Live Forensics from the perspective of Law Enforcement

May 12, 2022

Who’s the dude

Isp. Davide ‘Rebus’ Gabrini

Gabinetto Regionale Polizia Scientifica per la Lombardia
Unità Indagini Elettroniche

Precedentemente:

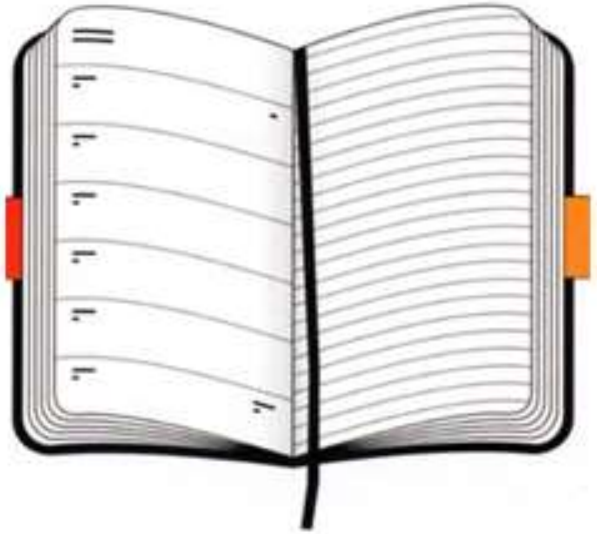
- Squadra Reati Informatici c/o Procura di Milano
- Polizia Postale, Compartimenti di Torino e Milano

Oltre a ciò:

- Professore a contratto in Informatica e Sicurezza Informatica presso il Dipartimento di Giurisprudenza dell’Università degli Studi di Pavia, A.A. 2021/2022
- Collaboratore del Laboratorio di Informatica Forense dell’Università degli Studi di Pavia, afferente al Laboratorio Nazionale di Cybersecurity
- Contributor di Tsurugi Linux, P.M. di Bento
- Socio fondatore di Inclusive Hacker Framework
- Curatore della newsletter Rebus’ Digest

Agenda

- Digital Forensics and CSI
- Best practices
- Practical on-the-spot investigations
  - Identification and emergent issues
  - Live forensics: needs, greeds, opportunities and mistakes
  - Evidence Collection
  - Forensic tools
- Bonus track: laboratory activities



ON-THE-SPOT INVESTIGATIONS

Crime Scene Investigations

- Crime scene investigators document the crime scene.
- We take photographs and physical measurements of the scene, identify and collect forensic evidence, and maintain the proper chain of custody of that evidence.
- We collect evidence such as fingerprints, footprints, tire tracks, blood and other body fluids, hairs, fibers, fire debris, gunshot residues… and of course digital evidence from electronic devices.

Accertamenti urgenti

Art.354 cpp: Accertamenti urgenti sui luoghi, sulle cose e sulle persone

- 1. Gli ufficiali e gli agenti di polizia giudiziaria curano che le tracce e le cose pertinenti al reato siano conservate e che lo stato dei luoghi e delle cose non venga mutato prima dell'intervento del pubblico ministero.
- 2. Se vi è pericolo che le cose le tracce e i luoghi indicati nel comma 1 si alterino o si disperdano o comunque si modifichino e il pubblico ministero non può intervenire tempestivamente ovvero non ha ancora assunto la direzione delle indagini, gli ufficiali di polizia giudiziaria compiono i necessari accertamenti e rilievi sullo stato dei luoghi e delle cose. In relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, gli ufficiali della polizia giudiziaria adottano altresì le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità. Se del caso, sequestrano il corpo del reato e le cose a questo pertinenti.
- 3. Se ricorrono i presupposti previsti dal comma 2, gli ufficiali di polizia giudiziaria compiono i necessari accertamenti e rilievi sulle persone diversi dalla ispezione personale.

DIGITAL FORENSICS

The need of Digital Forensics

- A relatively new branch of forensic science
- Essential in a pervasive computing era
- Nearly impossible, today, to find a crime scene without digital elements
- Electronic devices can be involved…
  - …as a **target**
  - …as a **tool**
  - …as a **witness**

The need of Digital Forensics

- Despite pervasiveness, the real functioning of I.T. technologies remains mysterious to the most

- Digital evidence, on the other hand, can be extremely delicate and requires specific knowledge to be handled correctly

The digital forensic process

- **Identification**

- **Acquisition/Preservation**
- Analysis/Evaluation

- Reporting

BEST PRACTICES

Best practices: international and local guidelines

- RFC3227: Guidelines for Evidence Collection and Archiving
- ISO 27037: Guidelines for identification, collection, acquisition and preservation of digital evidence
- Council of Europe: Electronic Evidence Guide
- ENISA: Good practice material for first responders
- U.S. Secret Service: Best Practices for Seizing Electronic Evidence
- **Servizio Polizia Scientifica**:
  - PT67: procedura tecnica per il sopralluogo informatico
  - PT35: procedura di acquisizione ed analisi forense di supporti informatici
  - PT38: procedura di acquisizione dati da dispositivi mobili
  - PG04: procedura di acquisizione e accettazione reperti
  - PG15: procedura di gestione magazzino reperti e magazzini di laboratorio

Golden rules

There are general principles shared by all guidelines in this field. Among them:

- Whenever possible, it is best to have a trained Digital Forensic Examiner/ Analyst collect electronic evidence
- Check the legal basis you have to inspect or seize the device (plain view, search warrant, consent, etc.)
- If you have reason to believe that the device is involved in the crime you are investigating, take immediate steps to preserve the evidence
  - "Do nothing" is not a valid option
- Ensure both physical e logical isolation
- If a device is OFF, leave it OFF. Do NOT power it on to begin searching through the device relying on the device itself.
- If the device is ON and it's upon you to proceed, follow guidelines in order to properly secure the device and preserve evidence
- If you reasonably believe that the device is destroying evidence, immediately shut it down by pulling the power cord or removing battery
  - Beware: it's a one-way move
- In all instances, you have to document the location and state of the device through video recordings, photos and description.
  - If the device is on and the screen is blank, wake it up (moving the mouse, pressing modifier keys, inserting USB cable etc.) and then take photos of the screen

RFC3227: Guidelines for Evidence Collection and Archiving

Dated February 2002, is still a valid international reference

Among other things, it recommends:

- Keep detailed notes, including dates and times, considering timezone and time skew
- Minimise changes to the data and its metadata as you are collecting it
- Remove external avenues for change
- When confronted with a choice between collection and analysis you should do collection first and analysis later
- Be methodical. If possible, procedures should be automated for reasons of speed and accuracy.
- Proceed from the volatile to the less volatile
- Perform bit-to-bit copies and generate checksums/signatures
- Don't shutdown until you've completed evidence collection
- Don't trust the programs on the system

Order of volatility

- Registers, cache
- Routing table, arp cache, process table, kernel statistics, memory
- Temporary file systems
- Disk
- Remote logging and monitoring data that is relevant to the system in question
- Physical configuration, network topology
- Archival media

Chain of custody

You should be able to clearly describe how the evidence was found, how it was handled and everything that happened to it.

The following need to be documented:

- Where, when, and by whom was the evidence discovered and collected.
- Where, when and by whom was the evidence handled or examined.
- Who had custody of the evidence, during what period. How was it stored.
- When the evidence changed custody, when and how did the transfer occur (include shipping numbers, etc.)

