Open-Source Tools for Digital Forensics

MSAB MOBILE FORENSICS DIGITAL SUMMIT 2026

ANDREA LAZZAROTTO

ANDREALAZZAROTTO.COM

Agenda

INTRODUCTION

The main phases of digital forensics

FORENSIC ACQUISITION

The imaging process

PARSING & ANALYSIS

Extracting answers from data

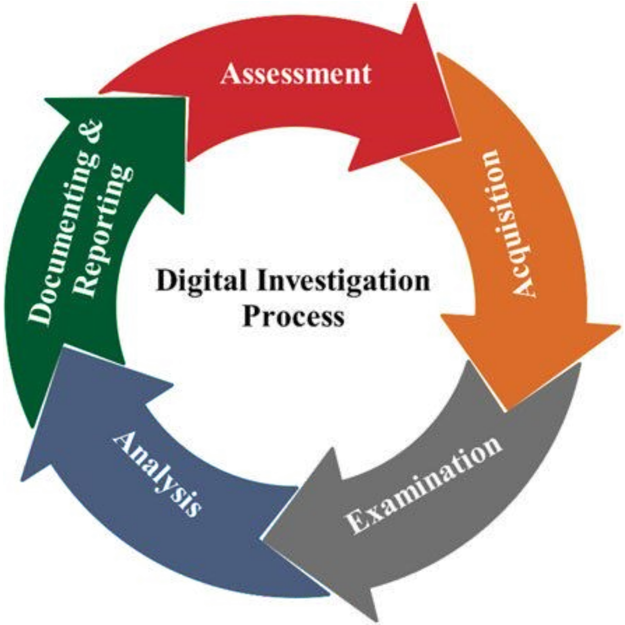
About me

- Master’s degree in Computer Science
- Digital Forensics Consultant and Software Developer
- Interests include WhatsApp forensics and anti-forensics
- Author of several open-source tools, such as **RecuperaBit** for NTFS reconstruction and **Carbon14** for estimating the publication date of a web page (both included in CAINE)
- **Author of Fuji,** the new open source program for the forensic acquisition of macOS

Introduction

THE MAIN PHASES OF DIGITAL FORENSICS

THE PHASES OF DIGITAL FORENSICS

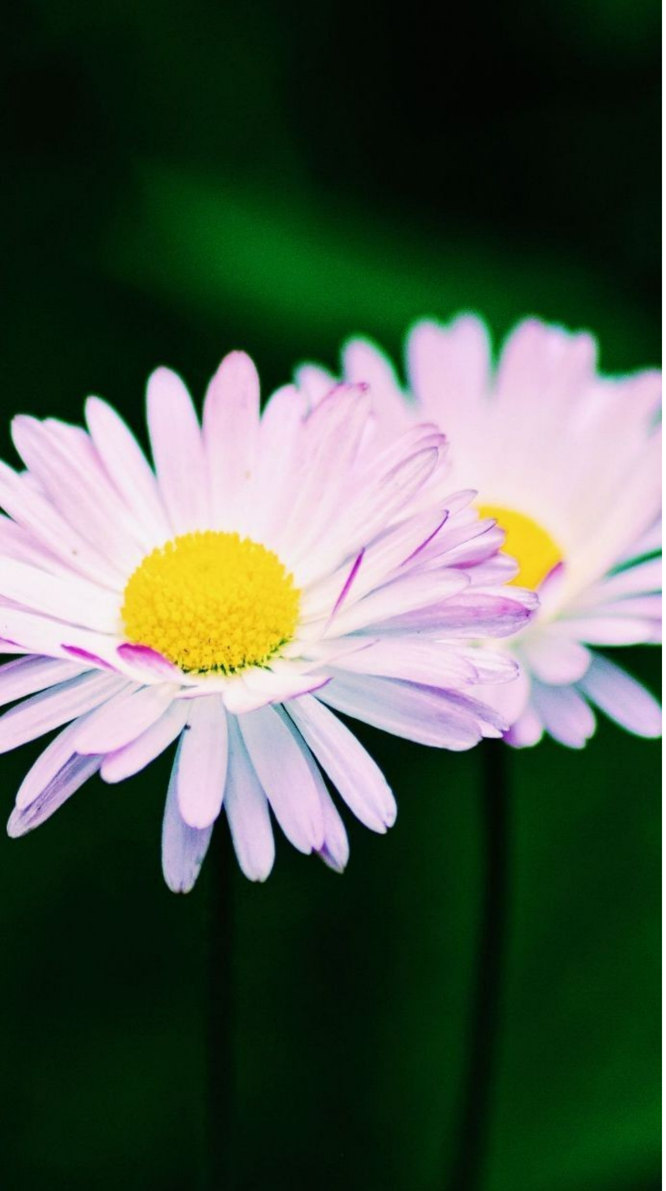


https://doi.org/10.1007/978-3-030-33596-0_22

Searching for *"digital forensics phases"* yields many different models — some even listing up to 9 phases.

Tools are mainly used for:

- Acquisition
- Examination
- Analysis



Acquisition

The acquisition phase is crucial for creating forensic copies, i.e. duplicating the content of media to be analyzed.

Original evidence is only touched to create copies, which must be **“frozen” by calculating a hash.**

A hash function generates a fixed-length value that changes entirely with even the slightest modification of the input.

This allows for later verification to determine whether the copy is genuine or has been altered.

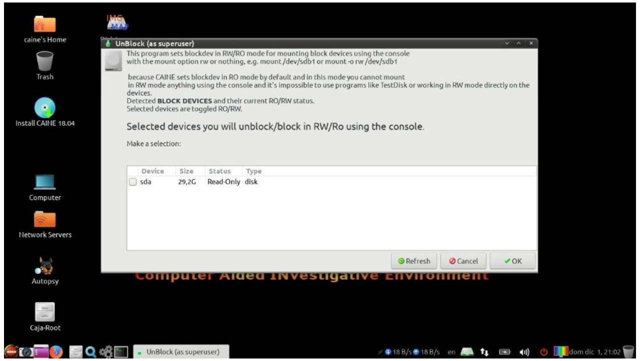
Examination & analysis

Some models separate examination (extracting specific data) from analysis, the intellectual work that provides meaning and answers the given questions.

Regardless, the key is **to follow the scientific method** and validate the data, properly justifying every conclusion. What makes the difference are skill, experience, intuition, and methodical work.

Avoid becoming a *“push-the-button”* forensic expert!

ITALIAN LINUX DISTRIBUTIONS



UnBlock (as superuser)

This program sets blockdev in RW/RO mode for mounting block devices using the console
with the mount option rw or nothing, e.g. mount /dev/sdb1 or mount -o rw /dev/sdb1

because CAINE sets blockdev in RO mode by default and in this mode you cannot mount
in RW mode anything using the console and it's impossible to use programs like TestDisk or working in RW mode directly on the devices.
Detected **BLOCK DEVICES** and their current RO/RW status.
Selected devices are toggled RO/RW.

