Dalla copia live alla Fuji Cartridge

LA NUOVA FRONTIERA DELL'ACQUISIZIONE FORENSE DEI MAC

ANDREA LAZZAROTTO

ANDREALAZZAROTTO.COM

Tanto tempo fa...

Quando mi sono avvicinato all'informatica forense circa dieci anni fa, i computer potevano essere acquisiti facilmente.

Bastava avere un *write blocker* o una distribuzione Linux forense, come CAINE o Tsurugi. Si poteva ricavare un'acquisizione EWF o anche **usare semplicemente dd.**

Non era fantastico?

Agenda

INTRODUZIONE

Ostacoli all’acquisizione forense di macOS

FUNZIONI E NOVITÀ

Tutto ciò che Fuji può fare per voi

PROCESSO DI SVILUPPO

Come è stato realizzato

A proposito di me

- Laurea magistrale in Informatica
- Consulente informatico forense e sviluppatore
- Attività di ricerca sulla *WhatsApp forensics* 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 programma open-source per l'acquisizione forense facile dei computer con macOS

Introduzione

OSTACOLI ALL'ACQUISIZIONE FORENSE DI MACOS

I nuovi Mac

Apple ha introdotto la crittografia hardware con il chip T2 nel 2017 e l'ha perfezionata con Apple Silicon alla fine del 2020.

Inoltre, tutti i Mac moderni hanno unità di archiviazione saldate alla scheda madre.

Il mio studio è iniziato perché non sapevo molto sull'analisi forense dei Mac. Volevo capire meglio le tecniche di acquisizione per i computer Apple moderni.

Apple Silicon

I modelli recenti usano un’architettura ARM, non x64.

Dopo diversi tentativi di personalizzare le partizioni di ripristino di macOS, mi sono reso conto che era inutile.

Questi Mac non possono avviare distribuzioni Linux forensi, anzi non possono avviare del tutto sistemi operativi esterni:

*Yes, you can create a bootable installer [...], **but your Mac won't actually start up from it.** Instead, it will start up from an internal copy of macOS Recovery, and only leverage your bootable installer when you choose to reinstall macOS.*

HTTPS://DISCUSSIONS.APPLE.COM/THREAD/254091163

Un nuovo paradigma

Non possiamo ottenere un’immagine fisica (decifrabile).

È utile pensare all’acquisizione dei Mac con Apple Silicon **come se fosse quella degli smartphone.**

Quando non è possibile ottenere un’immagine fisica, ci sforziamo di ottenere un’estrazione Full File System (FFS) mentre il dispositivo è acceso.

Faccio sempre
ciò che non so fare
per imparare come va fatto.

