Strumenti open-source per l'informatica forense

Digital Forensics Talks — by ONIF —

ANDREA LAZZAROTTO

ANDREALAZZAROTTO.COM

Agenda

INTRODUZIONE ALLA DISCIPLINA

L’informatica forense e le sue fasi

ACQUISIZIONE FORENSE

Realizzare i vari tipi di copie

PARSING E ANALISI

Estrarre risposte dai dati

A proposito di me

- Laurea magistrale in Informatica
- Consulente informatico forense e sviluppatore
- Attività di ricerca sulla *WhatsApp forensics* e *anti-forensics* (manipolazione delle chat) e l'acquisizione e analisi dei metadati dei profili Instagram
- Autore di alcuni strumenti open-source, come **RecuperaBit** per la ricostruzione di NTFS e **Carbon14** per datare le pagine web (entrambi si trovano in CAINE)
- **Autore di Fuji,** il nuovo software open-source per l'acquisizione forense dei computer con macOS

Introduzione alla disciplina

L’INFORMATICA FORENSE E LE SUE FASI

Definizione

La *digital forensics* (informatica forense) è la disciplina scientifica che ha l'obiettivo di identificare, preservare, recuperare, analizzare e presentare fatti di natura digitale.

Questa materia riguarda sicuramente i reati informatici, ma più in generale tutti i casi nei quali compaiono computer, smartphone e altri dispositivi che memorizzano o trasmettono informazioni.

Le scienze forensi in generale servono per introdurre elementi scientifici validi come prove nei procedimenti civili o penali (principalmente, ma non solo).

LE FASI DELLA DIGITAL FORENSICS

https://doi.org/10.1007/978-3-030-33596-0_22

Cercando il concetto di *“digital forensics phases”* si trovano moltissimi schemi diversi, arrivando persino a 9 fasi.

Nella trattazione considereremo:

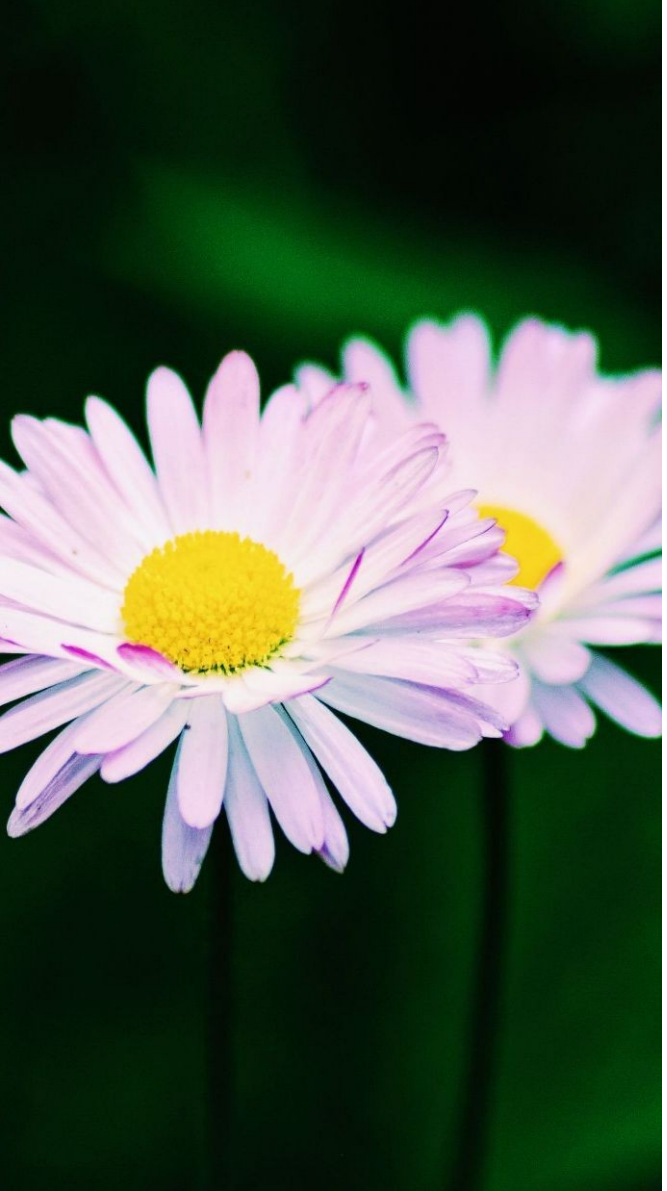
- Identificazione
- Acquisizione
- Esame e analisi
- Presentazione

Identificazione

Una volta arrivati sulla scena, è importantissimo determinare cosa deve essere considerato, ciò che è rilevante (cioè in genere può immagazzinare dati) e ciò che non lo è.

Quali sono i dispositivi che possono contenere dati?

- Computer
- Smartphone
- Chiavette USB
- ...



Acquisizione

La fase di acquisizione è cruciale per la realizzazione delle copie forensi, cioè la duplicazione del contenuto dei supporti che devono essere sottoposti ad analisi.

Infatti i reperti originali si toccano soltanto per fare le copie, le quali dovranno essere **"fissate" con il calcolo dell'hash.**

La funzione di hash genera un valore alfanumerico di lunghezza nota, il quale cambia totalmente alla minima modifica dell'input.

Questo permette di verificare a posteriori se la copia è genuina o se ha subito alterazioni.

