

Fuji

La soluzione open-source per la copia forense
dei Mac con processori Intel e Apple Silicon

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

FUNZIONALITÀ E UTILIZZO

Tutto ciò che Fuji può fare per voi

PROCESSO DI SVILUPPO

Tecnologie utilizzate e progetti futuri

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

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 M1, M2, ecc... 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.



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.

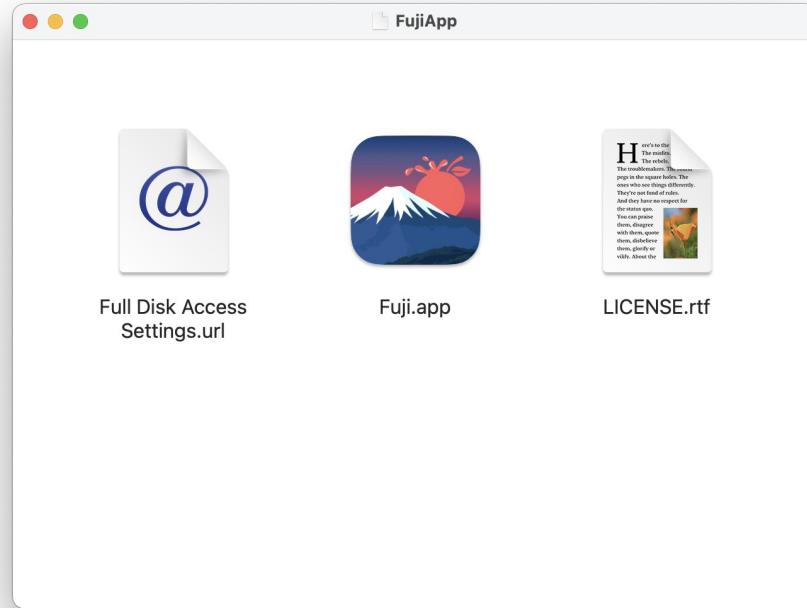


[HTTPS://GITHUB.COM/LAZZA/FUJI](https://github.com/Lazza/FUJI)

