



# 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](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](https://FUJIAPP.TOP)

# **Funzioni e novità**

TUTTO CIÒ CHE FUJI PUÒ FARE PER VOI



# Interfaccia

The screenshot shows the Fuji application window with the following fields and options:

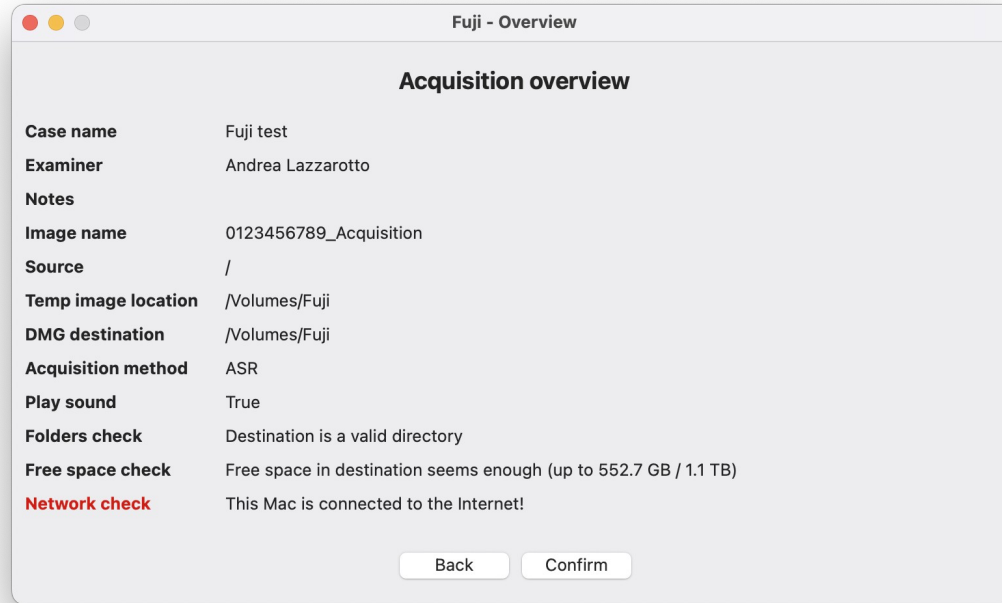
- Title Bar:** Fuji - Forensic Unattended Juicy Imaging
- Header:** Fuji, Forensic Unattended Juicy Imaging, Version 1.2.0 by Andrea Lazzarotto, <https://fujiapp.top>
- Case name:** Fuji test
- Examiner:** Andrea Lazzarotto
- Notes:** (empty text area)
- Image name:** 0123456789\_Acquisition
- Source location:** /System/Volumes/Data (with a Browse button and a "List of drives and partitions" button below it)
- Output destination:** /Volumes/Fuji (with a Browse button)
- Temporary files:** /Volumes/Fuji (with a Browse button)
- Acquisition method:** Rsync (with a dropdown arrow)
- Footer:** **Rsync:** Files and directories are copied using Rsync. This is a bit slow but it can be used on any source directory. Errors are ignored.  Play loud sound when acquisition is completed. Continue button.