Esame e analisi

Alcuni schemi dividono la fase di esame (cioè l'estrazione di specifici dati) da quella di analisi, vale a dire il lavoro intellettuale che vi attribuisce significato e risponde alle domande poste.

In ogni caso, la cosa fondamentale è **lavorare seguendo il metodo scientifico** e validare i dati, giustificando in modo corretto ogni conclusione che viene tratta.

Gli elementi che fanno la differenza sono la bravura, l'esperienza, l'intuito e la metodicità con cui si lavora.

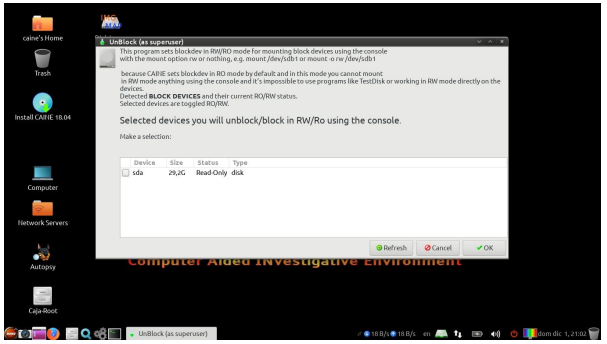
Bisogna evitare di fare il *"push-the-button forensic expert"*!

Presentazione

La relazione tecnica può essere prodotta come prova nei procedimenti civili, penali e non solo.

Riassume ciò che è stato svolto, nonché le analisi effettuate e all’interno il consulente trae le opportune conclusioni.

DISTRIBUZIONI LINUX ITALIANE

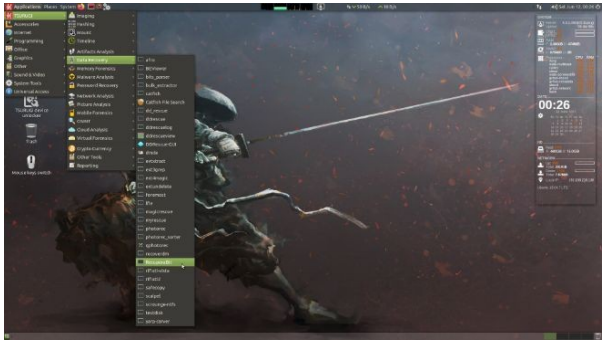


CAINE

Mantenuta da Nanni Bassetti, veloce e leggera, ideale per copie forensi “live”

DRIFT

Creata da Massimiliano Dal Cero nel 2026, con ottimo supporto al Secure Boot



Tsurugi

Sistema molto completo e ricco di programmi, anche per una workstation

Altre distribuzioni

CSI LINUX

Un buon mix di strumenti, anche per attività di OSINT

SIFT WORKSTATION

La soluzione “ufficiale” di SANS Institute

PALADIN LTE

Eccellente per acquisizioni forensi “live”, ma va precisato che non è open-source al 100%

Acquisizione forense

REALIZZARE I VARI TIPI DI COPIE

La copia forense

Le analisi forensi non vengono effettuate sui reperti originali (siano essi hard disk, smartphone o altro) ma si opera esclusivamente sulle copie.

L'esigenza è quella di **effettuare l'acquisizione di una copia che risulti *uguale* all'originale,** ma cosa significa "uguale"?

Per gli hard disk la risposta è abbastanza semplice: si effettua una copia "bit-a-bit", cioè ogni singolo bit del dispositivo viene clonato, compreso lo spazio non utilizzato.

Bisogna anche **garantire l'inalterabilità** della prova.

Tipi di acquisizione

COPIA BITSTREAM

Immagine bit-a-bit di tutto il dispositivo (preferita per i PC)

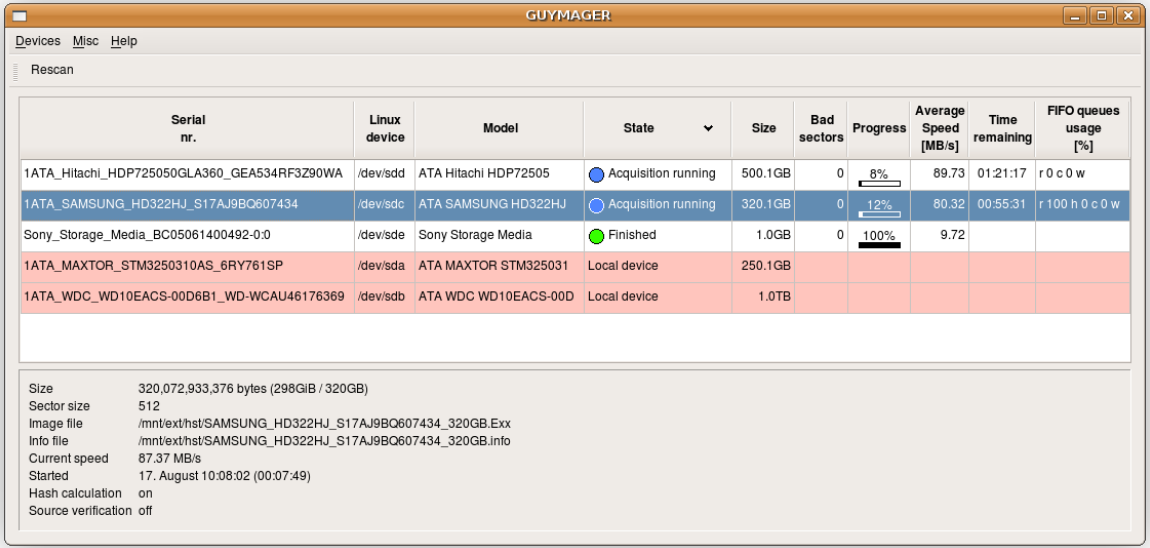
FULL FILE SYSTEM

Copia completa di tutti i file allocati

COPIA LOGICA

Acquisizione che comprende solo un certo insieme di file, oppure artefatti che il dispositivo “espone”

GUYMAGER



È un programma di acquisizione forense di dischi rigidi, già installato nelle principali distribuzioni del settore.

