Fuji: A New Open Source Tool For Full File System Acquisition of Mac Computers

ANDREA LAZZAROTTO

DFIR EUROPE SUMMIT

SANS

About me

- Digital Forensics Consultant and Software Developer
- Interests include WhatsApp forensics and anti-forensics (chat manipulation), as well as the forensic acquisition and analysis of Instagram profile metadata
- Author of several open-source tools, including **RecuperaBit** for NTFS reconstruction and **Carbon14,** which is used to estimate the publication date of a web page (both included in CAINE)
- Recently published **Fuji,** the topic of this presentation

Agenda

INTRODUCTION

Challenges of macOS forensic acquisition

FEATURES AND USAGE

Everything that Fuji can do for you

DEVELOPMENT PROCESS

Technologies employed and future plans

Introduction

CHALLENGES OF MACOS FORENSIC ACQUISITION

Back in the day

When I became interested in digital forensics about a decade ago, computers could be acquired easily.

You just needed a write blocker or a forensic Linux distribution, such as CAINE or Tsurugi. You could get an EWF acquisition or even **just use dd.**

Wasn’t it great?

Then came modern Macs

Apple introduced hardware-based encryption with the T2 security chip in 2017 and doubled down with Apple Silicon in late 2020.

Moreover, all modern Macs come with storage drives soldered to the motherboard.

My learning path started because I didn’t know much about Mac forensics. I wanted to understand more about the acquisition techniques for modern Apple computers.

Apple Silicon

M1, M2, and M3 models use an ARM architecture, not x64.

After several attempts at customizing macOS recovery partitions, I realized that it was pointless.

Apple Silicon Macs can't boot forensic Linux distributions, but they also cannot boot external operating systems at all:

> *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

A new paradigm

We cannot obtain a (decryptable) physical disk image.

It is useful to think about the forensic acquisition of Apple Silicon Macs **in the same way as what is done on modern smartphones.**

When a physical image cannot be obtained, we strive to get a Full File System (FFS) extraction while the device is turned on.

I am always doing
what I can't do yet
in order to learn how to do it.

VINCENT VAN GOGH

Fuji: Forensic Unattended Juicy Imaging

Fuji is a software application for the forensic acquisition of Mac computers, providing the analyst with a **Full File System image.**

It provides an easy-to-use, modular and extensible GUI, leveraging several existing macOS utilities. **It is free and open source.**

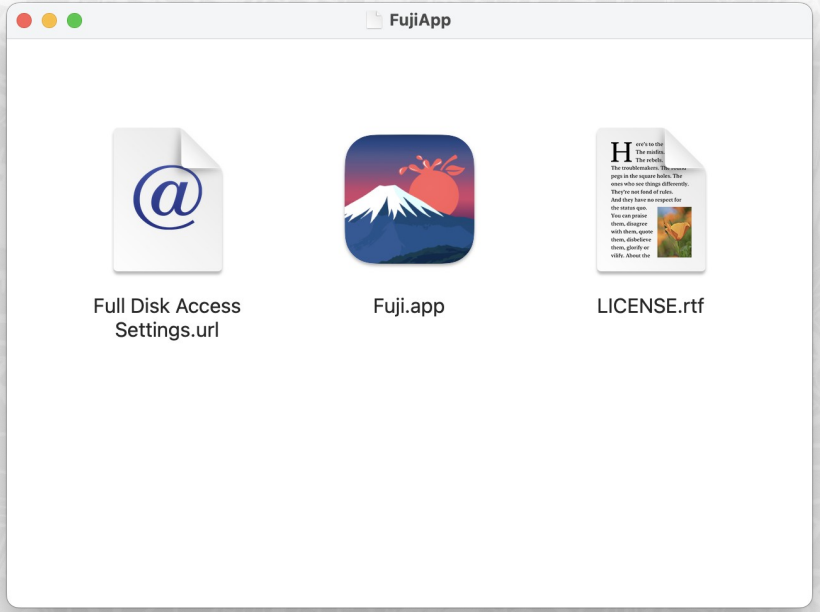
Fuji is also a kind of apple.