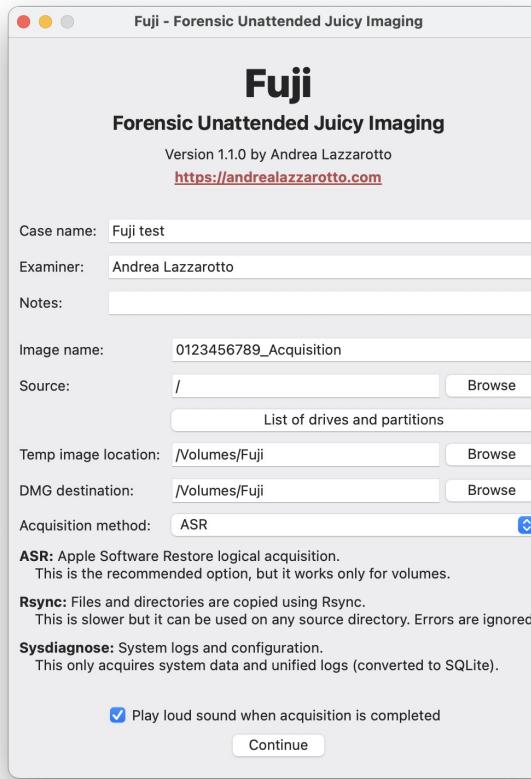
Funzionalità e utilizzo

TUTTO CIÒ CHE FUJI PUÒ FARE PER VOI

CONTENUTO DEL FILE DMG



Interfaccia

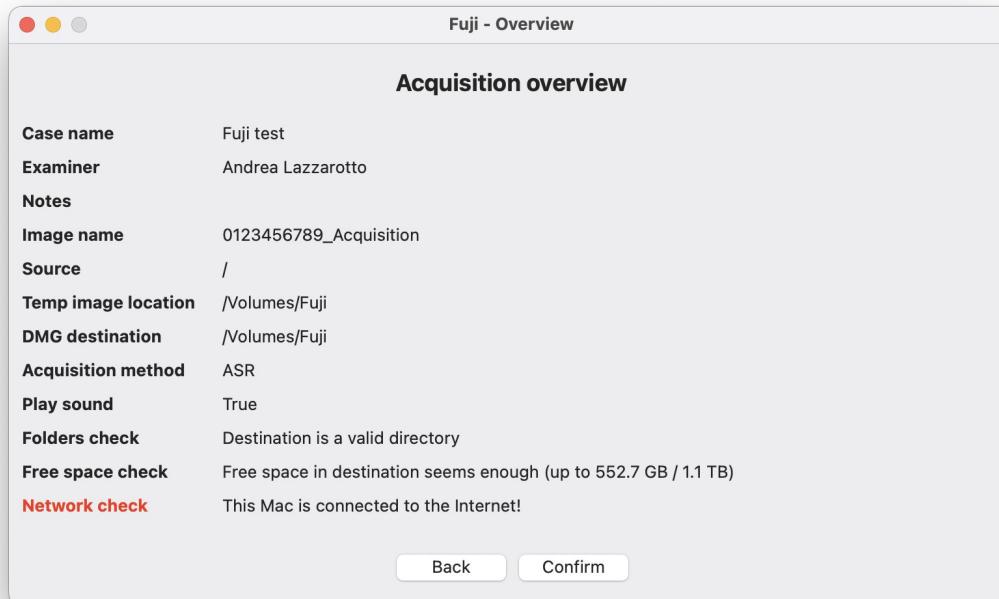


DATI DEL CASO

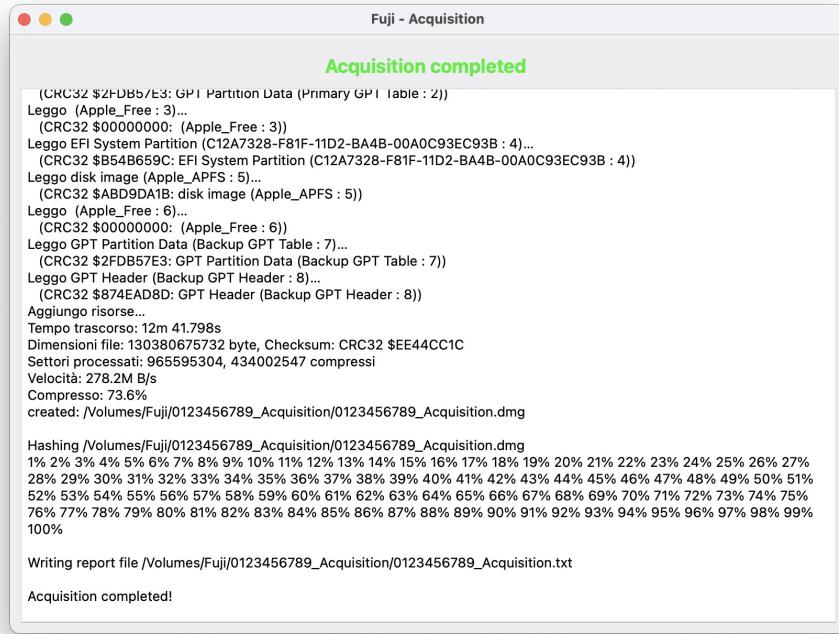
SORGENTE E DESTINAZIONE

METODO DI ACQUISIZIONE

FINESTRA DI RIEPILOGO



FINESTRA DI ACQUISIZIONE



ASR

Clone fatto tramite Apple Software Restore:

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

Rsync

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

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

Sysdiagnose



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 SQLite per voi

Nome	Data di modifica
pluginkit-501.txt	21 ago 2024, 23:55
pmset_everything.txt	21 ago 2024, 23:55
powermetrics.txt	21 ago 2024, 23:55
ps_thread.txt	21 ago 2024, 23:54
ps.txt	21 ago 2024, 23:54
README.txt	21 ago 2024, 23:54
remotectl_dumpstate.txt	21 ago 2024, 23:55
resolv.conf	18 ago 2024, 18:36
sample-8710-highcpu.txt	21 ago 2024, 23:55
sample-8711-highcpu.txt	21 ago 2024, 23:55
sample-8773-highcpu.txt	21 ago 2024, 23:55
securebootvariables.txt	21 ago 2024, 23:55
security-sysdiagnose.txt	21 ago 2024, 23:55
sfltool.LSSharedF....FavoriteItems.txt	21 ago 2024, 23:55
sfltool.LSSharedF...voriteVolumes.txt	21 ago 2024, 23:55
sfltool.LSSharedF...st.iCloudItems.txt	21 ago 2024, 23:55
smcDiagnose.txt	21 ago 2024, 23:55
spindump.txt	21 ago 2024, 23:56
sw_vers.txt	21 ago 2024, 23:55
swutil_show.txt	21 ago 2024, 23:55
sysctl.txt	21 ago 2024, 23:55
sysdiagnose.log	21 ago 2024, 23:56
system_logs.logarchive	21 ago 2024, 23:56
systemextensionsctl_diagnose.txt	21 ago 2024, 23:55
tailspin-info.txt	21 ago 2024, 23:54
talagent-501.txt	21 ago 2024, 23:55
taskinfo.txt	21 ago 2024, 23:54
taskSummary.csv	21 ago 2024, 23:56
tbtDiagnose.txt	21 ago 2024, 23:55
thermal.txt	21 ago 2024, 23:55
top.txt	21 ago 2024, 23:55
transparency.log	21 ago 2024, 23:55
uptime.txt	21 ago 2024, 23:55
vm_stat.txt	21 ago 2024, 23:55
WindowServer.external.winfo.plist	21 ago 2024, 23:55
xartutil.txt	21 ago 2024, 23:55
zprint.txt	21 ago 2024, 23:55
system_logs.db	22 ago 2024, 00:13

RISULTATO

```
Fusion Drive: No
APFS Volume Group: 9B5548D1-73A6-43F3-834E-CF42FFFC4037
EFI Driver In macOS: 2236101001000000
Encrypted: No
FileVault: No
Sealed: Broken
Locked: No

APFS Snapshots are defined upon this APFS Volume. Snapshot list:
Snapshot UUID: A3C874EF-0F58-4234-B0E3-BB88B6942ABF
Name:
com.apple.os.update-39AFBADD5AD7CDAB000800931F501492F46ACCAF14B9622A5EFF21BDA87326B8
XID: 434

-----
Generated files:
- /Volumes/Fuji/0123456789_Acquisition/0123456789_Acquisition.sparseimage
- /Volumes/Fuji/0123456789_Acquisition/0123456789_Acquisition.dmg

-----
Computed hashes (/Volumes/Fuji/0123456789_Acquisition/0123456789_Acquisition.dmg):
- MD5: 799c1a37d91e917d1ab810687e2d9de6
- SHA1: 0d7baebfc95da2fa5d668a9c8d536ddbb776dd8e
- SHA256: c9097eae546ddffa5b7078b6bb65dc6a20e9f6ad154596de3f092dfc39e5f392
```

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.

Alla fine potete eliminare la sparse image temporanea.

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

L'opzione più compatibile: funziona con qualsiasi Mac uscito negli ultimi dieci anni.

11+

ASR e Sysdiagnose

Entrambi i metodi sono particolarmente adatti ai nuovi Mac, Apple Silicon e Intel.

Processo di sviluppo

TECNOLOGIE UTILIZZATE E PROGETTI FUTURI

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, 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.**



Progetti futuri

AUMENTARE LA COMPATIBILITÀ

Testare e migliorare la compatibilità di ASR e Sysdiagnose sulle versioni legacy di OS X.

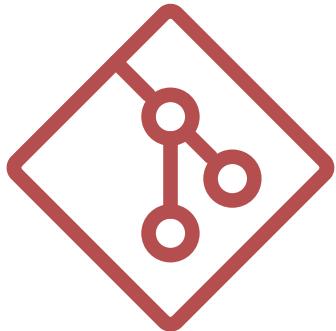
MIGLIORAMENTI ALL'INTERFACCIA UTENTE

Alcuni aspetti probabilmente possono essere migliorati.

AMBIENTE DI RECUPERO

Servono altri test per verificare quali funzioni di Fuji possono essere usate avviando il Mac in modalità di recupero.

PUNTI CHIAVE



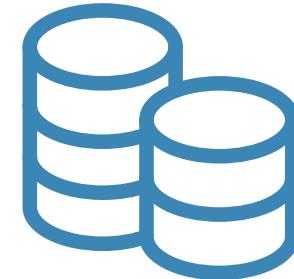
Open-source

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

X / Twitter

[@thelazza](https://twitter.com/thelazza)

Mastodon

[@lazza@mastodon.social](https://mastodon.social/@lazza)