Consente di creare immagini nei formati EWF, AFF e RAW, calcolando gli hash automaticamente.

Usando la riga di comando

IL SEMPLICE “DD”

Disponibile su qualunque sistema operativo Linux o UNIX

DCFLDD

Versione potenziata, con funzionalità avanzate

DDRESCUE

Pensato per il recupero di dati da supporti danneggiati

Fuji: Forensic Unattended Juicy Imaging

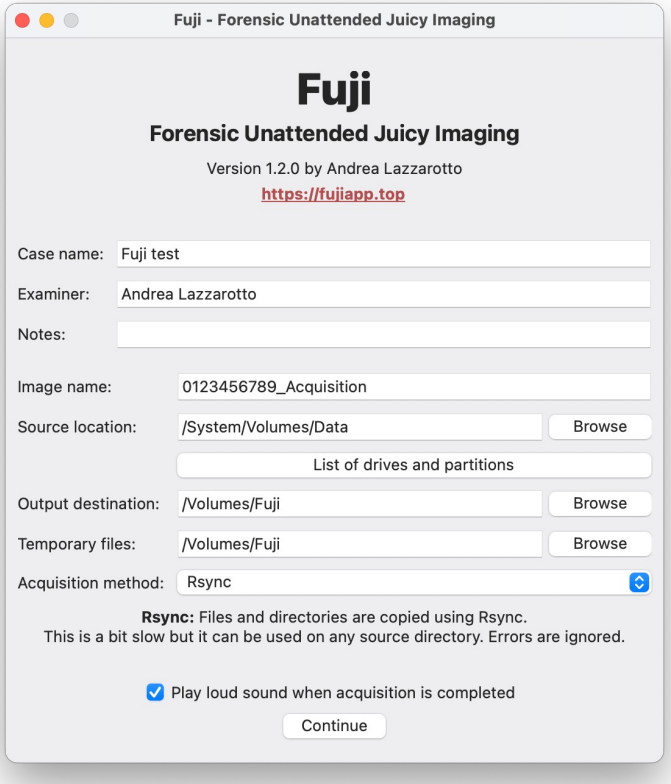
Fuji è un’applicazione per l'acquisizione forense dei Mac, che fornisce al consulente **un'immagine Full File System.**

Offre un'interfaccia grafica modulare, estensibile e facile da usare, che sfrutta vari strumenti di macOS. **È gratis e open-source.**

Fuji è anche una tipologia di mela

HTTPS://GITHUB.COM/LAZZA/FUJI

Interfaccia



DATI DEL CASO

SORGENTE E DESTINAZIONE

METODO DI ACQUISIZIONE

Foto gentilmente fornita da Derek Eiri
https://lazza.me/GB26
Macintosh HD
FujiApp
Options
Shut Down
Restart
LATO ESTERNO

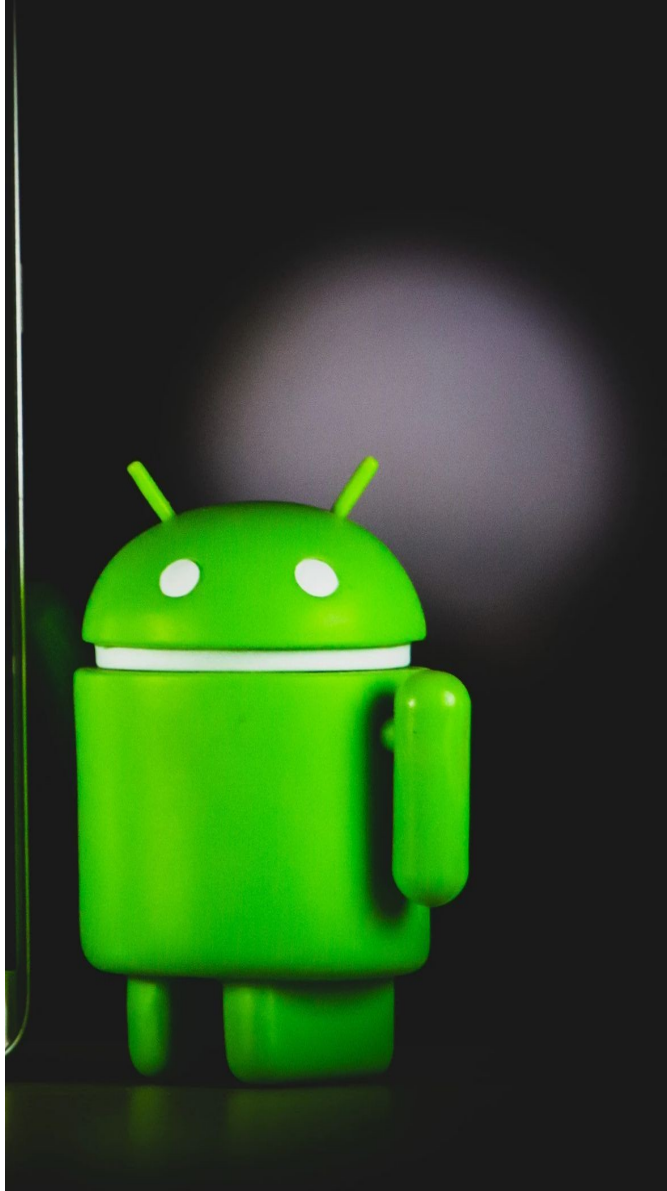
Acquisizione logica (Android)