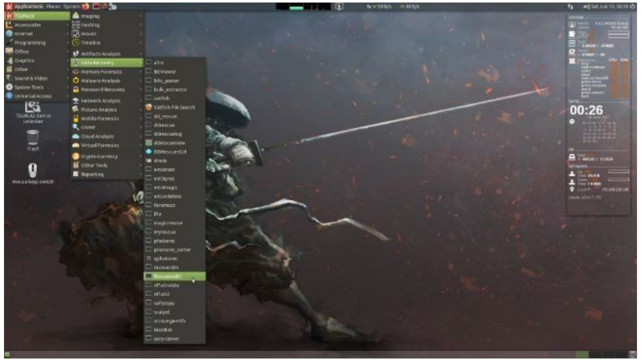
Selected devices you will unblock/block in RW/Ro using the console.

Make a selection:

	Device	Size	Status	Type
□	sda	29,2G	Read-Only	disk

CAINE

Maintained by Nanni Bassetti, fast and lightweight, ideal for live forensic imaging



Tsurugi

A complete and rich OS for setting up a Linux forensic workstation

Other distributions

CSI LINUX

Good mix of tools, also for OSINT activities

SIFT WORKSTATION

The “official” solution from SANS Institute

PALADIN LTE

Excellent for live forensic acquisitions, although it’s not 100% open-source, to be precise

Forensic acquisition

THE IMAGING PROCESS

The forensic copy

Forensic analysis is never performed on original evidence (hard drives, smartphones, etc), but only on copies.

The goal is **to acquire a copy that is *identical* to the original,** but what does “identical” mean?

For hard drives, the answer used to be quite simple: performing a “bit-by-bit” copy, every single bit is cloned, including unused space.

Integrity of the evidence must also be guaranteed.

Types of acquisition

BITSTREAM COPY

Bit-by-bit image of the entire device (preferred for PCs)

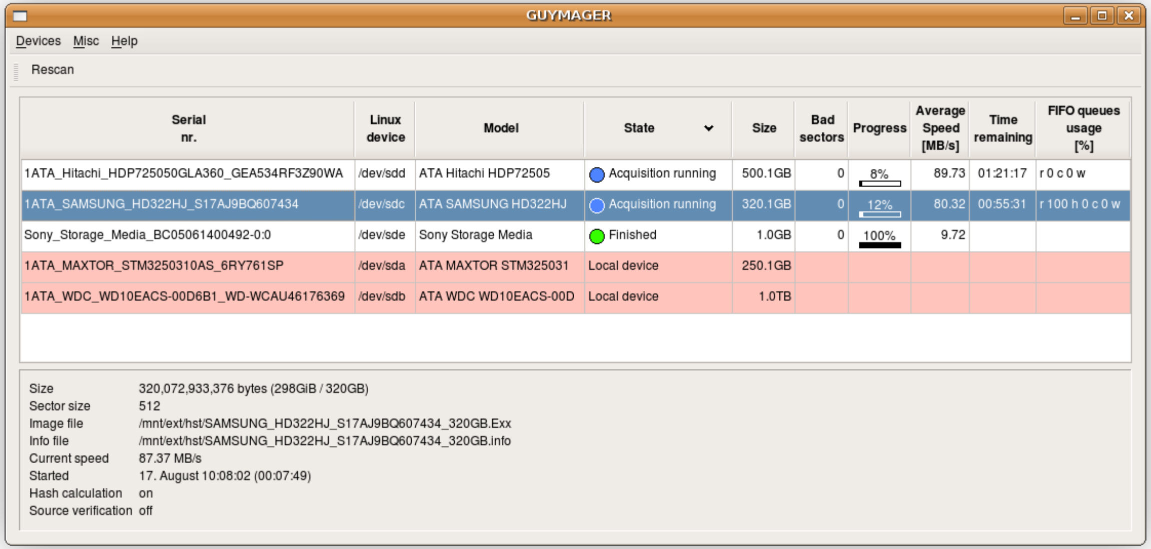
FULL FILE SYSTEM IMAGE

Complete copy of all allocated files

LOGICAL COPY

Acquisition of only a specific set of files or artifacts “exposed” by the device

GUYMAGER



Serial nr.	Linux device	Model	State	Size	Bad sectors	Progress	Average Speed [MB/s]	Time remaining	FIFO queues usage [%]
1ATA_Hitachi_HDP725050GLA360_GEA534RF3Z90WA	/dev/sdd	ATA Hitachi HDP72505	● Acquisition running	500.1GB	0	8%	89.73	01:21:17	r 0 c 0 w
1ATA_SAMSUNG_HD322HJ_S17AJ9BQ607434	/dev/sdc	ATA SAMSUNG HD322HJ	● Acquisition running	320.1GB	0	12%	80.32	00:55:31	r 100 h 0 c 0 w
Sony_Storage_Media_BC05061400492-0:0	/dev/sde	Sony Storage Media	● Finished	1.0GB	0	100%	9.72		
1ATA_MAXTOR_STM3250310AS_6RY761SP	/dev/sda	ATA MAXTOR STM325031	Local device	250.1GB					
1ATA_WDC_WD10EACS-00D6B1_WD-WCAU46176369	/dev/sdb	ATA WDC WD10EACS-00D	Local device	1.0TB					

Size	320,072,933,376 bytes (298GiB / 320GB)
Sector size	512
Image file	/mnt/ext/hst/SAMSUNG_HD322HJ_S17AJ9BQ607434_320GB.Exx
Info file	/mnt/ext/hst/SAMSUNG_HD322HJ_S17AJ9BQ607434_320GB.info
Current speed	87.37 MB/s
Started	17. August 10:08:02 (00:07:49)
Hash calculation	on
Source verification	off

A forensic disk acquisition tool, which is pre-installed in major forensic distributions.

It creates images in EWF, AFF, and RAW formats, automatically calculating hashes.