VINCENT VAN GOGH

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.**

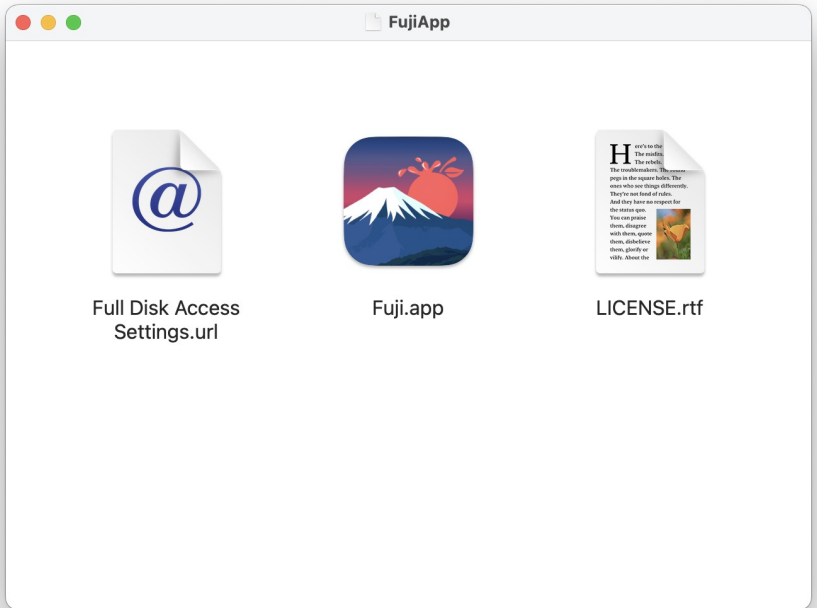
Fuji è anche una tipologia di mela

HTTPS://FUJIAPP.TOP

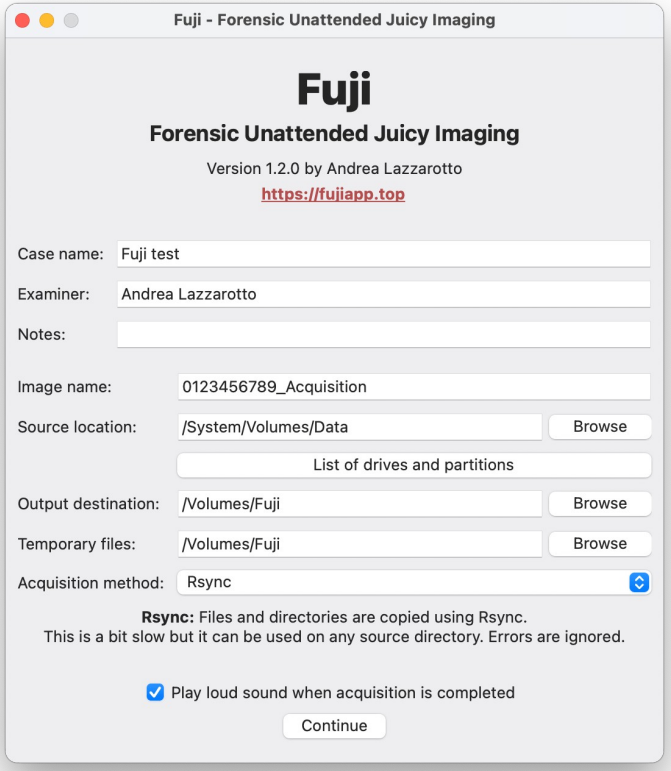
Funzioni e novità

TUTTO CIÒ CHE FUJI PUÒ FARE PER VOI

CONTENUTO DEL FILE DMG



Interfaccia

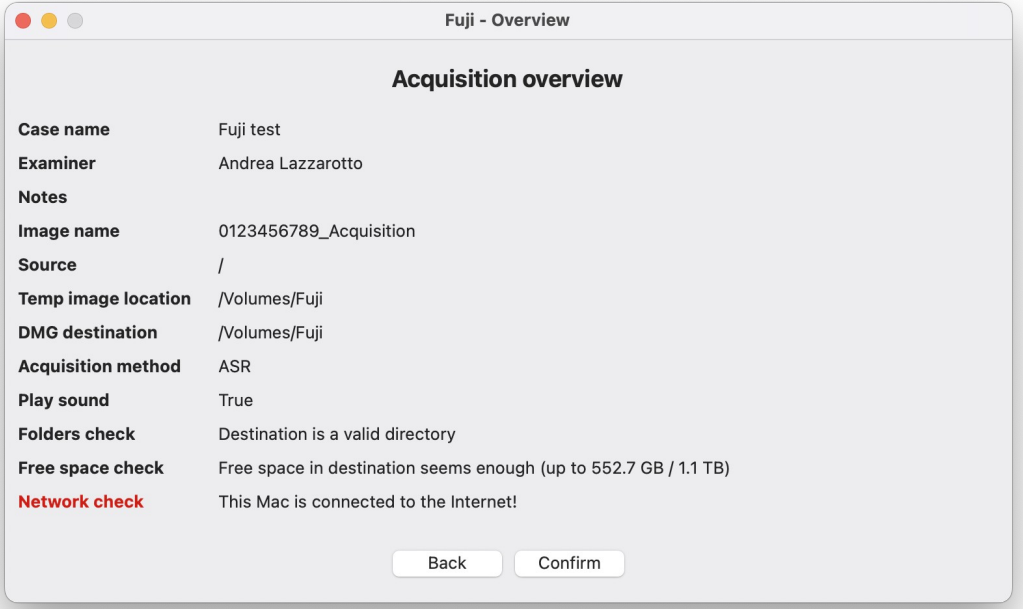


DATI DEL CASO

SORGENTE E DESTINAZIONE

METODO DI ACQUISIZIONE

FINESTRA DI RIEPILOGO



FINESTRA DI ACQUISIZIONE

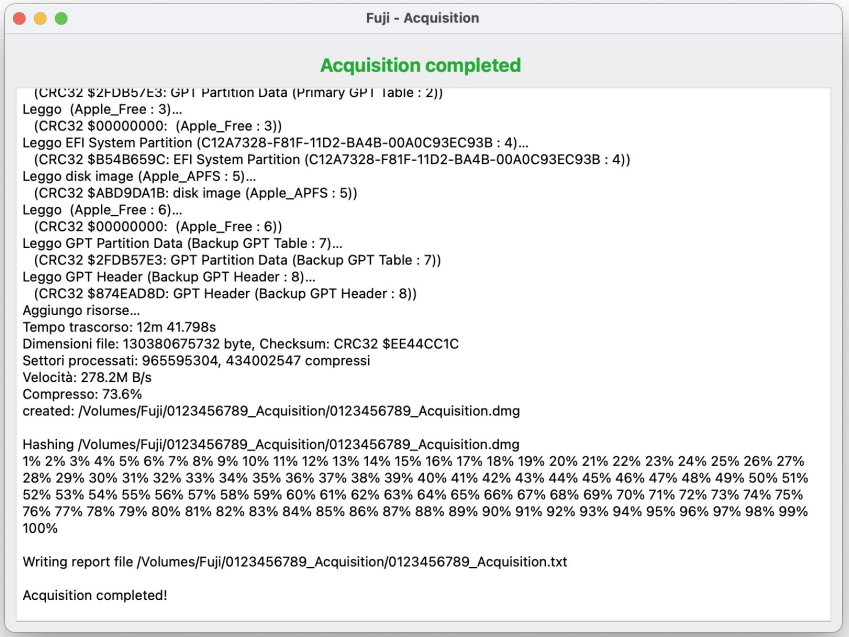



Foto gentilmente fornita da Derek Eiri
https://lazza.me/GB26
Macintosh HD
FujiApp
Options
Shut Down
Restart
LATO ESTERNO

Avvio con Fuji Cartridge

L’immagine DMG di Fuji 1.2.0 è compatibile con balenaEtcher e può essere scritta su **qualunque pendrive USB da 256 MB.**

Partendo all’avvio del Mac, Fuji si copia in un RAM disk e **la porta USB torna libera.**

Se il computer non ha FileVault attivo, non è necessario conoscere la password.

HTTPS://FUJIAPP.TOP

Rsync

I file vengono copiati in un’immagine disco con Rsync:

- Utility UNIX collaudata
- Elaborazione un po’ più lenta
- **Funziona con qualsiasi directory sorgente**
- Non fallisce per piccoli problemi del file system
- I file che non possono essere copiati vengono saltati

Disponibile in modalità live

Ditto

I file vengono copiati in un’immagine disco con Ditto:

- Utility di macOS presente su tutte le versioni
- Elaborazione un po’ più lenta
- **Funziona con qualsiasi directory sorgente**
- Può bloccarsi se subentra la protezione dati di macOS
- I file che non possono essere copiati vengono saltati

Disponibile in modalità recovery

ASR

Clone fatto tramite Apple Software Restore:

- Metodo di backup “ufficiale” Apple
- **Procedura più veloce**
- Funziona solo su volumi interi
- Può fallire in caso di errori nel file system
- Pieno di bug su macOS 13 (Ventura)