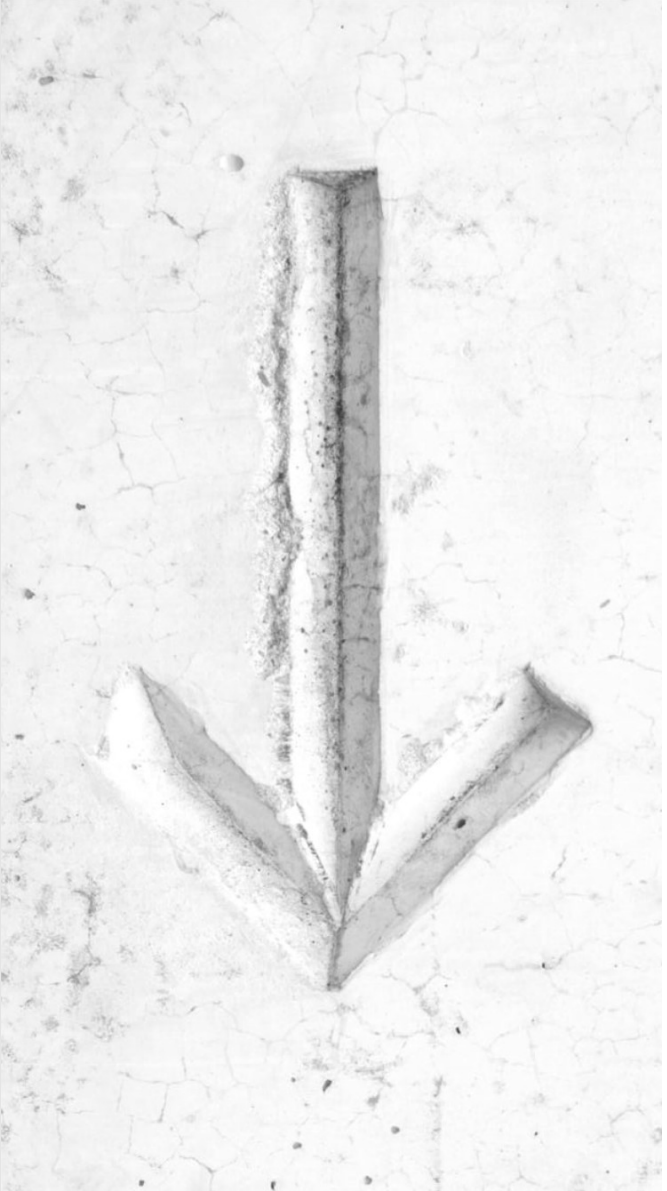
Gli smartphone Android sono un insieme vastissimo di dispositivi differenti. Per effettuare la copia logica **della maggior parte degli elementi** si utilizzano le funzioni di backup tramite ADB (*Android Debug Bridge*):

```
adb backup -apk -shared -all -system -f out.ab
```

Alcuni strumenti forensi usano un “agente” installato sul dispositivo per estrarre ulteriori elementi (come gli SMS).

HTTPS://ANDROID.STACKEXCHANGE.COM/Q/28296/68742





APK downgrade

Le app possono escludere i propri dati dal backup. Questo problema **a volte si aggira con l'APK downgrade.**

```
adb shell pm uninstall -k com.whatsapp
```

A questo punto, l'app è stata rimossa (ma non i dati). Se il dispositivo ha una versione di Android superiore alla 6.0 **bisogna riavviare lo smartphone.**

Poi si installa un APK più vecchio che abbia la funzione di backup attiva, e si procede come già spiegato.

HTTPS://BLOG.SALVATIONDATA.COM/2018/08/06/CASE-STUDY/

Acquisizione logica (iOS)