First responder

- In Digital Forensics and Incident Response, dealing with running systems is the most delicate part fo the job
- First responders have a **unique opportunity** to:
  - observe and document what's going on
  - take countermeasures
  - set up probes
  - capture and preserve volatile data
    - Dump RAM, capture network traffic etc.
- In a few words, perform **live forensics**

First responder

First responders have also the opportunity to make **irreparable mistakes** that could drive to:

- loss of relevant data
- degradation of evidence
- alteration of timeline
- lack of documentation (i.e. weak chain of custody)
- obstruction to future investigations

First thing first

- You're in charge! So, take control of the scene:
  - Prioritize intervention on running systems
  - Don't let anybody stay near devices, power sources, cables…
  - Don't shutdown devices before being completely sure it's safe
    - We don't want to lose useful data,
    - nor to stop a productive environment without reasons!
- Keep both **physical** and **logical isolation** while operating

LINE DO NOT CROSS POLICE LINE DO NOT CROSS POL
OSS POLICE LINE DO NOT CROSS

Consider environment

- Environment may contains relevant elements in order to describe human behaviors and habits
  - The last user of a workstation in an open space
  - The traditional yellow post-it containing credentials
  - Password noted under the keyboard and so on…
- Some of those elements may have not digital records…
- If not taken by responders on the scene, they will remain unknown to the analysts on lab, and probably lost for ever
- First step is **identification**: if you fail that, it could be hard to remedy later
- Identification it's not always so easy
  - You better know what you're looking for
  - Data and storage medium may be hidden (logically, physically or both) or simply somewhere else

Good old storage devices

Flash

Floppy Disk

Zip Disk

CD + RW

CD + R

DVD + RW

DVD + R

Storage Tape

Smart Media

Removable Hard – Drive

Micro Drive

Memory Stick

Smart Cards

Online Storage Site

PC Card

Hard Disk

Network Storage Device

Pervasive and ubiquitous computing

- Smart things
- Smart watches
- Smart home
- Smart cars
- Smart clothes
- Smart crap…

Acquisition plan

- Probably you don’t need *every* piece of data you can reach
  - it will costs time and resources
  - sometimes more is less and less is more
- You need to define **what** is useful and **how** to acquire it, respecting order of volatility
  - …and obviously if you have the rights to acquire it
- Consider also external sources:
  - Log files from network appliance (firewall, IDS, Radius, remote Syslog, application server…) that can describe events occurred to your target
  - Physical access to the target (videosurveillance, badge logs etc.)
  - Data retained by third-party (ISP logs, **cloud data**, phone records…)
    - This will probably be acquired later, unless immediate availability

Live vs Post-mortem analysis

- When you find a running system, you're at a crossroads:
  - **Turn it off and proceed to seizure and post-mortem analysis, as it would be found off**
  - Perform examination while it's running

- Both choices have pros and cons, depending on:
  - Training of first responders
  - Disposal of tools, time and resources
  - Loss of relevant data
- In every instances, probably you will need to evaluate the right way to shut down the device at the end

Shutdown

- Think about what you’ll lose:
    - Content of volatile memory
    - State of network/system/services/applications etc.
        - i.e. shell or chat history…
        - Every event or condition not recorded in a log
    - **Access to encrypted volumes** (BitLocker, FileVault, TrueCrypt, PGDisk, BestCrypt etc.)
    - Access to remote shares or cloud resources
- You need to be aware of that before to proceed
    - It's a one-way move.
    - Evaluate to perform something useful *before* that.

LIVE FORENSICS

Analisi Live vs Post-mortem

- When you find a running system, you’re at a crossroads:
  - Turn it off and proceed to seizure and post-mortem alanysis, as it would be found off
  - **Perform examination while it’s running**

- From general to specific, take descriptive notes. I.e.:
  - External appareance in his envinronment
  - Content of display
  - Date and time reported
  - Task visible in foreground
  - State of logical connections
- Take photos and videos (art. 234 c.p.p. – Prova documentale)
- As a Law Enforcement Officer, proceed to the proper action according to circumstances (perquisizione, ispezione, sequestro, accertamento urgente…) applying methods and tools for live forensics

Remember me?

- This is now our checklist:
  - Content of volatile memory
  - State of network/system/services/applications etc.
    - i.e. shell or chat history…
    - Every event or condition not recorded in a log
  - **Access to encrypted volumes** (BitLocker, FileVault, TrueCrypt, PGDisk, BestCrypt etc.)
  - Access to remote shares or cloud resources
- Sometimes you *cannot* shutdown or seize the system
  - *live forensics* becames the only way

Invasiveness

- System is running: every interaction will produce traces
    - Try to minimize your impact
- Ask yourself (before someone else asks to you) which kind of traces you are leaving
    - Can you refer about it?
    - Can *someone* refer about it?
    - Those traces compromise the meaning of the data you're acquiring?
    - This will have relevant impact on the results of analysis?
    - Any kind of write operation can overwrite something:
      is something relevant? Are you causing permanent loss of relevant data?

Live forensics requirements

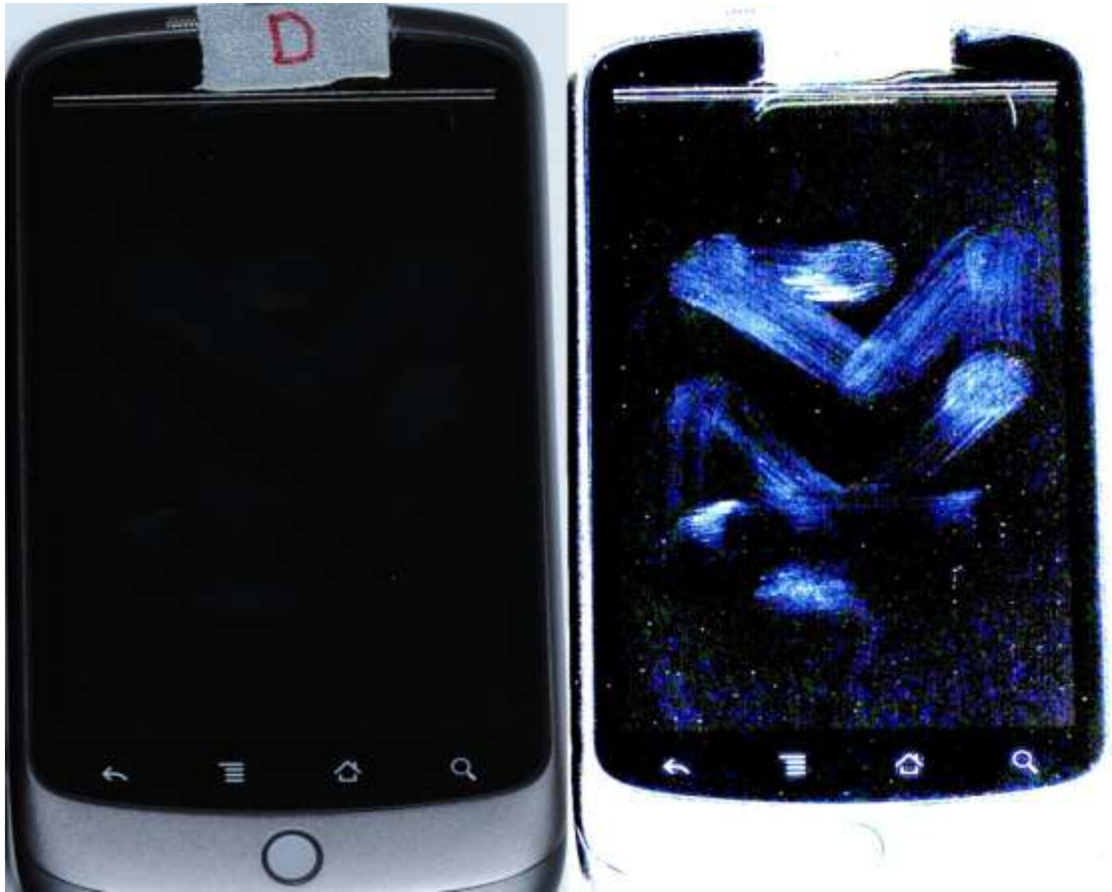
- **Completeness of data**: data that would be destroyed or affected after system shutdown should all be collected.
- **Order of volatility**: data should be collected in the order that would not be affecting other results.
- **Time required** and **Importance of evidence**: data should be collected within a reasonable time and depending on their importance.
- **Repeatability**: All data collected for testing should be available and performed actions should be as repeatable as possible.
- **Integrity of evidence**: data collected from live digital forensics investigation should be protected from being tampered.
- **Accuracy of evidence**: tools for collecting the data should be accurately recording the data
- **Verifiability** and **Reasonableness**: the actions performed should be verifiable in court and be reasonable to the case.
- **Case dependencies**: the actions performed in one particular live digital forensics investigation should be relevant and depending on the case