HTTPS://GITHUB.COM/LAZZA/FUJI

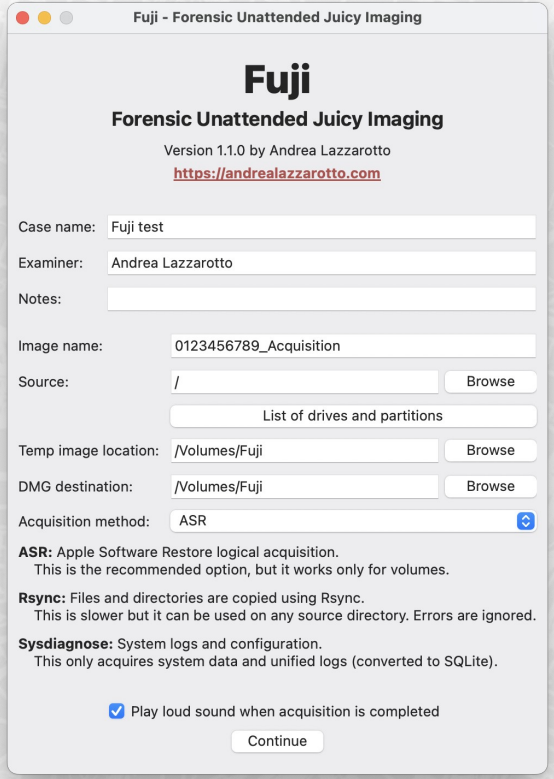
Features and usage

EVERYTHING THAT FUJI CAN DO FOR YOU

DMG CONTENTS



Main interface

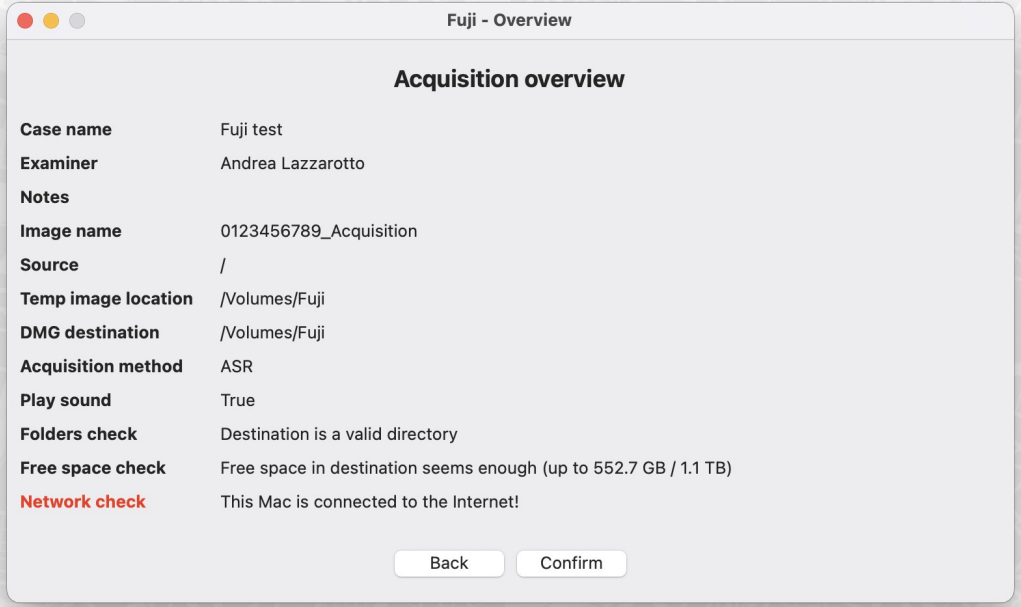


CASE DATA

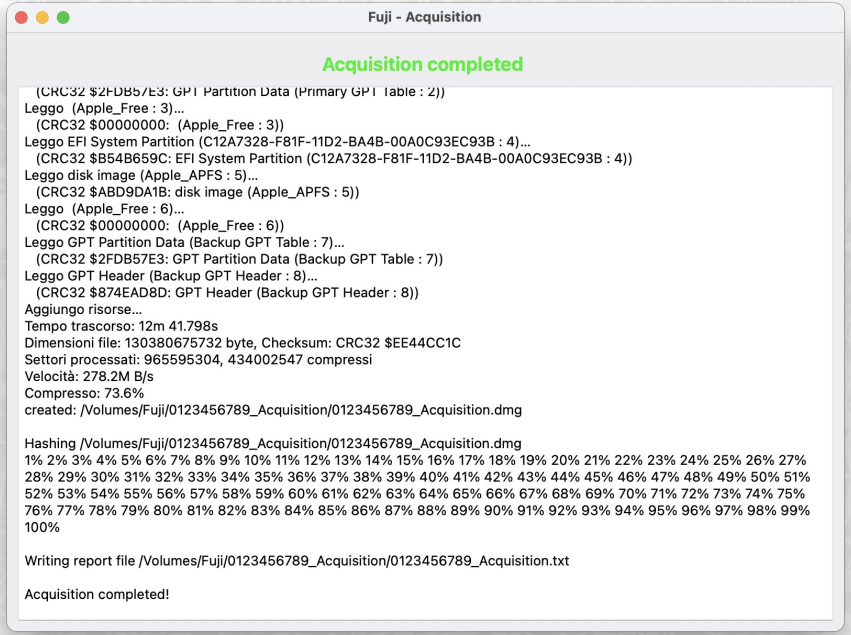
SOURCE AND DESTINATION

ACQUISITION METHOD

OVERVIEW WINDOW



ACQUISITION WINDOW



ASR

Cloning is done via Apple Software Restore:

- “Official” Apple backup method
- **Very fast**
- Works only on full volumes
- May fail due to file system errors
- Bug-ridden on macOS 13 (Ventura)