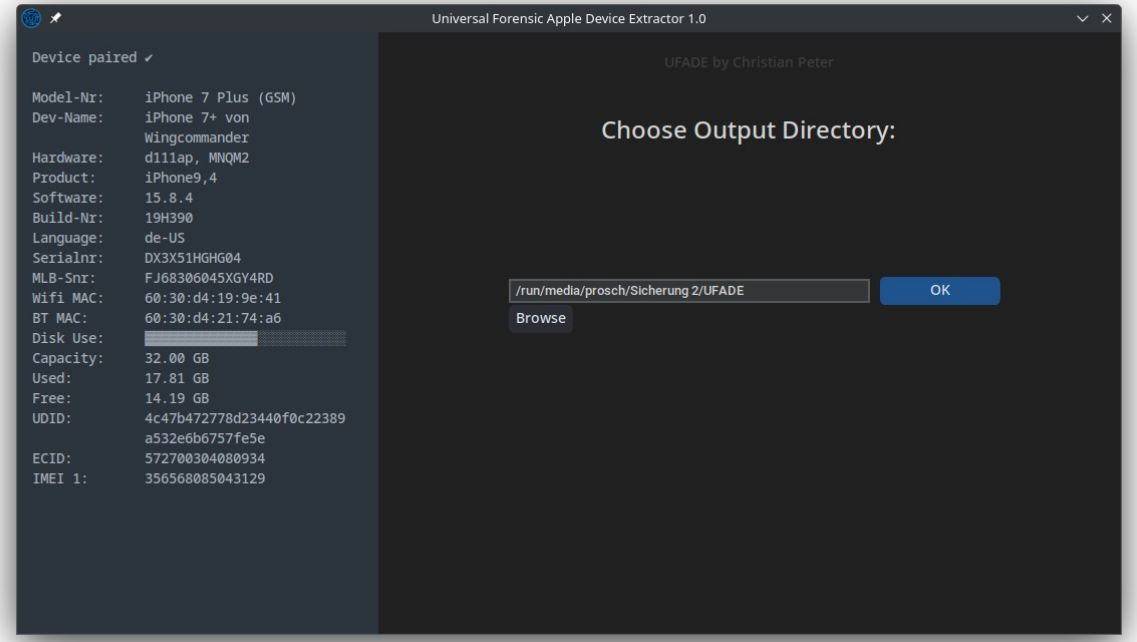
Nel caso di iOS esistono solo pochi modelli di telefono e il funzionamento è del tutto omogeneo.

L'acquisizione logica viene effettuata usando il protocollo di backup ufficiale di iTunes.

Tutti i software forensi usano questo sistema per le copie logiche. Per un'opzione a riga di comando, si può optare per *libimobiledevice* presente anche in Tsurugi.

In genere i backup iTunes **contengono moltissimi dati,** compresi quelli di quasi tutte le app di interesse.

UFADE



https://github.com/prosch88/UFADE

È uno strumento per l'estrazione forense da dispositivi mobili Apple, utilizzabile su tutte le piattaforme.

Permette di creare **backup in stile iTunes o acquisizioni "advanced logical"** compatibili con la suite commerciale Cellebrite UFED.

Acquisizione di pagine web

ArchiveWeb.page è un'applicazione che permette di archiviare (e poi riaprire) le pagine web.

Il formato WACZ è uno standard aperto utilizzato per l'attività di registrazione e conservazione dei contenuti web al fine di preservarne l'integrità, basato sul precedente WARC.

Si tratta di **uno dei formati raccomandati dalla Biblioteca del Congresso degli Stati Uniti d'America** per gli archivi web.