Live forensics best practices

- Reduce your footprint
- Take only needful actions
- Avoid every possible alteration to data and metadata
- Respect order of volatility
- Take notes of every action, the reason why it's required and his scope, the results obtained
- Use trusted tools, as much indipendent from the system as possible, with minimum needs of resources, preferibly specifically designed for forensic purposes
- Hash data and produce as many copy as needed
- If something can be postponed to post-mortem analysis, postpone it

Lockscreens

- Document the presence and type of lockscreen
- Take photos, notice availability of biometric access
- Limits physical manipulation
  - Don't trigger sensors (that includes front camera)
  - Don't mess with surfaces, especially with touchscreen



Logical isolation of mobile devices

- Sometimes is necessary to seize a device powered on
- If possibile, set airplane/flight mode ON
- Turn off WiFi, BT, mobile data, GPS, alarms
- Think about removing the SIM
    - Bad idea on iOS, still good on some Androids
- Use Faraday bags
    - maybe with a power bank inside or an external power source
- ...but if you can, shut it down :-)
    - and take apart SIM cards

SHUTTING DOWN SYSTEMS

Shutdown

1) Ordinary procedures are generally deprecated

- Start button > Power button > Shut down
- # shutdown –h now

- Ordinary procedures alter a lot of data on filesystem and registry!
- Any kind of *write operation* can *overwrite* something (something relevant?) and cause permanent data loss
- Shutdown command can trigger *clean routines*

Shutdown

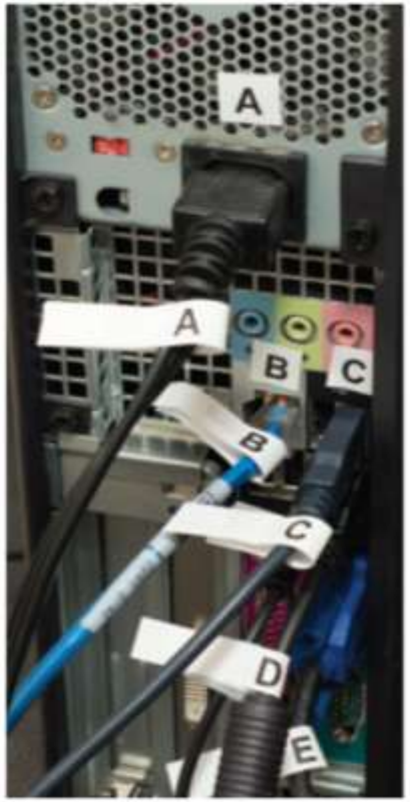
2) Physically disconnect power source

- Pull the cord from the back of the PC and/or remove battery
  - Don’t trust buttons
- Impact on data is minor than operating shutdown
- Risk of damage due to electric shock is remote
- You don’t need trained personnel to do that
- On the other hand, operations not yet recorded could be lost
  - DB of filesystem transactions
  - Contents of caches

COLLECTION

Power off → seizure

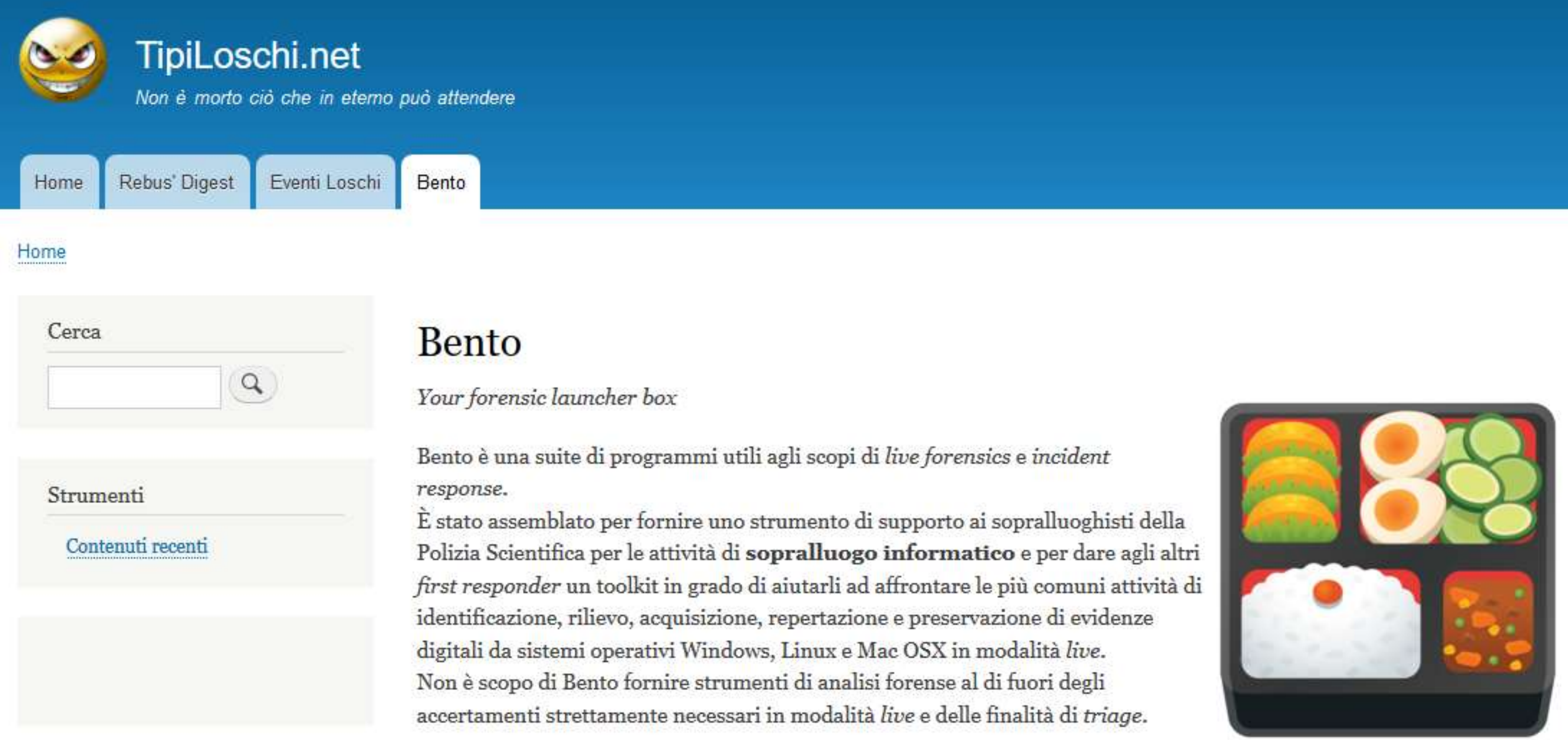
- Take note of serial numbers and significant labels
- Label every item with a unique identifier
- Take step by step photos
- Don’t forget CD or memory card in slots
- Count supports, not covers!
- Don’t forget chargers, cables, adapters and useful accessories
- Original packages can be useful
- Preserve devices from possibile demage caused by temperature, humidity, static charge, EM fileds, mechanical shock
- Start a strong **chain of custody**