Rsync

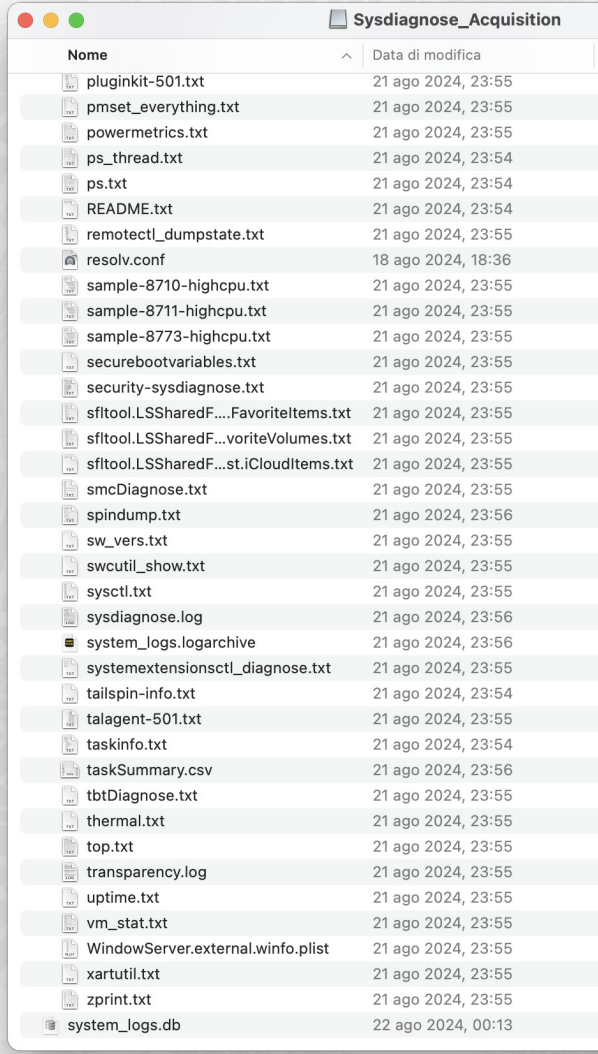
Files are copied in a disk image using Rsync:

- Battle-tested UNIX utility
- Slower processing
- **Works on any source directory**
- Doesn’t fail for small file system issues
- Files that cannot be copied are skipped

Sysdiagnose

The acquisition includes system data and logs:

- Not a full file system image
- Processes information, network, and file activity
- More data that does not fit in a screenshot
- Includes unified logs in *logarchive* format
- **Fuji converts them to SQLite for you**



THE OUTCOME

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-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 generates a report and a read-only DMG file containing all the acquired data.

It can be imported into Autopsy, FTK Imager, or any of your favorite tools.

You can delete the temporary sparse image.

Finally, national Law Enforcement agencies can tackle the complex scenarios of the macOS world without having to resort to expensive commercial software.

ANONYMOUS
OFFICER, ITALIAN FINANCIAL POLICE

I had to deal with a Mac running macOS 10.13, stuck in an encryption “limbo” despite FileVault being off. Using Fuji, I was able to acquire a DMG file of the entire content of the file system.

ISMAELE DI NATALE
FORENSIC EXPERT, VINTEK ENGINEERING

OPERATING SYSTEM COMPATIBILITY

10.10+

Rsync

This is the most compatible option, working with any Mac released in the last ten years.

11+

ASR and Sysdiagnose

Both methods are especially suited for newer Apple Silicon and Intel Macs.

Development process

TECHNOLOGIES EMPLOYED AND FUTURE PLANS

Technologies

Fuji is developed using Python 3.10, and each acquisition method inherits from a base class carrying the **shared logic.**

The user interface makes use of wxPython. It was developed with the help of ChatGPT and Duck AI.

The program invokes several native macOS utilities, including **asr, rsync, sysdiagnose, hdiutil, and diskutil.**

Gaining permissions

The DMG includes a link to jump to *Full Disk Access* settings:

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

Root permissions are requested with:

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

Building the DMG

Fuji is assembled into a macOS app with PyInstaller. The basic script has been edited to perform the following actions:

- Compile the app
- Rename the binary
- Copy the root permissions helper
- Prepare the DMG using dmgbuild

We go from source code to DMG **in one command.**

Future plans

IMPROVE COMPATIBILITY

Test and improve compatibility of ASR and Sysdiagnose on legacy OS X versions.

USER INTERFACE ENHANCEMENTS

Some rough edges can probably be smoothed.

RECOVERY ENVIRONMENT

Additional testing is needed to see what Fuji features can be used while booted in macOS recovery.

KEY TAKEAWAYS

Open source

The inner workings can be checked and reviewed. No black boxes.

Straightforward

Most of the code is actually related to the GUI. It can be easily extended.

Invaluable

Fuji saves you time and money. Install on as many drives as you like, without dongles.

CONTACT

Web
andrealazzarotto.com

GitHub
Lazza

Twitter
@thelazza

Mastodon
@lazza@mastodon.social