HTTPS://ARCHIVEWEB.PAGE

ALTRI STRUMENTI

mitmproxy

Eccellente per analizzare e registrare flussi HTTP

Wireshark

Può registrare il traffico di rete e ispezionare i protocolli

Carbon14

Serve a stimare la data di pubblicazione di una pagina

Parsing e analisi

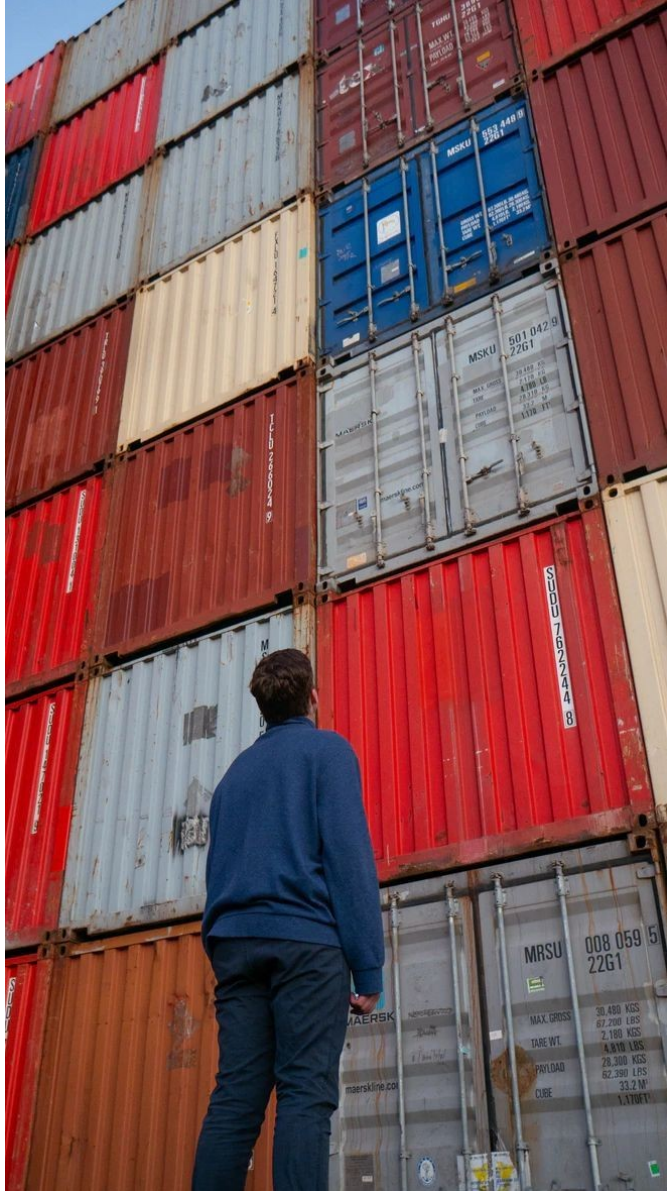
ESTRARRE RISPOSTE DAI DATI

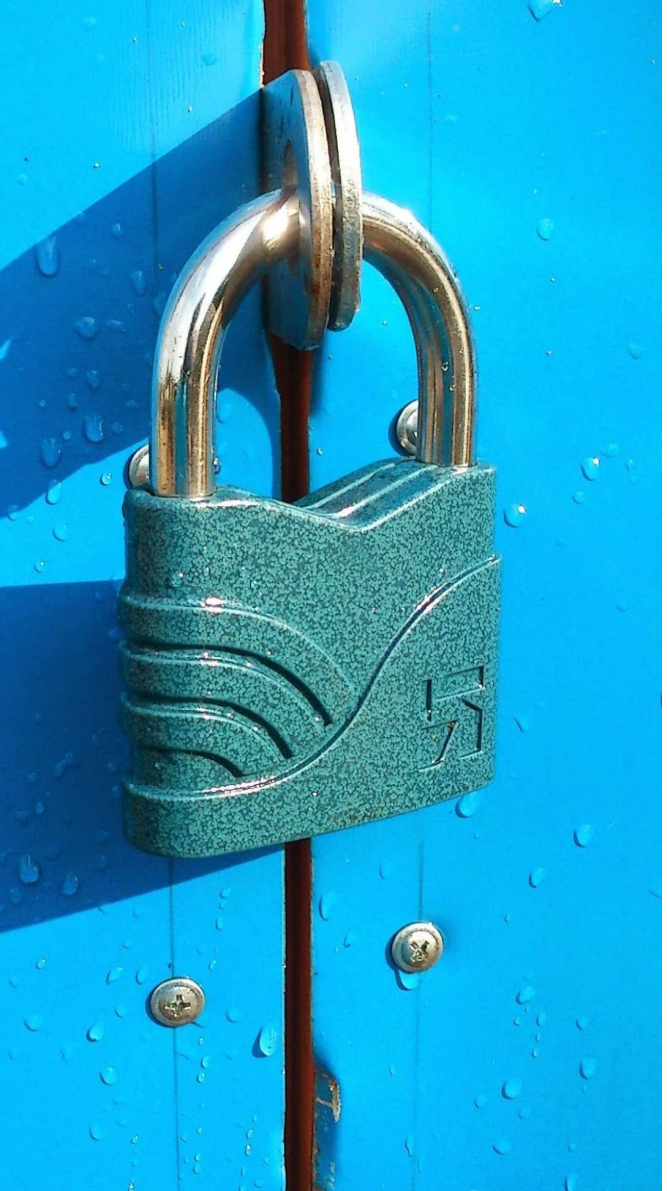
Problemi operativi

Col passare del tempo la capacità delle memorie diventa sempre più elevata, conseguentemente ci si trova a dover analizzare moltissimi dati.

Una volta ho letto una relazione tecnica americana scritta verso la fine degli anni ‘90: il PC analizzato aveva **un unico hard disk di 10 GB.** Oggi il mio smartphone ne ha 256.

Inoltre, bisogna tenere presente che i dati e i documenti potrebbero essere memorizzati con formati proprietari, o comunque poco conosciuti e non supportati dagli strumenti.





Dati nascosti o protetti

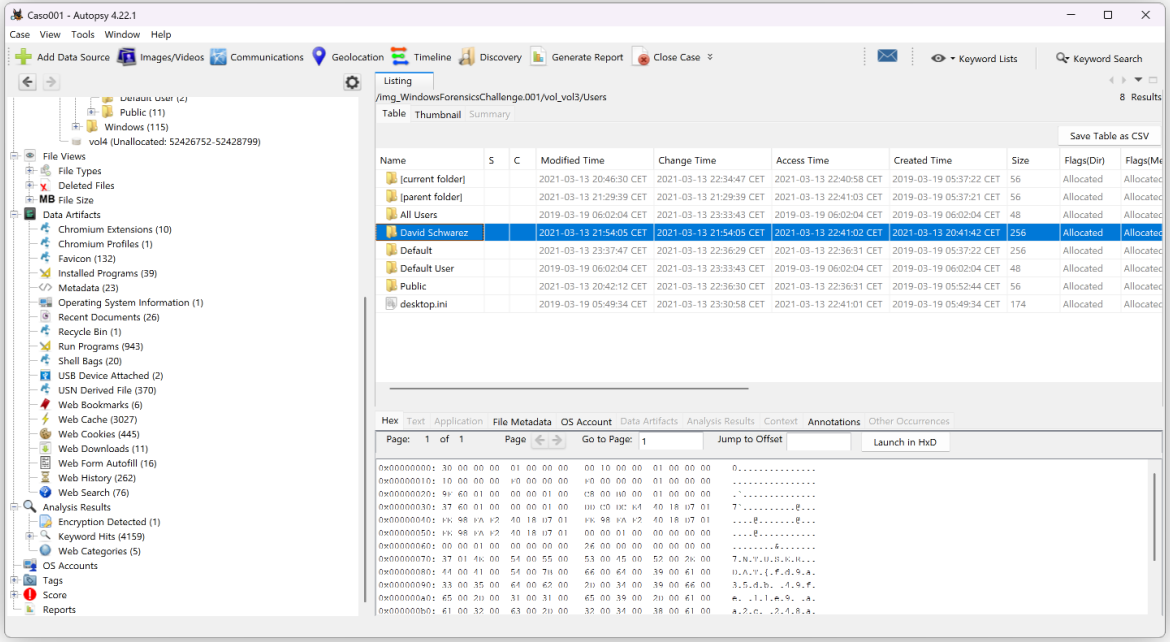
Oltre alle protezioni crittografiche, gli utenti più smaliziati potrebbero usare altri trucchi per nascondere dei dati.