Using the command line

GOOD OL' DD

Available on any Linux or UNIX operating system

DCFLDD

Enhanced version with advanced features

DDRESCUE

Designed for data recovery from damaged media

Fuji: Forensic Unattended Juicy Imaging

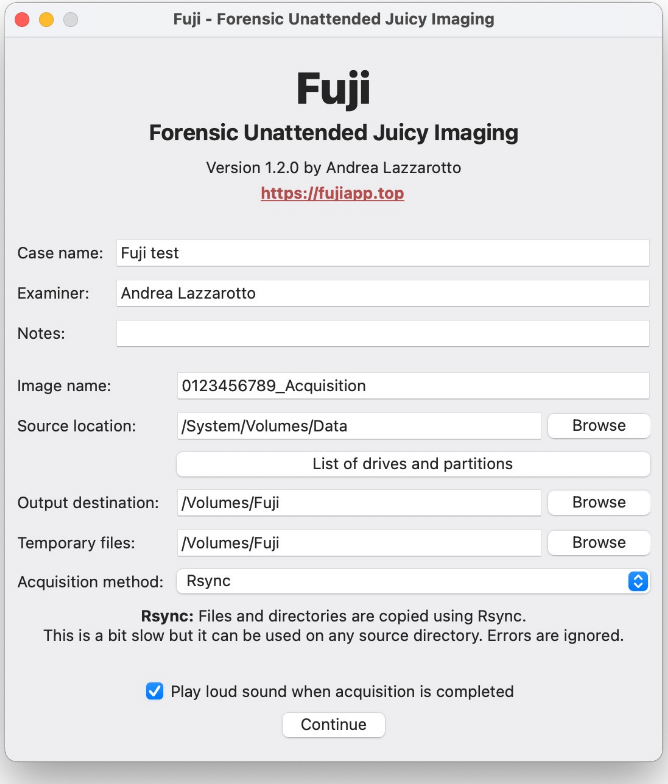
Fuji is a software application for the forensic acquisition of Mac computers, providing the analyst with a **Full File System image.**

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://FUJIAPP.TOP

Main interface



Fuji - Forensic Unattended Juicy Imaging

Fuji

Forensic Unattended Juicy Imaging

Version 1.2.0 by Andrea Lazzarotto

https://fujiapp.top

Case name: Fuji test

Examiner: Andrea Lazzarotto

Notes:

Image name: 0123456789_Acquisition

Source location: /System/Volumes/Data

Output destination: /Volumes/Fuji

Temporary files: /Volumes/Fuji

Acquisition method: Rsync

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

CASE DATA

SOURCE AND DESTINATION

ACQUISITION METHOD

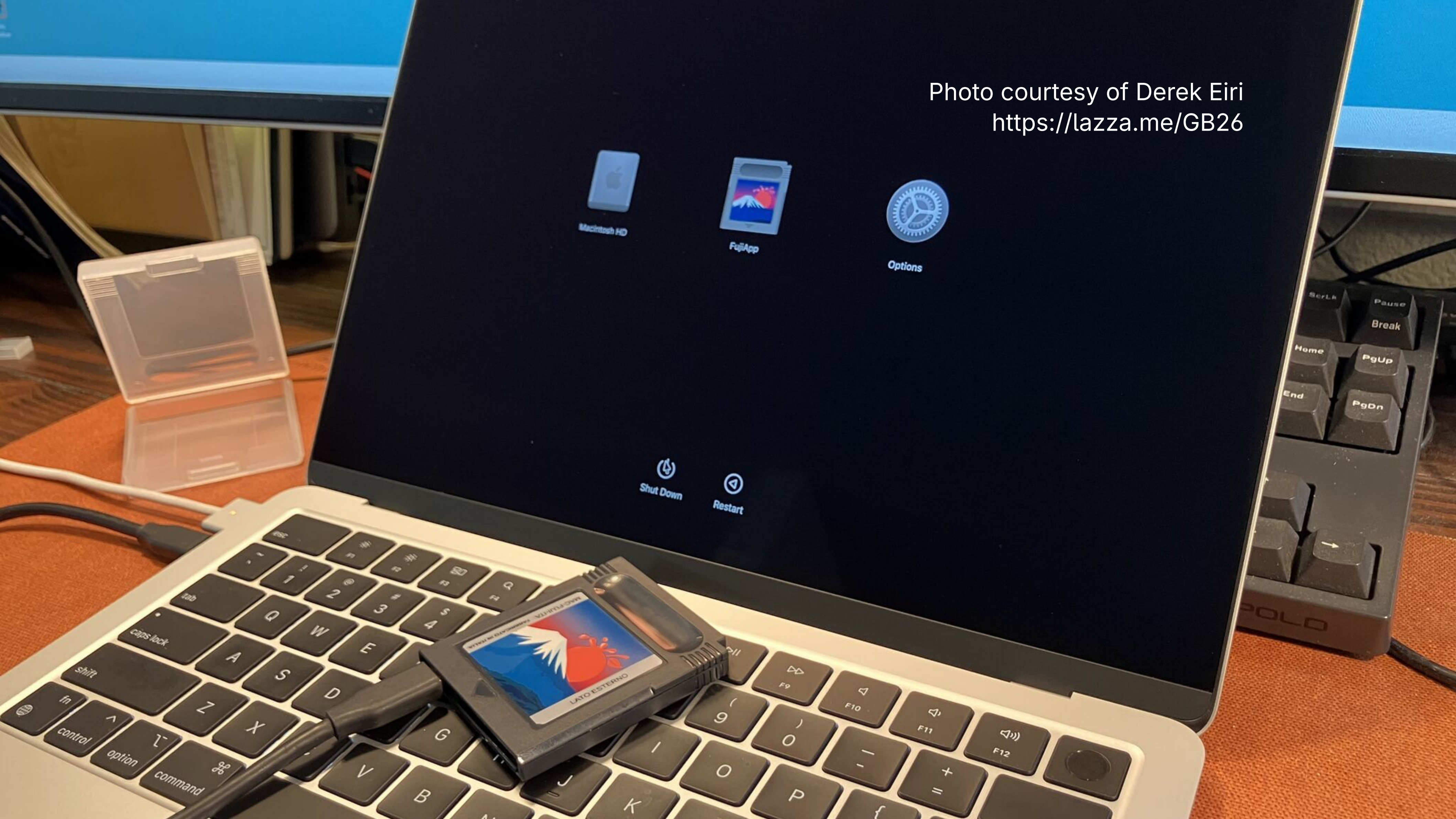


Photo courtesy of Derek Eiri
https://lazza.me/GB26

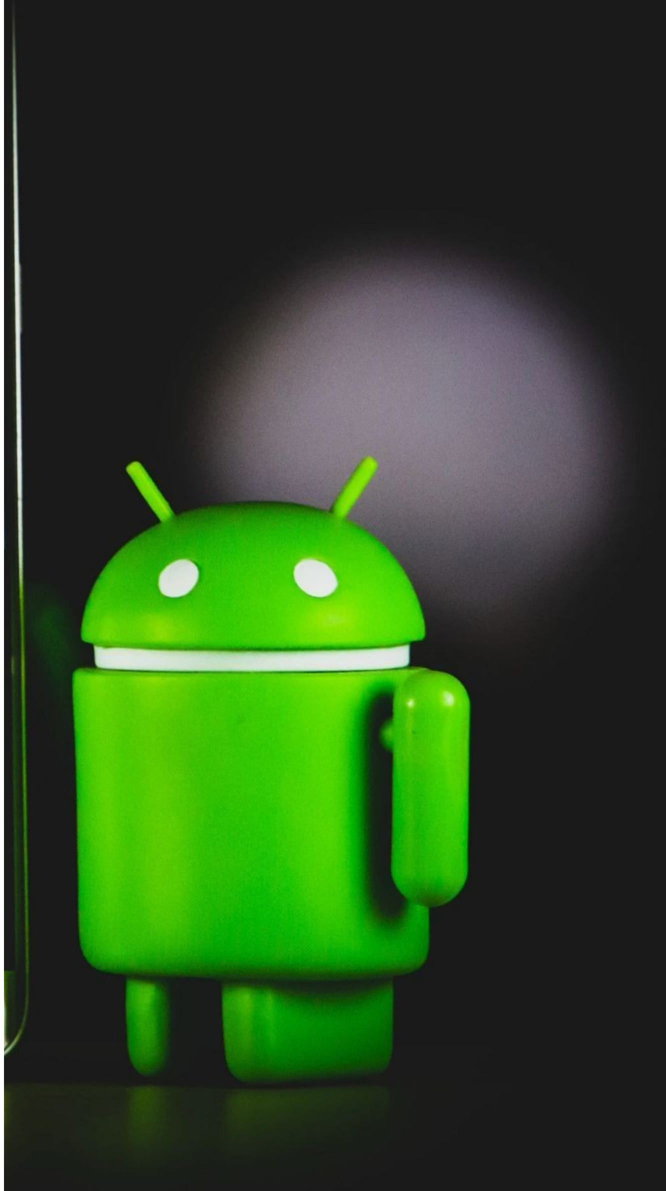
Logical acquisition (Android)

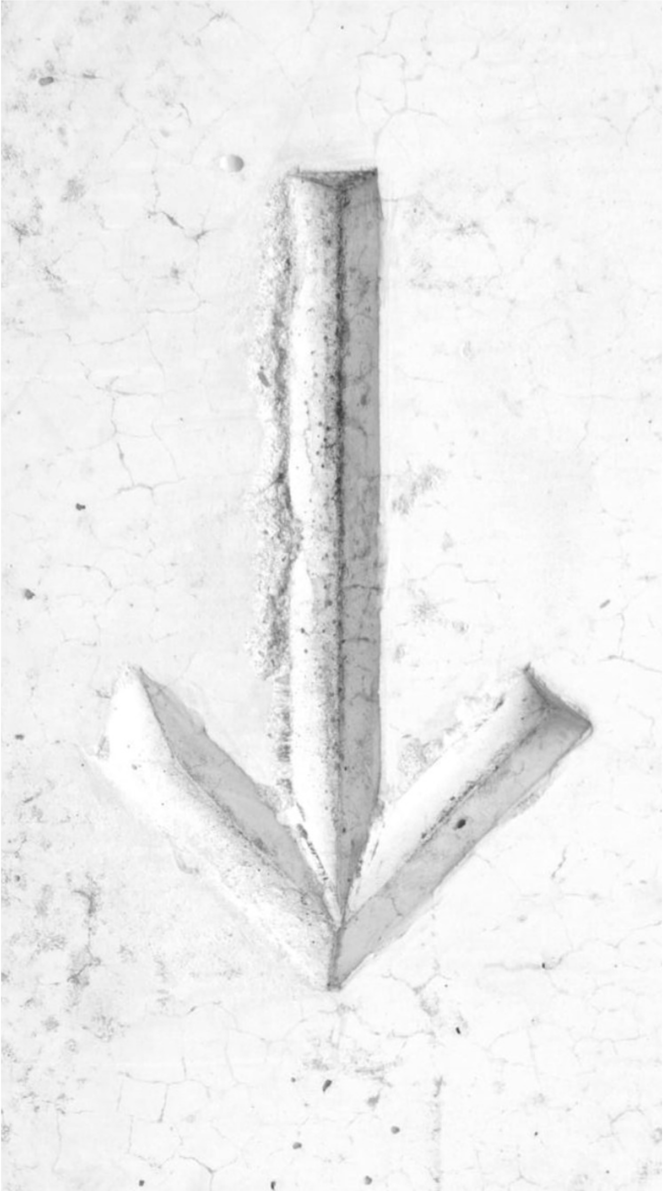
Android smartphones include a wide variety of devices.
To perform a logical copy of **most elements,** use the backup functions provided by ADB (*Android Debug Bridge*):

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

Some forensic tools use an “agent” installed on the device to extract additional elements, such as SMS.

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





APK downgrade

Apps can exclude their own data from backup. This problem can **sometimes be circumvented with APK downgrade:**

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

At this point, the app is removed (but not its data). On recent devices, you must **restart the phone.**

Then install an older APK with backup features enabled, and proceed as previously explained.

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

Logical acquisition (iOS)

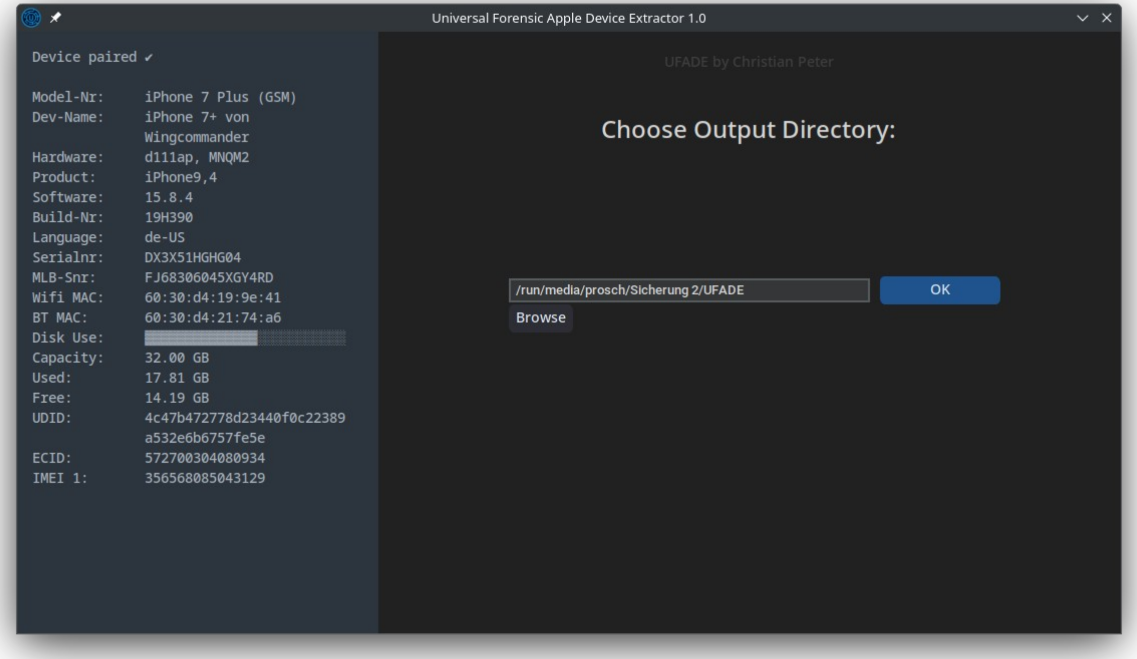
When it comes to iOS devices, they are limited in models and they function uniformly.