LIVE FORENSICS TOOLS

BENTO

YOUR FORENSIC LAUNCHER BOX

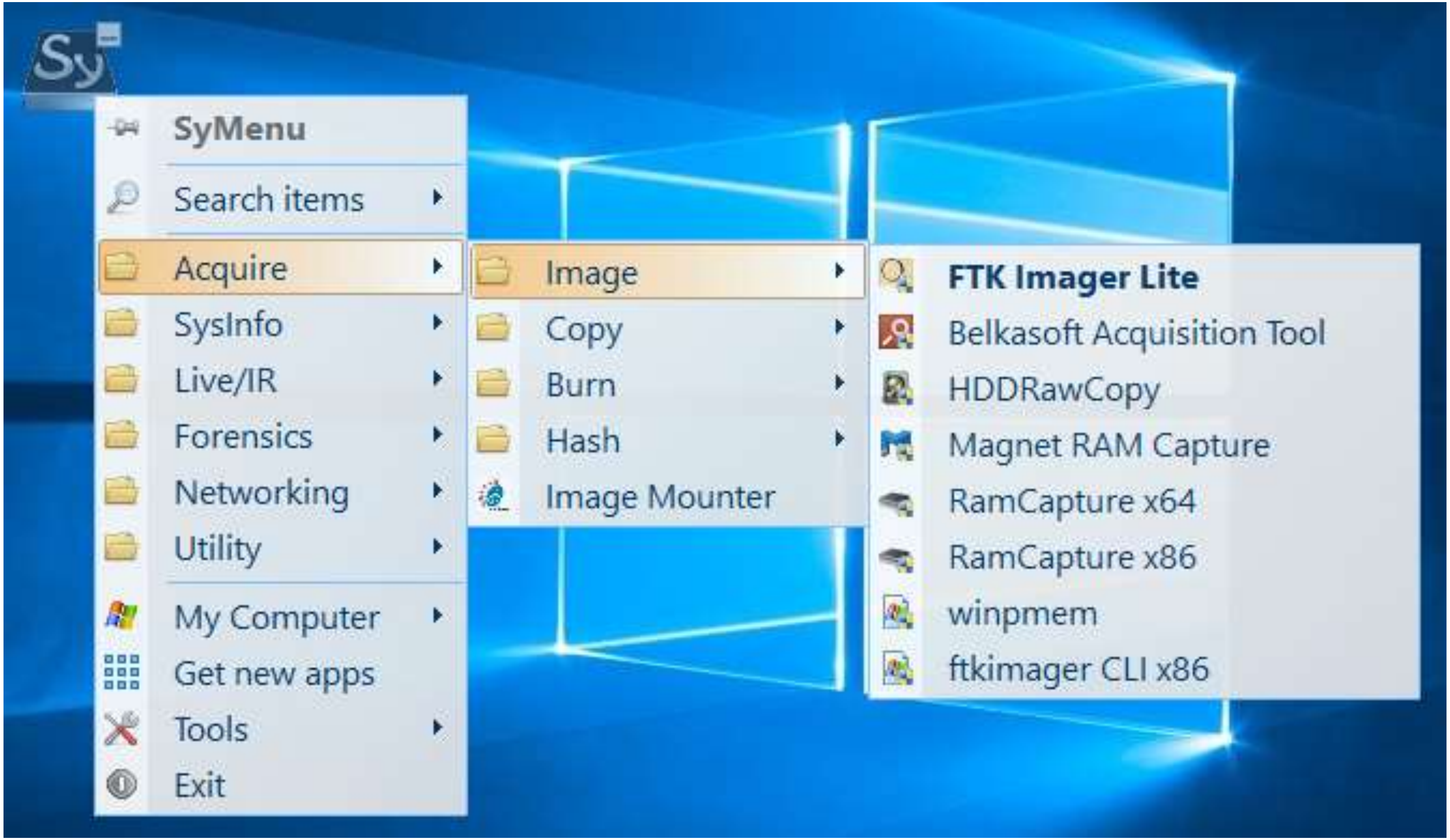


Bento

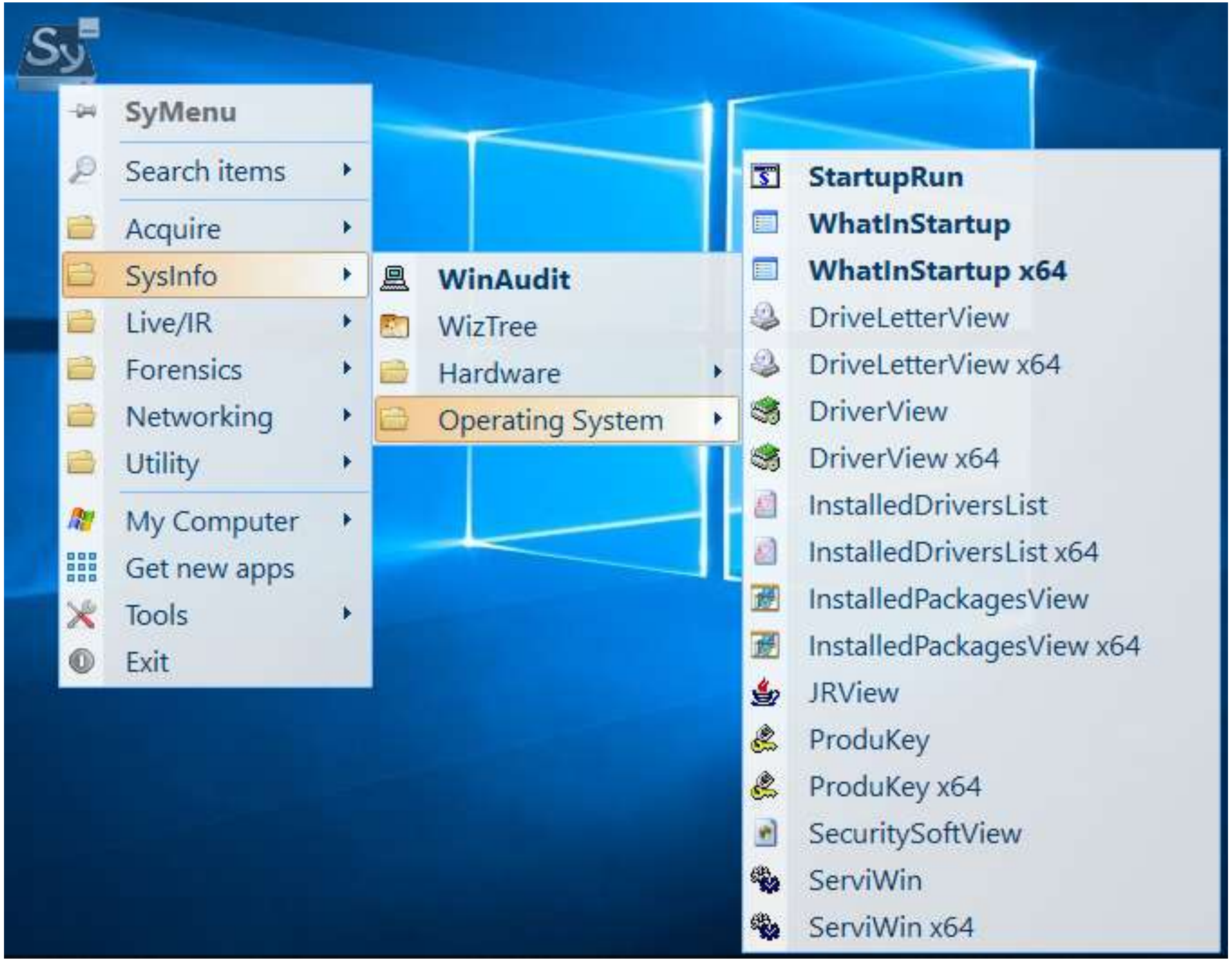
Your forensic launcher box

Bento è una suite di programmi utili agli scopi di *live forensics* e *incident response*.
È stato assemblato per fornire uno strumento di supporto ai sopralluoghisti della Polizia Scientifica per le attività di **sopralluogo informatico** e per dare agli altri *first responder* un toolkit in grado di aiutarli ad affrontare le più comuni attività di identificazione, rilievo, acquisizione, repertazione e preservazione di evidenze digitali da sistemi operativi Windows, Linux e Mac OSX in modalità *live*.
Non è scopo di Bento fornire strumenti di analisi forense al di fuori degli accertamenti strettamente necessari in modalità *live* e delle finalità di *triage*.