A volte un semplice **cambio di estensione** potrebbe ingannare qualcuno, per esempio spostando un archivio ZIP in una cartella di sistema con il nome di una DLL.

Su NTFS i file possono avere più di un contenuto dati. Gli *Alternate Data Stream* sono accessibili aggiungendo ":" dopo il nome principale del file: `appunti.txt:calc.exe`

Qualcosa potrebbe sfuggire!

AUTOPSY



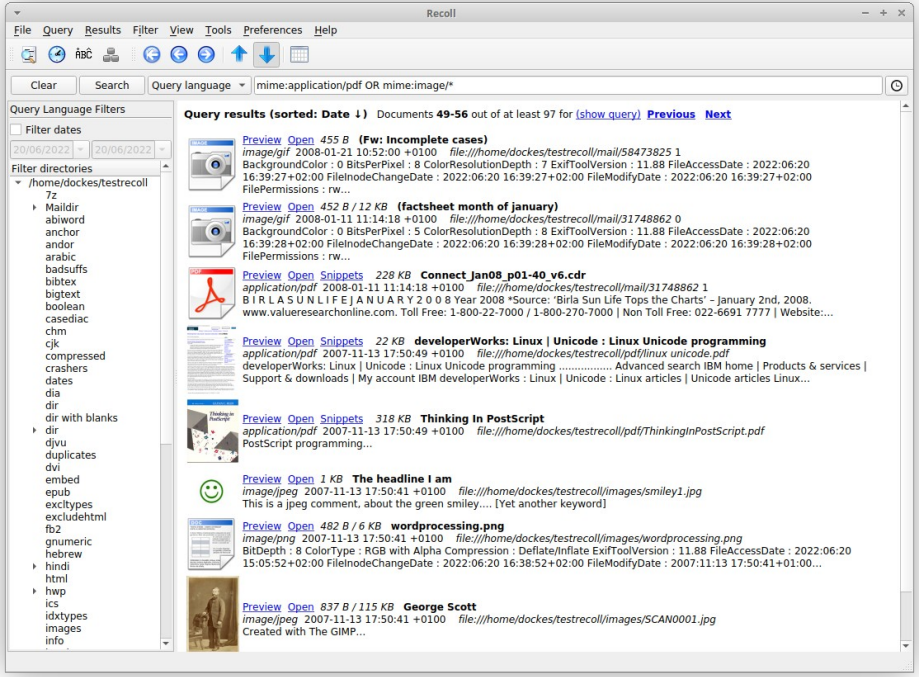
https://www.autopsy.com

Autopsy è una suite open-source molto completa per la *computer forensics*.

Consente di estrarre artefatti e indicizzare i file, creare dei segnalibri e infine generare report in diversi formati.

Un’alternativa interessante è IPED.

RECOLL

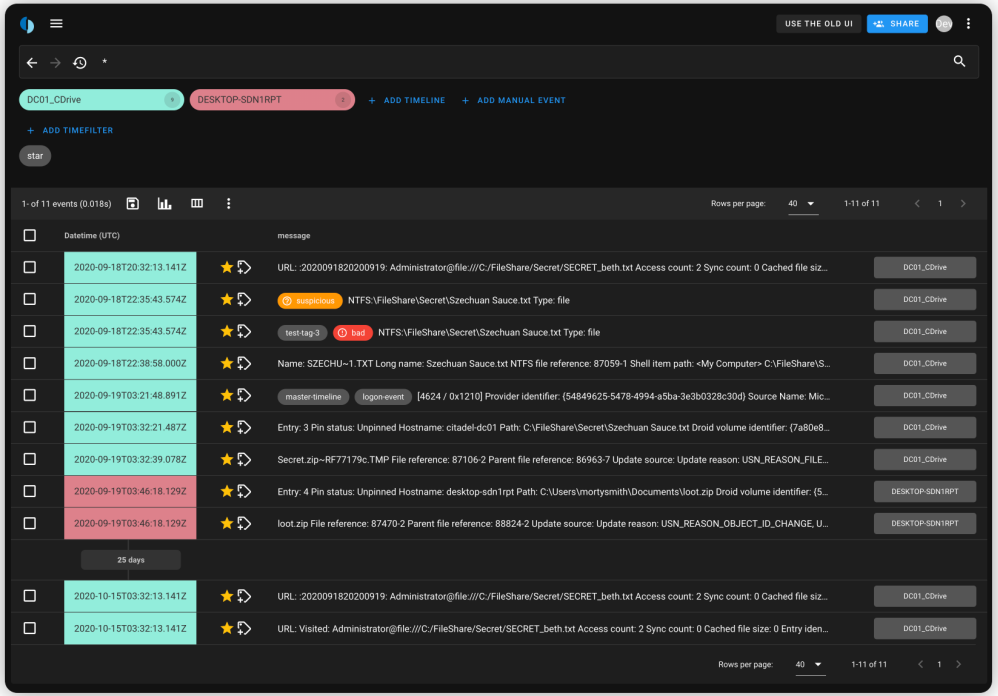


https://www.recoll.org

È un software libero di ricerca *full-text* che indicizza e analizza documenti, email e archivi compressi in numerosi formati.