Logical acquisition is performed by relying on iTunes' official backup protocol.

All forensic programs use this system for logical copies.
On the command-line you can use *libimobiledevice* (also available in Tsurugi).

Generally speaking, iTunes backups **contain a lot of data,** including almost all apps of interest.

UFADE



```
Device paired ✔

Model-Nr:     iPhone 7 Plus (GSM)
Dev-Name:     iPhone 7+ von
              Wingcommander
Hardware:     d111ap, MNQM2
Product:      iPhone9,4
Software:     15.8.4
Build-Nr:     19H390
Language:     de-US
Serialnr:     DX3X51HGHG04
MLB-Snr:      FJ68306045XGY4RD
Wifi MAC:     60:30:d4:19:9e:41
BT MAC:       60:30:d4:21:74:a6
Disk Use:     ▓▓▓▓▓▓▓▓▓▓▓▓▓▓░░░░░░░░░░░
Capacity:     32.00 GB
Used:         17.81 GB
Free:         14.19 GB
UDID:         4c47b472778d23440f0c22389
              a532e6b6757fe5e
ECID:         572700304080934
IMEI 1:       356568085043129
```

/run/media/prosch/Sicherung 2/UFADE

https://github.com/prosch88/UFADE

It is a tool for forensic extraction from Apple mobile devices, which can be used on all platforms.

UFADE can create **iTunes backups, or “advanced logical” acquisitions** fully compatible with Cellebrite UFED.

FIT: Freezing Internet Tool

The project was started by Fabio Zito as a thesis project.

It resulted in a **multi-platform, modular, extensible, open-source program** for acquiring web content, blog posts, videos, and emails.

FIT is developed by forensic examiners for forensic examiners, thus aligned with professional needs.

HTTPS://GITHUB.COM/FIT-PROJECT/FIT

OTHER TOOLS

mitmproxy

Excellent for analyzing and recording HTTP flows

Wireshark

Can record network traffic and inspect protocols

Carbon14

Estimates the publication date of a web page

Parsing & analysis

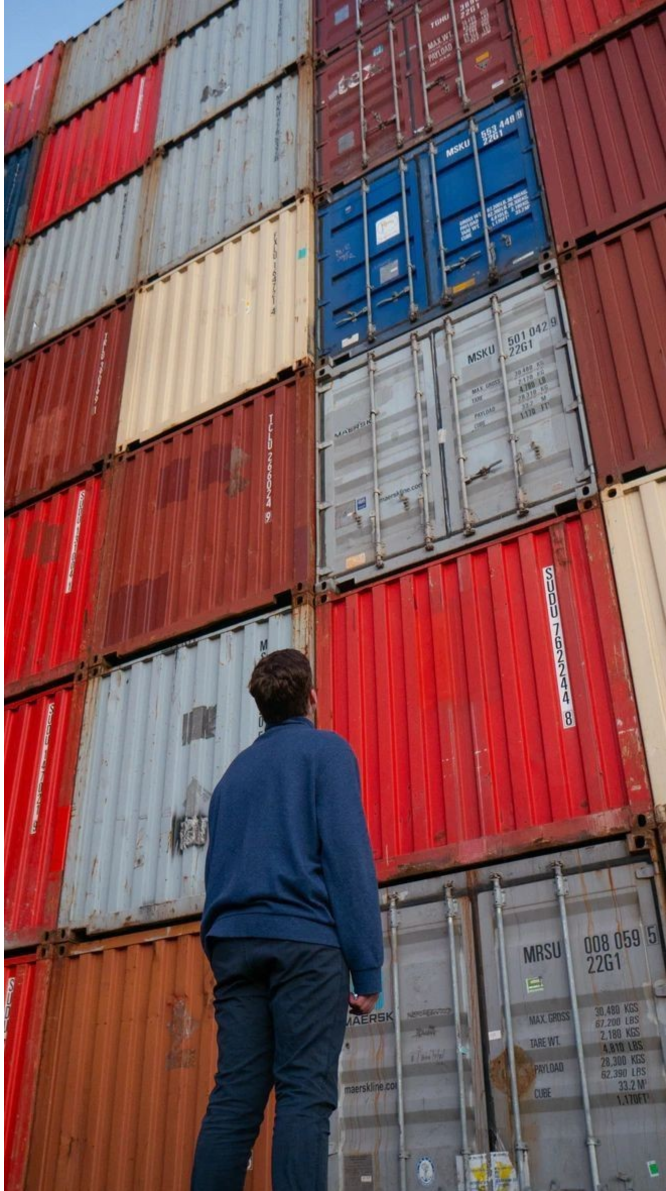
EXTRACTING ANSWERS FROM DATA

Operational challenges

Over time, the capacity of storage devices continues to increase, requiring analysis of vast amounts of data.

I once read an American technical report written in the late 1990s: the analyzed PC had **a single 10 GB hard drive.** Today, my smartphone has 256 GB of storage.

Additionally, keep in mind that data and documents may be stored in proprietary or otherwise obscure formats not supported by tools.



Hidden or protected data

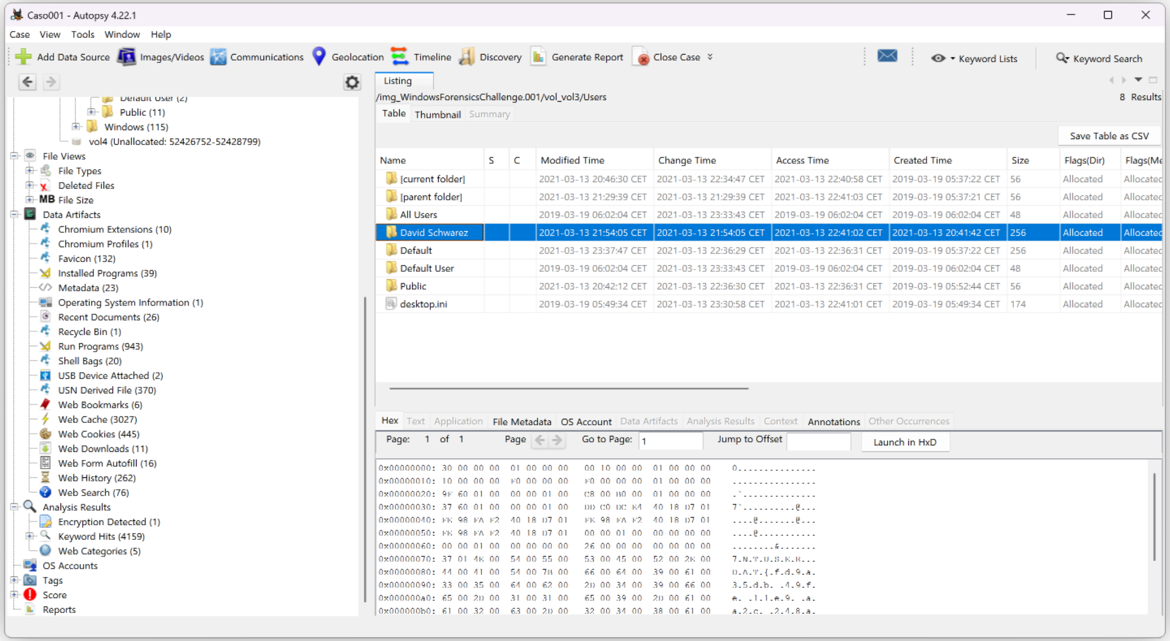
Beyond cryptographic protections, savvy users may use other tricks to hide data.

