Il giorno ____/____/____, alle ore ____/____, in _____, presso gli uffici del _____.-

Il sottoscritto Ufficiale di P.G. _____, in servizio al Reparto in intestazione, riferisce alla competente A.G. quanto segue che:

In riferimento alla Decreto in oggetto, in data odierna, presso _____ ha proceduto alla perquisizione informatica dall'apparecchio _____, di proprietà/in suo a _____ quale indagato nel predetto Procedimento Penale, alla presenza del medesimo e del genitore (se minorenne).-

Si dà atto di aver reso edotto il sig. _____ dei motivi dell'operazione e della facoltà riconosciutagli di farsi rappresentare o assistere da un difensore di fiducia o altra persona purché prontamente reperibile ed idonea ad essere testimone ad atti del procedimento.-

Il sig. _____ ha rinunciato a tale facoltà / si è fatto appresentare o assistere dall'avv. _____

o dal Sig. _____ che è stato contattato telefonicamente alle ore ____ del _____ ed è giunto alle ore ____ del _____.-

Il difensore ha osservato / ha chiesto _____

Alle ore ____ del _____, si è dato quindi inizio alle operazioni.-

L'apparecchio, essendo stato sottoposto a sequestro in data _____ e repertato secondo le modalità previste, documentate con atto a parte, è già in possesso di questo Ufficio.-

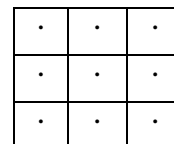
Ovvero

L'apparecchio che è nella disponibilità del sig. _____, lo consegna allo scrivente che accerta quanto segue:

- ✓ l'apparecchio è acceso/spento;
- ✓ Connesso alla linea telefonica TIM/WIND/VODAFONE ecc
- ✓ connesso ad internet/in modalità AEREO;
- ✓ con l'indicatore di carica della batteria al 10%

1. Ore ____ del _____, l'apparecchio viene acceso e viene rilevato che è bloccato da pin/password/segno *ovvero* privo di blocchi.-

Ore ____ del _____, l'apparecchio viene sbloccato con il pin/password _____ *ovvero* con il segno
fornito dal sig. _____



2. Ore ____ del _____, l'apparecchio viene posto in modalità "AEREO" *ovvero* viene

rilevato che è in modalità AEREO.-
3. Ore _____ del _____, l'apparecchio viene collegato alla rete elettrica mediante caricabatteria in uso all'operante/all'utilizzatore;
4. Ore _____ del _____ viene aperta l'App di messaggistica istantanea WhatsApp e viene rilevato quanto segue: - - - - Nella chat intercorsa con in soggetto avente <i>nickname</i> "XXXXXX" ovvero nella chat del gruppo denominato "XXXXXX" vengono rilevati una serie di messaggi vocali che vengono ascoltati, registrati e successivamente integralmente trascritti in quanto ritenuti d'interesse per le indagini.- Le registrazioni saranno salvate su apposito supporto informatico non riscrivibile DVD-R che viene allegato al presente verbale.- (Vedesi foto nr. 1, 2, 3, 4 del fascicolo fotografico allegato)
5. Ore _____ del _____ viene aperta l'App di gestione degli SMS rilevando quanto segue: - - - (Vedesi foto nr. 5, 6, 7, 8 del fascicolo fotografico allegato)
6. Ore _____ del _____ viene visionato il registro chiamate rilevando quanto segue: - - - (Vedesi foto nr. 9, 10, 11 del fascicolo fotografico allegato)
7. Ore _____ del _____ si procede allo spegnimento dell'apparecchio, in modalità AEREO con la batteria all'8%.-

Si dà atto che tali operazioni, eseguite in via ordinaria, potrebbero verosimilmente aver alterato il contenuto del telefono cellulare ed i dati in esso contenuti.

Le operazioni di ispezione del telefono cellulare vengono concluse alle ore _____ del _____.-

Il dispositivo (se non sottoposto a sequestro), viene immediatamente restituito al sig. _____.-

Si precisa che, all'interno dell'apparecchio era installato:

- Scheda SD da 4 Gb;
- SIMCARD nr. _____ / L'apparecchio è privo di SIM Card.-

Nel corso delle operazioni sopra descritte sono state riprodotte una serie di fotografie con le quale viene composto un fascicolo fotografico che costituisce parte integrante del presente verbale.-

Tanto si comunica per dovere d'Ufficio.-

Fatto, letto, confermato e sottoscritto in data e luogo di cui sopra. -

Le parti

Il difensore

L' Ufficiale di P.G.

BIBLIOGRAFIA

- La Digital Forensics nel processo penale di ICT Security Magazine pub. 2022.
- IISFA Memberbook 2023 Digital Forensics
 - *Cyber-crime Investigation, live-Forensics & cloud* pub.2023.
- IISFA Memberbook 2019-2020 DIGITAL FORENSICS pub. 2020
- Interpol Global Guidelines for Digital Forensics Laboratories
- Digital forensics. Guida per i professionisti delle investigazioni informatiche pub. 2021
- Cyber forensics e indagini digitali. Manuale tecnico-giuridico e casi pratici pub.2021
- Digital forensics autore Roberto Murenec pub. 2021
- Requirements and Guidelines for a complete end-to-end mobile forensic investigation chain March 2022 FORMOBILE





Ringraziamenti

*A “maoxlr8”, per il suo contributo di
revisore di ogni mio lavoro.*

Il dubbio è uno dei nomi dell'intelligenza.

- Jorge Luis Borges

La conoscenza è avere la risposta giusta. L'intelligenza è avere la domanda giusta.

- Anonimo

CScorza

Analista OSINT e Multimedia Digital Forensics, socio di OSINTITALIA, ha aperto un profilo GitHub ("CScorza"), dove raccoglie tools e strumenti di OSINT, Digital Forensics e Cyber Security, e un Canale Telegram pubblico denominato CScorza "Indagini Telematiche".