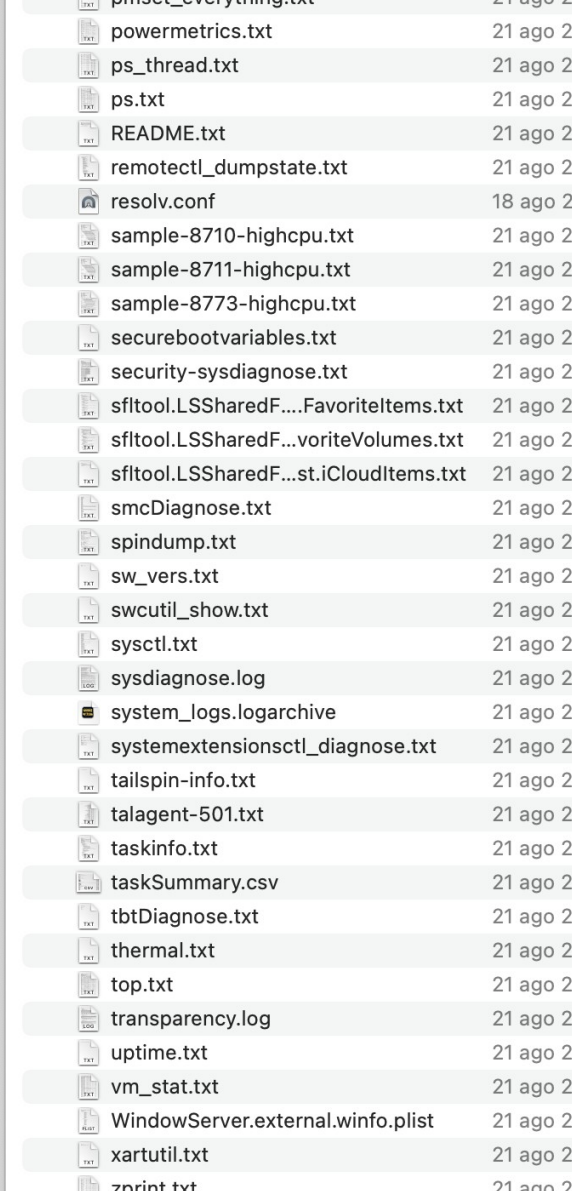
Sempre disponibile

Sysdiagnose and logs

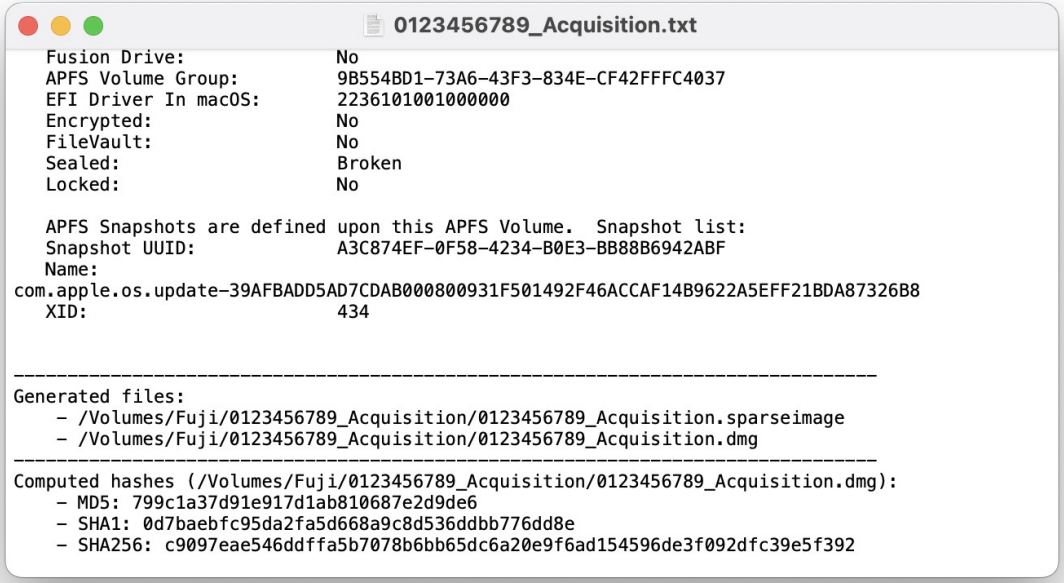
L'acquisizione include dati di sistema e registri:

- Non è un'immagine completa del file system
- Elabora informazioni su processi, rete e attività dei file
- Molti altri dati che non ci stanno nello screenshot
- Include gli *unified log* in formato *logarchive*
- **Fuji li converte in JSONL per voi**

Disponibile in modalità live



RISULTATO



Fuji genera un report e un file DMG in sola lettura contenente tutti i dati acquisiti.