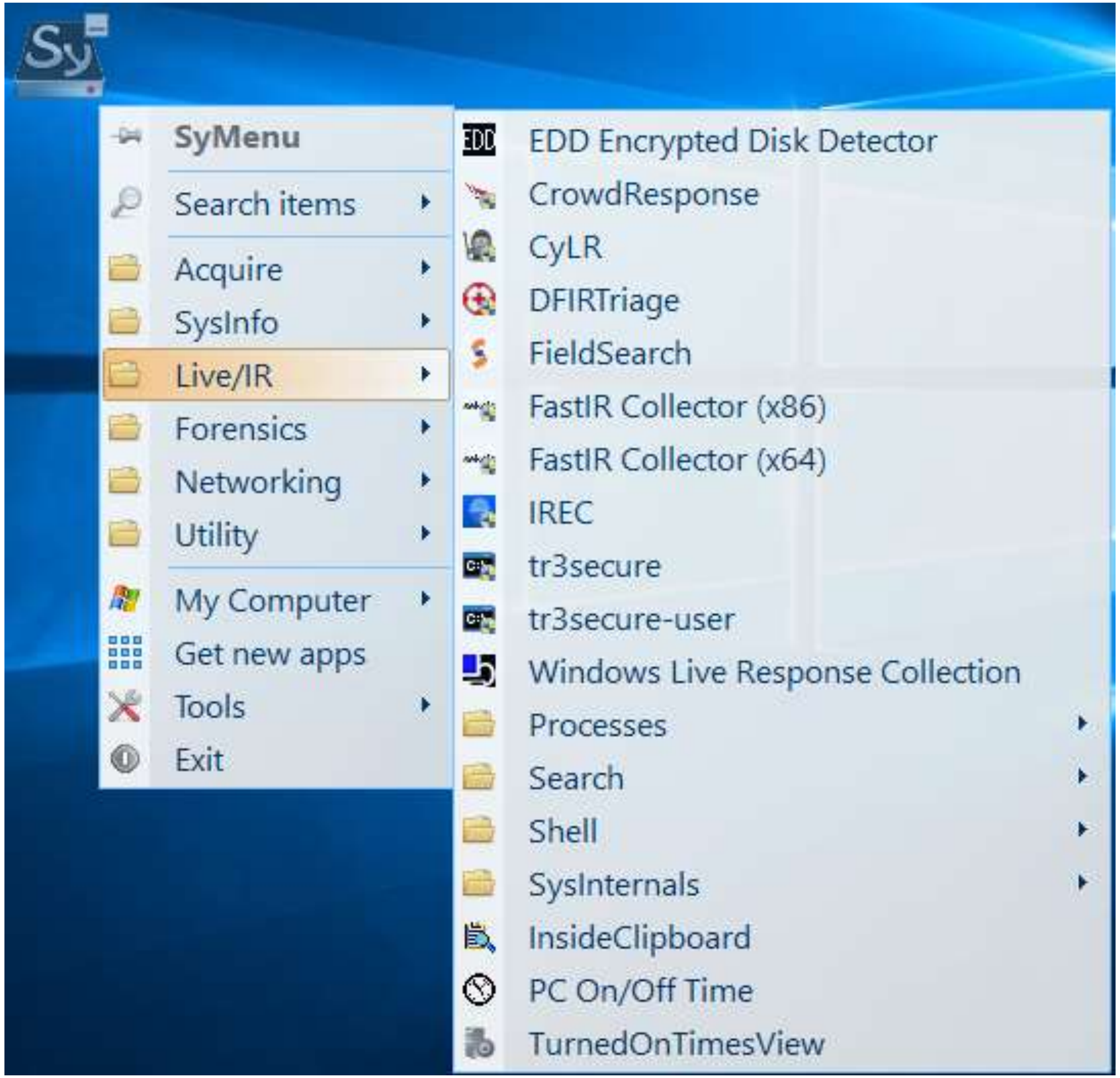
Bento - Acquisition



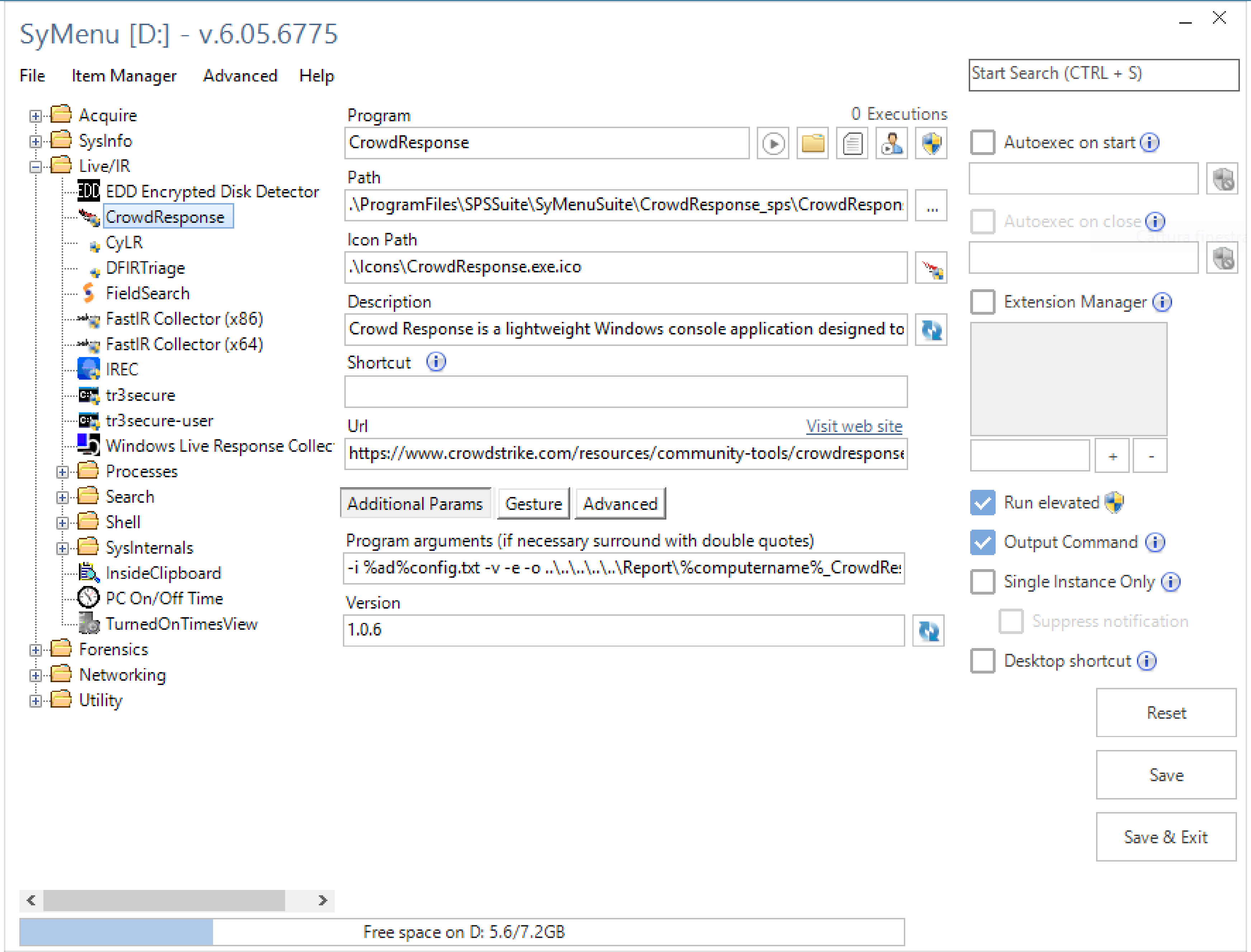
Bento – System Information Gathering



Bento – Live Forensics / Incident Response



High configurability



SyMenu [D:] - v.6.05.6775

Program: CrowdResponse

0 Executions

Path: .\ProgramFiles\SPSSuite\SyMenuSuite\CrowdResponse_sps\CrowdRespon

Icon Path: .\Icons\CrowdResponse.exe.ico

Description: Crowd Response is a lightweight Windows console application designed to

Shortcut:

Url: https://www.crowdstrike.com/resources/community-tools/crowdresponse

Program arguments (if necessary surround with double quotes): -i %ad%config.txt -v -e -o ..\..\..\..\..\Report\%computername%_CrowdRe:

Version: 1.0.6

□ Autoexec on start

□ Autoexec on close

□ Extension Manager

☑ Run elevated

☑ Output Command

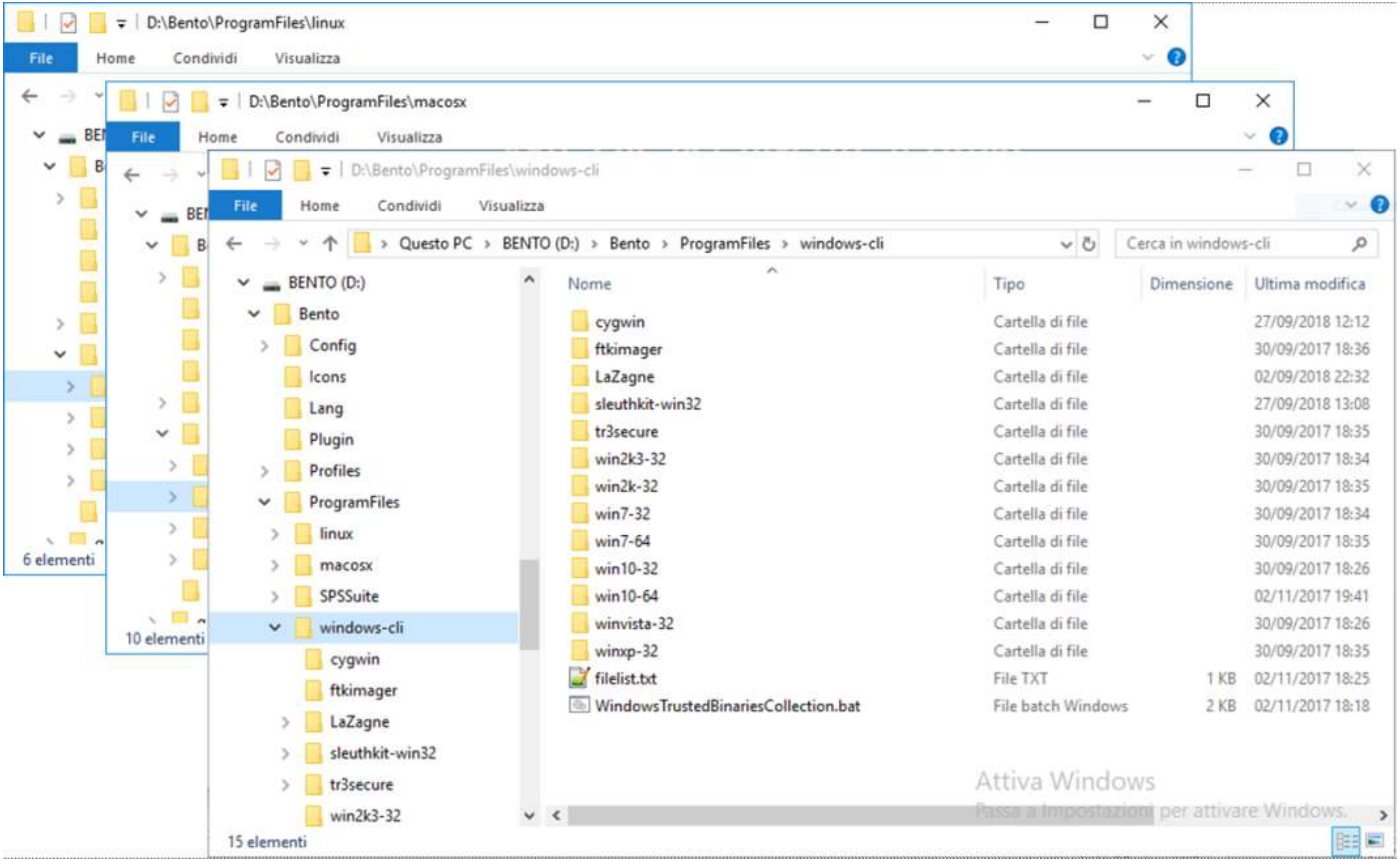
□ Single Instance Only

□ Suppress notification

□ Desktop shortcut

Free space on D: 5.6/7.2GB

Beyond the GUI: Linux, OSX e Windows CLI tools



D:\Bento\ProgramFiles\linux

6 elementi

D:\Bento\ProgramFiles\macosx

10 elementi

D:\Bento\ProgramFiles\windows-cli

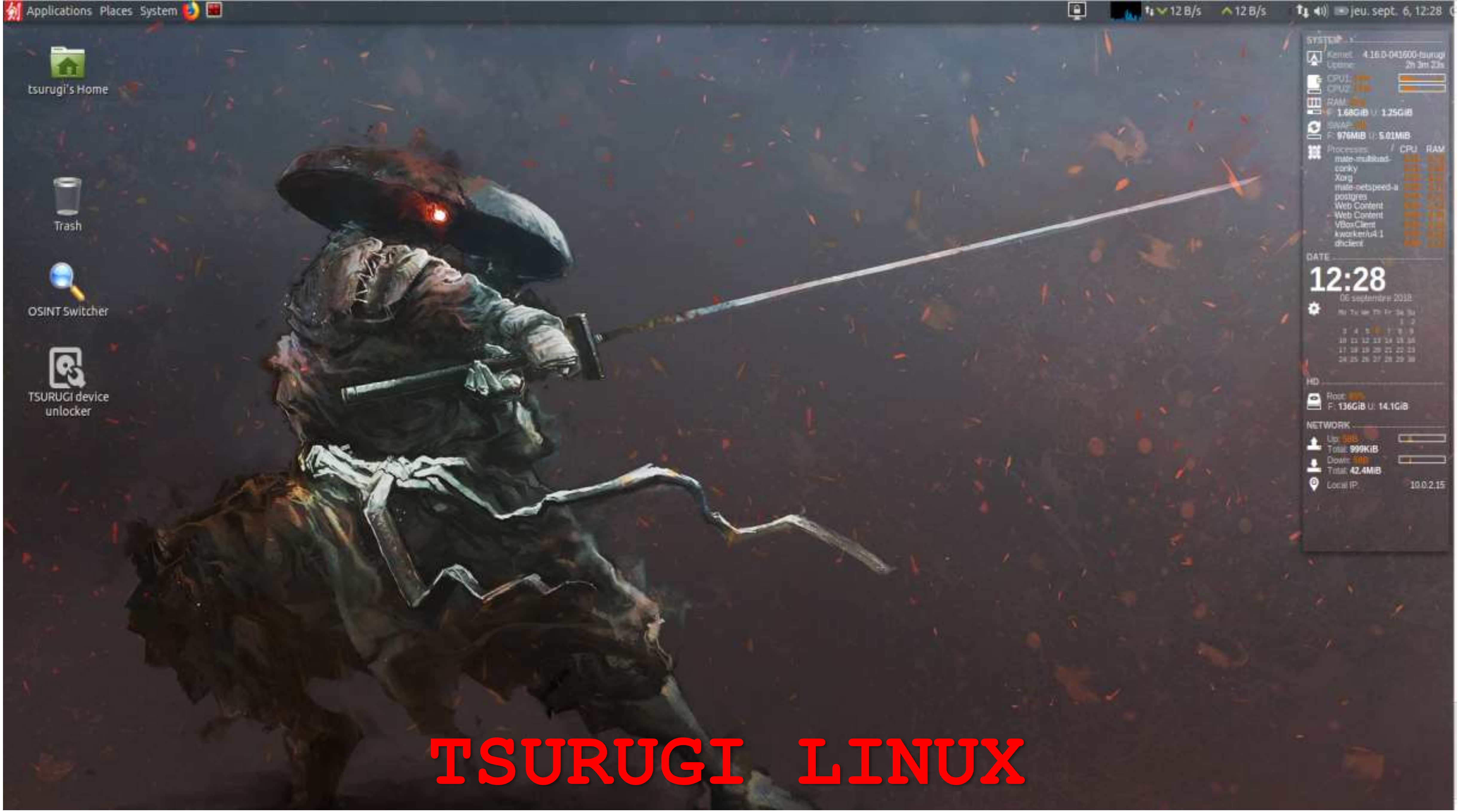
Questo PC › BENTO (D:) › Bento › ProgramFiles › windows-cli

Cerca in windows-cli

```
BENTO (D:)
  Bento
    Config
    Icons
    Lang
    Plugin
    Profiles
    ProgramFiles
      linux
      macosx
      SPSSuite
      windows-cli
        cygwin
        ftkimager
        LaZagne
        sleuthkit-win32
        tr3secure
        win2k3-32
```