DATI DEL CASO

SORGENTE E DESTINAZIONE

METODO DI ACQUISIZIONE

# FINESTRA DI RIEPILOGO



# FINESTRA DI ACQUISIZIONE

```
Fuji - Acquisition

Acquisition completed

(CRC32 $2FDB5/E3: GPT Partition Data (Primary GPT Table : 2))
Leggo (Apple_Free : 3)...
(CRC32 $00000000: (Apple_Free : 3))
Leggo EFI System Partition (C12A7328-F81F-11D2-BA4B-00A0C93EC93B : 4)...
(CRC32 $B54B659C: EFI System Partition (C12A7328-F81F-11D2-BA4B-00A0C93EC93B : 4))
Leggo disk image (Apple_APFS : 5)...
(CRC32 $ABD9DA1B: disk image (Apple_APFS : 5))
Leggo (Apple_Free : 6)...
(CRC32 $00000000: (Apple_Free : 6))
Leggo GPT Partition Data (Backup GPT Table : 7)...
(CRC32 $2FDB57E3: GPT Partition Data (Backup GPT Table : 7))
Leggo GPT Header (Backup GPT Header : 8)...
(CRC32 $874EAD8D: GPT Header (Backup GPT Header : 8))
Aggiungo risorse...
Tempo trascorso: 12m 41.798s
Dimensioni file: 130380675732 byte, Checksum: CRC32 $EE44CC1C
Settori processati: 965595304, 434002547 compressi
Velocità: 278.2M B/s
Compresso: 73.6%
created: /Volumes/Fuji/0123456789_Acquisition/0123456789_Acquisition.dmg

Hashing /Volumes/Fuji/0123456789_Acquisition/0123456789_Acquisition.dmg
1% 2% 3% 4% 5% 6% 7% 8% 9% 10% 11% 12% 13% 14% 15% 16% 17% 18% 19% 20% 21% 22% 23% 24% 25% 26% 27%
28% 29% 30% 31% 32% 33% 34% 35% 36% 37% 38% 39% 40% 41% 42% 43% 44% 45% 46% 47% 48% 49% 50% 51%
52% 53% 54% 55% 56% 57% 58% 59% 60% 61% 62% 63% 64% 65% 66% 67% 68% 69% 70% 71% 72% 73% 74% 75%
76% 77% 78% 79% 80% 81% 82% 83% 84% 85% 86% 87% 88% 89% 90% 91% 92% 93% 94% 95% 96% 97% 98% 99%
100%

Writing report file /Volumes/Fuji/0123456789_Acquisition/0123456789_Acquisition.txt

Acquisition completed!
```

Foto gentilmente fornita da Derek Eiri  
<https://lazza.me/GB26>



# Avvio con Fuji Cartridge

L'immagine DMG di Fuji 1.2.0 è compatibile con balenaEtcher e può essere scritta su **qualsunque 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](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*

pinset_everything.txt	21 ago 2
powermetrics.txt	21 ago 2
ps_thread.txt	21 ago 2
ps.txt	21 ago 2
README.txt	21 ago 2
remotectl_dumpstate.txt	21 ago 2
resolv.conf	18 ago 2
sample-8710-highcpu.txt	21 ago 2
sample-8711-highcpu.txt	21 ago 2
sample-8773-highcpu.txt	21 ago 2
securebootvariables.txt	21 ago 2
security-sysdiagnose.txt	21 ago 2
sftool.LSSharedF...FavoriteItems.txt	21 ago 2
sftool.LSSharedF...vorteVolumes.txt	21 ago 2
sftool.LSSharedF...st iCloudItems.txt	21 ago 2
smcDiagnose.txt	21 ago 2
spindump.txt	21 ago 2
sw_vers.txt	21 ago 2
swcutil_show.txt	21 ago 2
sysctl.txt	21 ago 2
sysdiagnose.log	21 ago 2
system_logs.logarchive	21 ago 2
systemextensionsctl_diagnose.txt	21 ago 2
tailspin-info.txt	21 ago 2
talagent-501.txt	21 ago 2
taskinfo.txt	21 ago 2
taskSummary.csv	21 ago 2
tbtDiagnose.txt	21 ago 2
thermal.txt	21 ago 2
top.txt	21 ago 2
transparency.log	21 ago 2
uptime.txt	21 ago 2
vm_stat.txt	21 ago 2
WindowServer.external.wininfo.plist	21 ago 2
xartutil.txt	21 ago 2
zprint.txt	21 ago 2

## RISULTATO

```
0123456789_Acquisition.txt
Fusion Drive:                No
APFS Volume Group:           9B554BD1-73A6-43F3-834E-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-39AFBADD5AD7CDAB00800931F501492F46ACCAF14B9622A5EFF21BDA87326B8
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: 0d7baebfc95da2fa5d668a9c8d536ddb776dd8e
- 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.**

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"
```



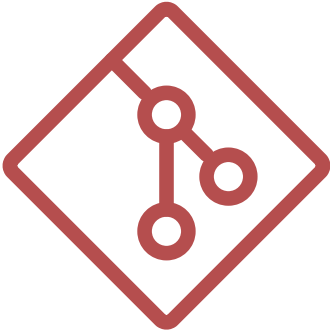
# Costruire il file DMG

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 `dmgbuid`

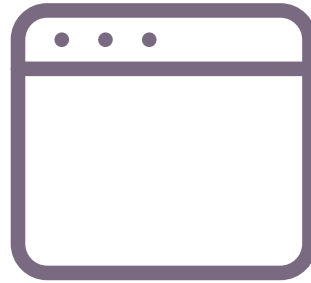
Passiamo da codice sorgente a DMG **in un comando.**

## 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](http://andrealazzarotto.com)

### **GitHub**

[Lazza](#)

### **Social link**

[bio.lazza.me](https://bio.lazza.me)