Permette di effettuare ricerche mirate su grandi volumi di dati, in modo più rapido rispetto ad Autopsy.

TIMESKETCH



https://timesketch.org

Descritto come uno strumento open-source per l'analisi forense collaborativa delle *timeline*.

Il principale punto di forza è il **supporto nativo per le *timeline* generate da Plaso.**

Include funzionalità avanzate di filtraggio e *tagging*.

Recupero dati

TESTDISK

Permette il ripristino di partizioni perse o file cancellati

PHOTOREC

Recupera foto e documenti tramite *carving*

RECUPERABIT

Effettua la ricostruzione forense avanzata di partizioni NTFS corrotte, inoltre permette il recupero dei file

Dispositivi mobili

Dopo l'acquisizione, quasi tutto il lavoro di analisi si basa sull'esame dei **dati contenuti nelle app.**

Le suite di *digital forensics* fanno "a gara" per supportare il maggior numero possibile di applicazioni, ma può capitare di **dover analizzare manualmente i dati di un'app,** perché non è supportata o per verificare meglio.

Alcuni progetti open-source si specializzano nell'analisi dei dati di specifiche applicazioni.

File multimediali

Il contenuto delle foto e delle miniature può risultare molto importante, specialmente perché le fotografie rappresentano una documentazione dei fatti potenzialmente ricca di dettagli e possono avere un buon grado di attendibilità.

Possiamo anche analizzare i metadati EXIF per ottenere ulteriori informazioni sul dispositivo utilizzato, la data e l'ora di scatto e la posizione GPS (se presente):

```
exiftool IMG_1234.jpg
```

MVT: Mobile Verification Toolkit

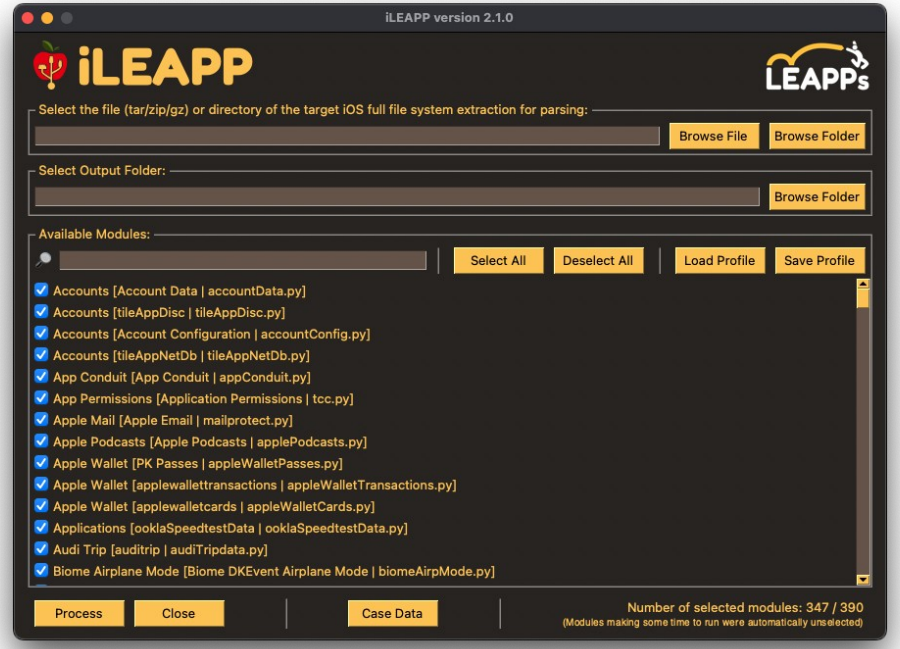
MVT è uno strumento open-source di analisi forense consensuale di dispositivi iOS e Android.

Il progetto è stato sviluppato da Amnesty International, principalmente per **individuare tracce di spyware** particolarmente insidiosi, come Pegasus.

Automatizza la raccolta e l'analisi dei dati dai dispositivi, confrontandoli con gli indicatori di compromissione pubblicati dai ricercatori.

HTTPS://MVT.RE

ALEAPP E ILEAPP



https://github.com/abrignoni

Sono strumenti di analisi per Android e iOS sviluppati da Alexis Brignoni.

Estraggono artefatti quali cronologia, messaggi, dati sulle posizioni GPS e uso delle app.

Generano report in formato HTML.

PUNTI CHIAVE

Verificabilità

Il codice aperto garantisce trasparenza e possibilità di verifica scientifica

Accessibilità

La disponibilità libera promuove la formazione e la diffusione di buone pratiche

Indipendenza

Queste soluzioni preservano l'indipendenza dai *vendor* e la sovranità digitale

CONTATTI

Web

andrealazzarotto.com

GitHub

Lazza

Social link

bio.lazza.me