Nome	Tipo	Dimensione	Ultima modifica
cygwin	Cartella di file		27/09/2018 12:12
ftkimager	Cartella di file		30/09/2017 18:36
LaZagne	Cartella di file		02/09/2018 22:32
sleuthkit-win32	Cartella di file		27/09/2018 13:08
tr3secure	Cartella di file		30/09/2017 18:35
win2k3-32	Cartella di file		30/09/2017 18:34
win2k-32	Cartella di file		30/09/2017 18:35
win7-32	Cartella di file		30/09/2017 18:34
win7-64	Cartella di file		30/09/2017 18:35
win10-32	Cartella di file		30/09/2017 18:26
win10-64	Cartella di file		02/11/2017 19:41
winvista-32	Cartella di file		30/09/2017 18:26
winxp-32	Cartella di file		30/09/2017 18:35
filelist.txt	File TXT	1 KB	02/11/2017 18:25
WindowsTrustedBinariesCollection.bat	File batch Windows	2 KB	02/11/2017 18:18

15 elementi



TSURUGI LINUX

tsurugi-linux.org

Tsurugi Linux

- Open source project, initially released in March 2018, dedicated to ***Digital Forensics*** and ***OSINT***

www.tsurugi-linux.org

- Three components:
  - **Tsurugi Acquire**
    - 32bit bootable Linux distribution, strictly designed for identification and acquisition *post mortem* of digital evidence
  - **Tsurugi Lab**
    - Full 64 bit Linux distribution designed for laboratory.
    - It comes with two user profiles:
      - a digital forensics analysis lab
      - an open source intelligence desktop
  - **Bento**
    - FLOSS toolkit designed for Live Forensics and Incident Response on the field, on Windows, Linux and OSX systems.

A QUICK OVERVIEW ON OUR

LABORATORY

Our laboratory activities

- **Refine collection on our LIMS**
    - Recognize and describe exhibits and their conditions
    - Assign unique IDs
    - Refine acquisition plan
- **Acquire data**
  - Remove or circumvent lockscreens, or crack passcodes
  - Execute forensic copies of exposed data
    - Mass storage devices (hard disks, SSD, thumbdrives, memory cards…)
    - Embedded memories from smartphones and tablets; drones; cams, bodycams, DVRs and other videosurveillance systems; IoT devices…
  - Dump data from cloud accounts (Google, Microsoft, iCloud, Facebook, Telegram…)
- **Analyse** data from:
  - Smartphones and tablets (Android e iOS, spreadtrum, KaiOS, Windows Phone, Blackberry, Symbian…)
  - Personal Computer and servers (Windows, Linux, OS X)
  - DVRs e NVRs
  - Drones
  - Vehicles (iVE)
  - Warrant returns (Google, Apple, Facebook, Instagram, Snapchat, Twitter…)

Types of forensic copy

Full bit stream image cannot always be obtained.

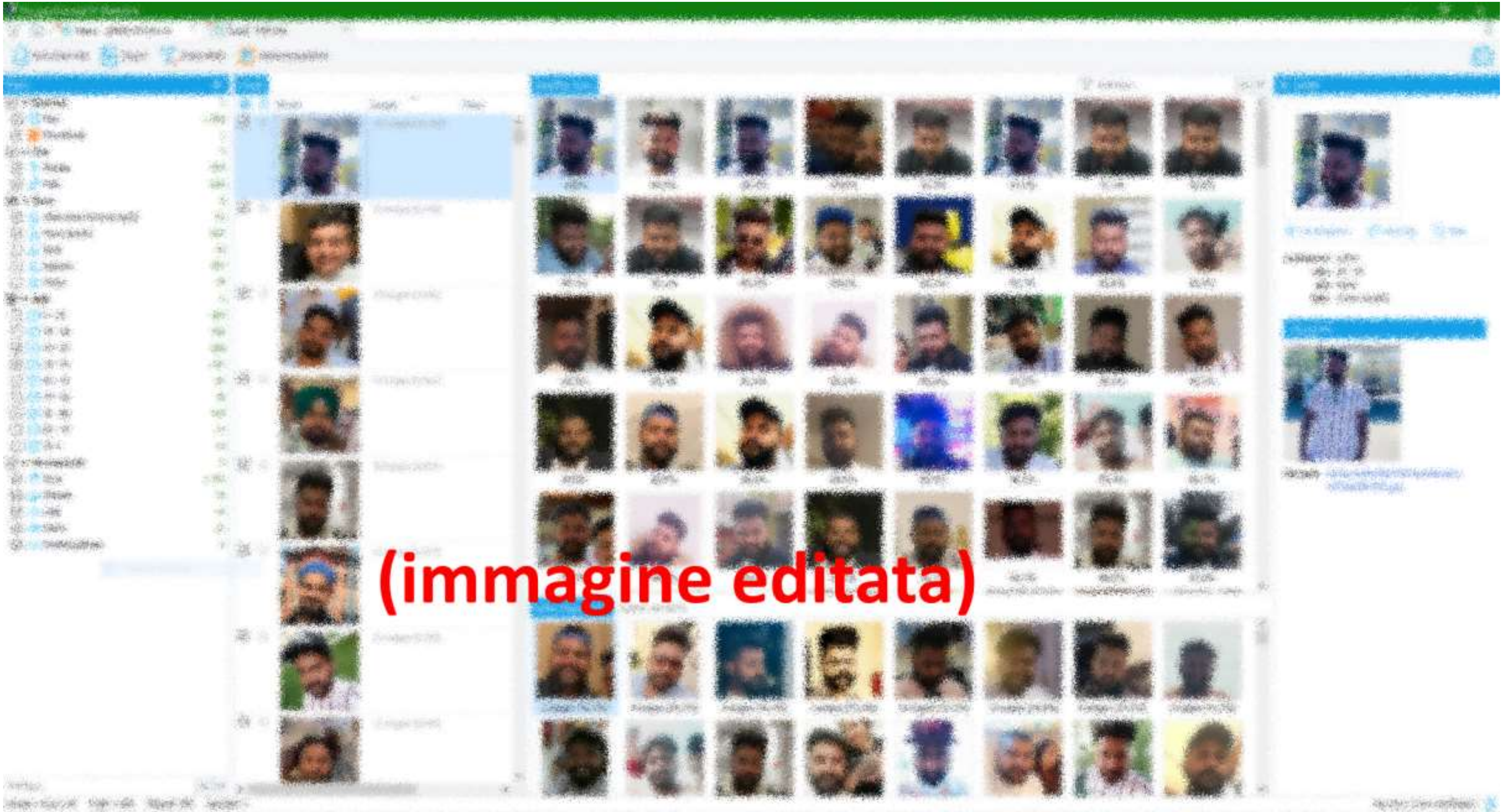
We can try to perform:

- Physical dump
  - The full bit stream image. It includes allocated and unallocated memory, so we can try to recover deleted files
- Full Filesystem dump
  - Full logical copy of every existent file and folder
- Partial Filesystem extraction
  - Logical copy of some filesystem branch (this may includes most of user's folders, but none of system's folders)
- Logical extraction
  - Logical copy of interpreted data, collected through resident operating system (contacts, messages, call logs, calendar, photos, videos, etc.)
- Screenshots and photo/video recordings