Changing a file extension might fool someone, e.g. moving a ZIP archive to a system folder, setting a DLL extension.

On NTFS, files can have multiple data contents. *Alternate Data Streams* are accessible by adding “:” after the main filename: `notes.txt:calc.exe`

Something might slip through!

AUTOPSY



/img_WindowsForensicsChallenge.001/vol_vol3/Users

8 Results

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Me
[current folder]			2021-03-13 20:46:30 CET	2021-03-13 22:34:47 CET	2021-03-13 22:40:58 CET	2019-03-19 05:37:22 CET	56	Allocated	Allocatec
[parent folder]			2021-03-13 21:29:39 CET	2021-03-13 21:29:39 CET	2021-03-13 22:41:03 CET	2019-03-19 05:37:21 CET	56	Allocated	Allocatec
All Users			2019-03-19 06:02:04 CET	2021-03-13 23:33:43 CET	2019-03-19 06:02:04 CET	2019-03-19 06:02:04 CET	48	Allocated	Allocatec
David Schwarez			2021-03-13 21:54:05 CET	2021-03-13 21:54:05 CET	2021-03-13 22:41:02 CET	2021-03-13 20:41:42 CET	256	Allocated	Allocatec
Default			2021-03-13 23:37:47 CET	2021-03-13 22:36:29 CET	2021-03-13 22:36:31 CET	2019-03-19 05:37:22 CET	256	Allocated	Allocatec
Default User			2019-03-19 06:02:04 CET	2021-03-13 23:33:43 CET	2019-03-19 06:02:04 CET	2019-03-19 06:02:04 CET	48	Allocated	Allocatec
Public			2021-03-13 20:42:12 CET	2021-03-13 22:36:30 CET	2021-03-13 22:36:31 CET	2019-03-19 05:52:44 CET	56	Allocated	Allocatec
desktop.ini			2019-03-19 05:49:34 CET	2021-03-13 23:30:58 CET	2021-03-13 22:41:01 CET	2019-03-19 05:49:34 CET	174	Allocated	Allocatec

Page: 1 of 1 Page Go to Page: 1 Jump to Offset

```
0x00000000: 30 00 00 00  01 00 00 00   00 10 00 00  01 00 00 00    0...............
0x00000010: 10 00 00 00  F0 00 00 00   F0 00 00 00  01 00 00 00    ................
0x00000020: 9F 60 01 00  00 00 01 00   C8 00 B0 00  01 00 00 00    .`..............
0x00000030: 37 60 01 00  00 00 01 00   DD C0 DC E4  40 18 D7 01    7`.........@...
0x00000040: FE 98 FA F2  40 18 D7 01   FE 98 FA F2  40 18 D7 01    ....@.......@...
0x00000050: FE 98 FA F2  40 18 D7 01   00 00 01 00  00 00 00 00    ....@...........
0x00000060: 00 00 01 00  00 00 00 00   26 00 00 00  00 00 00 00    ........&.......
0x00000070: 37 01 4E 00  54 00 55 00   53 00 45 00  52 00 2E 00    7.N.T.U.S.E.R...
0x00000080: 44 00 41 00  54 00 7B 00   66 00 64 00  39 00 61 00    D.A.T.{.f.d.9.a.
0x00000090: 33 00 35 00  64 00 62 00   2D 00 34 00  39 00 66 00    3.5.d.b.-.4.9.f.
0x000000a0: 65 00 2D 00  31 00 31 00   65 00 39 00  2D 00 61 00    e.-.1.1.e.9.-.a.
0x000000b0: 61 00 32 00  63 00 2D 00   32 00 34 00  38 00 61 00    a.2.c.-.2.4.8.a.
```

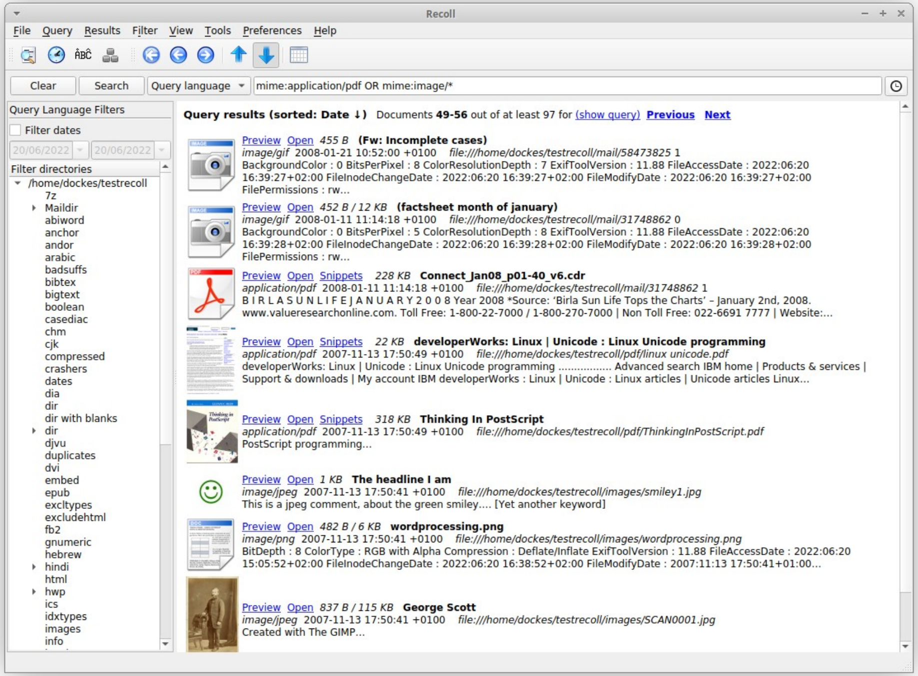
https://www.autopsy.com

A comprehensive open-source suite for *computer forensics.*

It extracts artifacts, indexes files, saves bookmarks, and generates reports in various formats.