Può essere aperto in Autopsy, FTK Imager o in molti dei vostri strumenti preferiti.

La documentazione include istruzioni per convertire il formato.

Finalmente le FFOO nazionali possono affrontare i complessi scenari del mondo macOS senza dover ricorrere a costosi software commerciali.

ANONIMO
GUARDIA DI FINANZA

Ho dovuto gestire un Mac con macOS 10.13, bloccato in un “limbo” di crittografia nonostante FileVault fosse disattivato. Con Fuji, sono riuscito ad acquisire un file DMG con l'intero contenuto del file system.

ISMAELE DI NATALE
FORENSIC EXPERT, VINTEK ENGINEERING

COMPATIBILITÀ CON I SISTEMI OPERATIVI

10.10+

Rsync e Ditto

Le opzioni più compatibili: funzionano con qualsiasi Mac uscito negli ultimi dieci anni

11+

ASR e Sysdiagnose

Entrambi i metodi possono essere utilizzati sui nuovi Mac, Apple Silicon e Intel

Processo di sviluppo

COME È STATO REALIZZATO

Tecnologie

Fuji è sviluppato utilizzando Python 3.10, e ogni metodo di acquisizione deriva da una classe base che contiene la **logica condivisa.**

L'interfaccia utente utilizza wxPython. È stata sviluppata con l'aiuto di ChatGPT e Duck AI.

Il programma invoca diversi strumenti nativi di macOS, tra cui **asr, ditto, rsync, sysdiagnose, hdiutil e diskutil.**

Acquisire i permessi

Il file DMG include un link per aprire le impostazioni di *Accesso completo al disco*:

```
[InternetShortcut]
URL=x-apple.systempreferences:com.apple.preference.security?Privacy_AllFiles
```

I permessi di root vengono richiesti con:

```
security execute-with-privileges "./Fuji.bin"
```

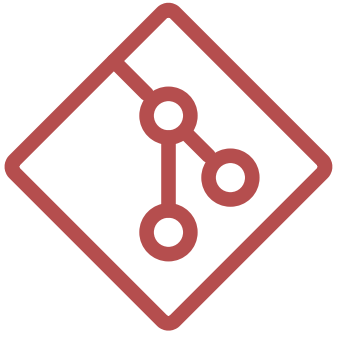
Costruire il file DMG

Fuji viene assemblato in un'app macOS con PyInstaller. Lo script di base è stato modificato per eseguire queste azioni:

- Compilare l'app
- Rinominare il file binario
- Copiare l'assistente per i permessi di root
- Preparare il file DMG utilizzando `dmgbuild`

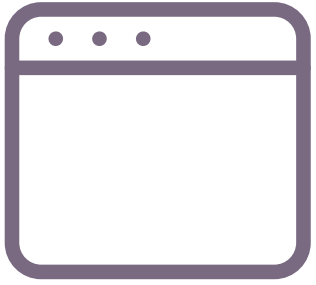
Passiamo da codice sorgente a DMG **in un comando.**

PUNTI CHIAVE



Open-source

Il funzionamento interno può essere verificato. Niente scatole nere.



Semplice

La maggior parte del codice riguarda l'interfaccia. Può essere facilmente esteso.

Inestimabile

Fuji vi fa risparmiare tempo e denaro. Installatelo ovunque vogliate, senza dongle.

CONTATTI

Web

andrealazzarotto.com

GitHub

Lazza

Social link

bio.lazza.me