An interesting alternative is IPED.

RECOLL



mime:application/pdf OR mime:image/*

Query results (sorted: Date ↓) Documents **49-56** out of at least 97 for (show query) **Previous** **Next**

Preview Open *455 B* **(Fw: Incomplete cases)**
image/gif 2008-01-21 10:52:00 +0100 *file:///home/dockes/testrecoll/mail/58473825* 1
BackgroundColor : 0 BitsPerPixel : 8 ColorResolutionDepth : 7 ExifToolVersion : 11.88 FileAccessDate : 2022:06:20 16:39:27+02:00 FileInodeChangeDate : 2022:06:20 16:39:27+02:00 FileModifyDate : 2022:06:20 16:39:27+02:00 FilePermissions : rw...

Preview Open *452 B / 12 KB* **(factsheet month of january)**
image/gif 2008-01-11 11:14:18 +0100 *file:///home/dockes/testrecoll/mail/31748862* 0
BackgroundColor : 0 BitsPerPixel : 5 ColorResolutionDepth : 8 ExifToolVersion : 11.88 FileAccessDate : 2022:06:20 16:39:28+02:00 FileInodeChangeDate : 2022:06:20 16:39:28+02:00 FileModifyDate : 2022:06:20 16:39:28+02:00 FilePermissions : rw...

Preview Open Snippets *228 KB* **Connect_Jan08_p01-40_v6.cdr**
application/pdf 2008-01-11 11:14:18 +0100 *file:///home/dockes/testrecoll/mail/31748862* 1
BIRLASUNLIFEJANUARY2008 Year 2008 *Source: ‘Birla Sun Life Tops the Charts’ – January 2nd, 2008. www.valueresearchonline.com. Toll Free: 1-800-22-7000 / 1-800-270-7000 | Non Toll Free: 022-6691 7777 | Website:...

Preview Open Snippets *22 KB* **developerWorks: Linux | Unicode : Linux Unicode programming**
application/pdf 2007-11-13 17:50:49 +0100 *file:///home/dockes/testrecoll/pdf/linux unicode.pdf*
developerWorks: Linux | Unicode : Linux Unicode programming .... Advanced search IBM home | Products & services | Support & downloads | My account IBM developerWorks : Linux | Unicode : Linux articles | Unicode articles Linux...

Preview Open Snippets *318 KB* **Thinking In PostScript**
application/pdf 2007-11-13 17:50:49 +0100 *file:///home/dockes/testrecoll/pdf/ThinkingInPostScript.pdf*
PostScript programming...

Preview Open *1 KB* **The headline I am**
image/jpeg 2007-11-13 17:50:41 +0100 *file:///home/dockes/testrecoll/images/smiley1.jpg*
This is a jpeg comment, about the green smiley.... [Yet another keyword]

Preview Open *482 B / 6 KB* **wordprocessing.png**
image/png 2007-11-13 17:50:41 +0100 *file:///home/dockes/testrecoll/images/wordprocessing.png*
BitDepth : 8 ColorType : RGB with Alpha Compression : Deflate/Inflate ExifToolVersion : 11.88 FileAccessDate : 2022:06:20 15:05:52+02:00 FileInodeChangeDate : 2022:06:20 16:38:52+02:00 FileModifyDate : 2007:11:13 17:50:41+01:00...

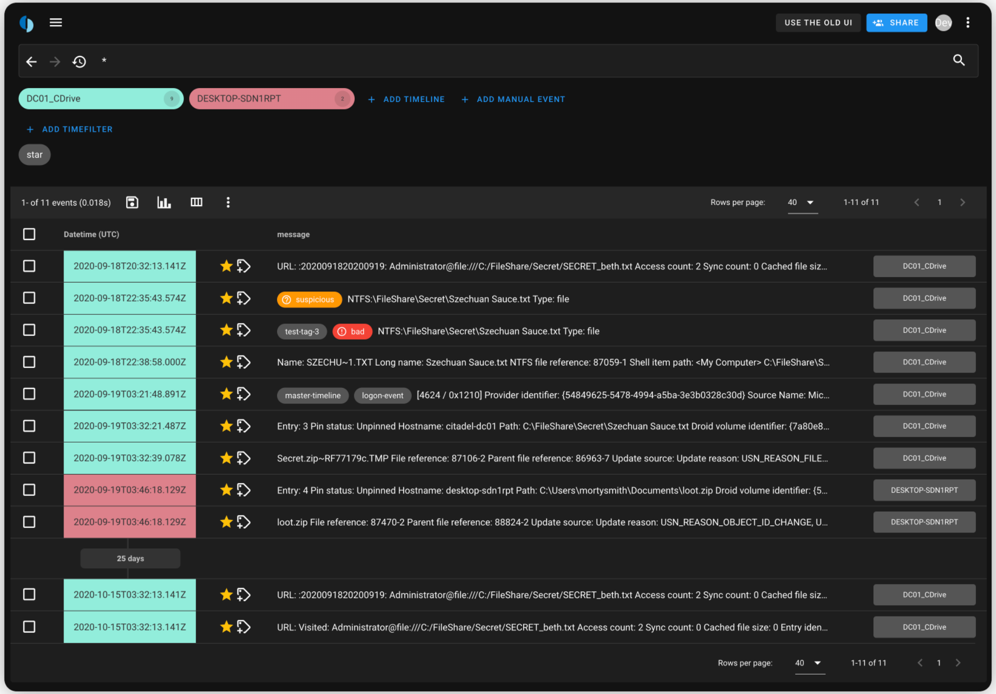
Preview Open *837 B / 115 KB* **George Scott**
image/jpeg 2007-11-13 17:50:41 +0100 *file:///home/dockes/testrecoll/images/SCAN0001.jpg*
Created with The GIMP...

https://www.recoll.org

A free *full-text* search program that reads and indexes emails, documents, and compressed archives in many formats.

It enables targeted searches on large volumes of data, faster than Autopsy.

TIMESKETCH



□	Datetime (UTC)		message	
□	2020-09-18T20:32:13.141Z	★	URL: :2020091820200919: Administrator@file:///C:/FileShare/Secret/SECRET_beth.txt Access count: 2 Sync count: 0 Cached file siz...	DC01_CDrive
□	2020-09-18T22:35:43.574Z	★	suspicious NTFS:\FileShare\Secret\Szechuan Sauce.txt Type: file	DC01_CDrive
□	2020-09-18T22:35:43.574Z	★	test-tag-3 bad NTFS:\FileShare\Secret\Szechuan Sauce.txt Type: file	DC01_CDrive
□	2020-09-18T22:38:58.000Z	★	Name: SZECHU~1.TXT Long name: Szechuan Sauce.txt NTFS file reference: 87059-1 Shell item path: <My Computer> C:\FileShare\S...	DC01_CDrive
□	2020-09-19T03:21:48.891Z	★	master-timeline logon-event [4624 / 0x1210] Provider identifier: {54849625-5478-4994-a5ba-3e3b0328c30d} Source Name: Mic...	DC01_CDrive
□	2020-09-19T03:32:21.487Z	★	Entry: 3 Pin status: Unpinned Hostname: citadel-dc01 Path: C:\FileShare\Secret\Szechuan Sauce.txt Droid volume identifier: {7a80e8...	DC01_CDrive
□	2020-09-19T03:32:39.078Z	★	Secret.zip~RF77179c.TMP File reference: 87106-2 Parent file reference: 86963-7 Update source: Update reason: USN_REASON_FILE...	DC01_CDrive
□	2020-09-19T03:46:18.129Z	★	Entry: 4 Pin status: Unpinned Hostname: desktop-sdn1rpt Path: C:\Users\mortysmith\Documents\loot.zip Droid volume identifier: {5...	DESKTOP-SDN1RPT
□	2020-09-19T03:46:18.129Z	★	loot.zip File reference: 87470-2 Parent file reference: 88824-2 Update source: Update reason: USN_REASON_OBJECT_ID_CHANGE, U...	DESKTOP-SDN1RPT
	25 days			
□	2020-10-15T03:32:13.141Z	★	URL: :2020091820200919: Administrator@file:///C:/FileShare/Secret/SECRET_beth.txt Access count: 2 Sync count: 0 Cached file siz...	DC01_CDrive
□	2020-10-15T03:32:13.141Z	★	URL: Visited: Administrator@file:///C:/FileShare/Secret/SECRET_beth.txt Access count: 2 Sync count: 0 Cached file size: 0 Entry iden...	DC01_CDrive

https://timesketch.org

Described as an open-source tool for collaborative forensic timeline analysis.

Its main selling point is the **native support for timelines generated by Plaso.**

It includes advanced filtering and tagging functionality.

Data recovery

TESTDISK

Restores lost partitions or deleted files

PHOTOREC

Recovers photos and documents via *carving*

RECUPERABIT

Performs advanced forensic reconstruction of corrupted NTFS partitions, also recovers files

Mobile devices

After acquisition, most analysis work essentially focuses on **examining app data.**

Forensic suites compete to support as many applications as possible, but **manual analysis may be needed** if an app is unsupported or requires deeper verification.

Some open-source projects are focused on analyzing data from specific applications.

Multimedia files

The content of photos and thumbnails can be very important, because pictures serve as potentially detailed documentation of events and can have a good level of reliability.

We can analyze EXIF metadata to obtain further information about the device used, the date and time the photo was taken, and the GPS location (if available):

```
exiftool IMG_1234.jpg
```

MVT: Mobile Verification Toolkit

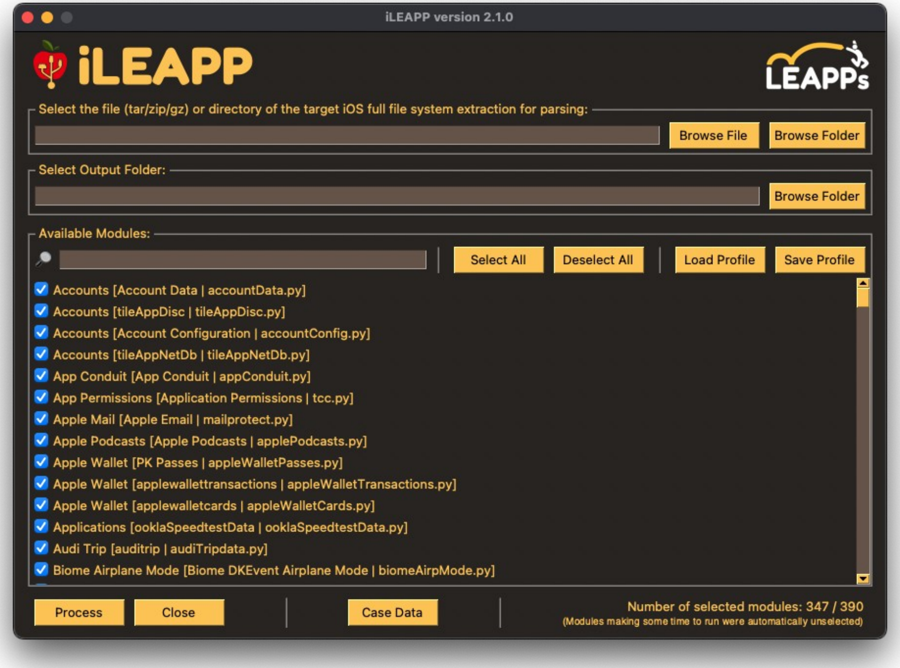
MVT is an open-source tool for consensual forensic analysis of iOS and Android devices.

The project was developed by Amnesty International, primarily **to detect traces of particularly insidious spyware,** such as Pegasus.

It automates the collection and analysis of data from devices, comparing it with indicators of compromise (IoC) published by researchers.

HTTPS://MVT.RE

ALEAPP & ILEAPP



iLEAPP version 2.1.0

Select the file (tar/zip/gz) or directory of the target iOS full file system extraction for parsing:

Select Output Folder:

Available Modules:

- ☑ Accounts [Account Data | accountData.py]
- ☑ Accounts [tileAppDisc | tileAppDisc.py]
- ☑ Accounts [Account Configuration | accountConfig.py]
- ☑ Accounts [tileAppNetDb | tileAppNetDb.py]
- ☑ App Conduit [App Conduit | appConduit.py]
- ☑ App Permissions [Application Permissions | tcc.py]
- ☑ Apple Mail [Apple Email | mailprotect.py]
- ☑ Apple Podcasts [Apple Podcasts | applePodcasts.py]
- ☑ Apple Wallet [PK Passes | appleWalletPasses.py]
- ☑ Apple Wallet [applewallettransactions | appleWalletTransactions.py]
- ☑ Apple Wallet [applewalletcards | appleWalletCards.py]
- ☑ Applications [ooklaSpeedtestData | ooklaSpeedtestData.py]
- ☑ Audi Trip [auditrip | audiTripdata.py]
- ☑ Biome Airplane Mode [Biome DKEvent Airplane Mode | biomeAirpMode.py]

Number of selected modules: 347 / 390
(Modules making some time to run were automatically unselected)

https://github.com/abrignoni

Analysis tools for Android and iOS developed by Alexis Brignoni.

Both extract artifacts such as history, messages, GPS location data, and app usage.

They generate nice HTML reports.

KEY TAKEAWAYS

Verifiability

Open code ensures transparency and scientific verification

Accessibility

Free availability promotes training and dissemination of best practices

Independence

These solutions preserve independence from vendors and digital sovereignty

CONTACT

Web

andrealazzarotto.com

GitHub

Lazza

Social links

bio.lazza.me