Tipical analysis

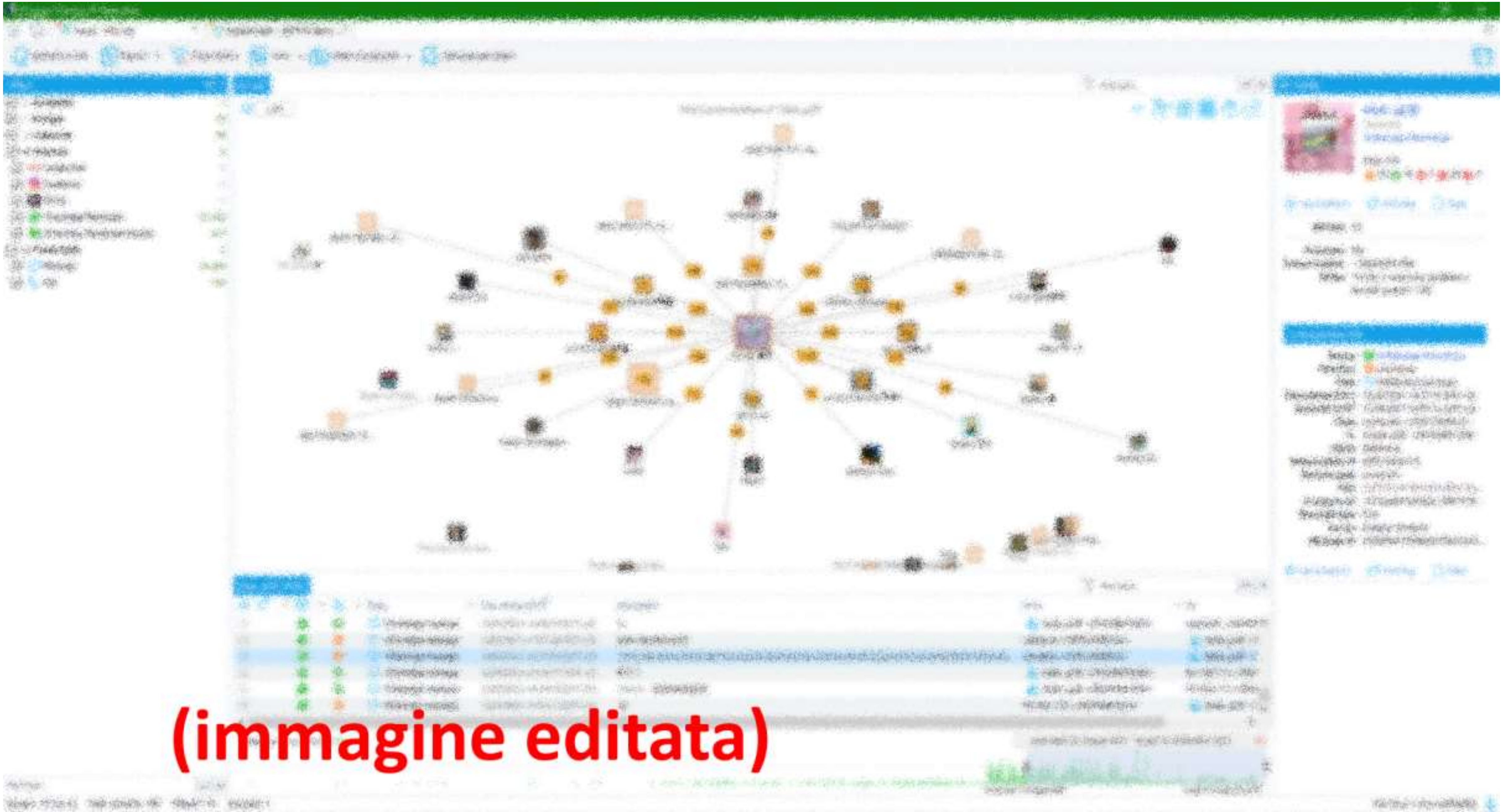
- Automatic detection, decoding, interpretation, deduplication and catalogation of artefacts describing user's activities
- Index and search text documents
- Categorize images and videos
  - Find similarity
  - Face detection and face recognition
  - Content recognition (vehicles and plates, drugs, weapons, nudity and CSA, Ids and credit cards, screenshot etc.)
  - Optical character recognition (OCR)
- Automated transcription of vocal tracks into searchable text
- Link analysis
- Timeline recostruction

Face similarity



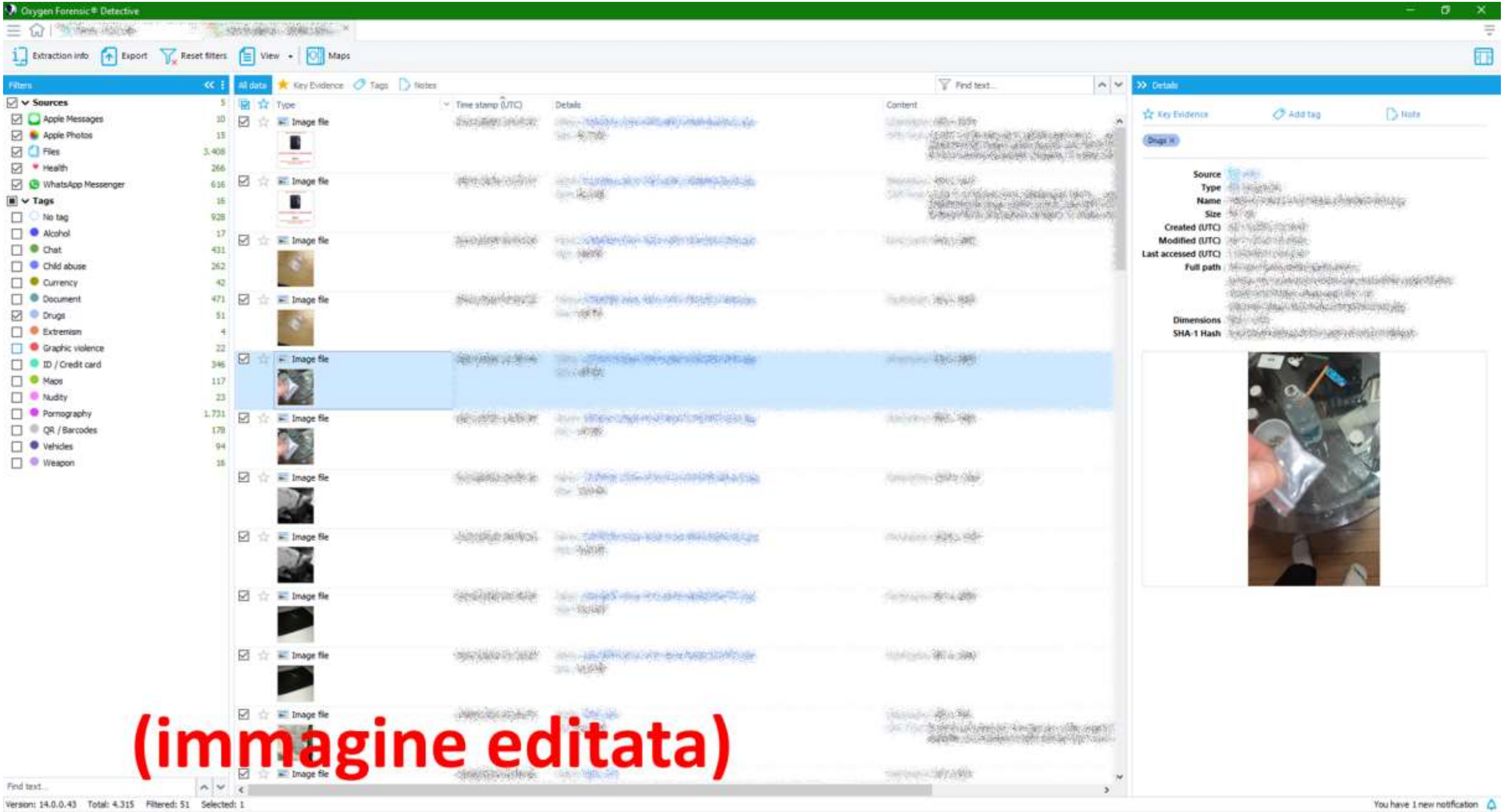
(immagine editata)

Social network analysis



(immagine editata)

Content recognition



Oxygen Forensic® Detective

Extraction info | Export | Reset filters | View | Maps

Filters

☑	**Sources**	5
☑	Apple Messages	10
☑	Apple Photos	15
☑	Files	3.408
☑	Health	266
☑	WhatsApp Messenger	616
▣	**Tags**	16
□	No tag	928
□	Alcohol	17
□	Chat	431
□	Child abuse	262
□	Currency	42
□	Document	471
☑	Drugs	51
□	Extremism	4
□	Graphic violence	22
□	ID / Credit card	346
□	Maps	117
□	Nudity	23
□	Pornography	1.731
□	QR / Barcodes	179
□	Vehicles	94
□	Weapon	16

All data | Key Evidence | Tags | Notes | Find text...

Type	Time stamp (UTC)	Details	Content
☑ Image file			
☑ Image file			
☑ Image file			
☑ Image file			
☑ Image file			
☑ Image file			
☑ Image file			
☑ Image file			
☑ Image file			
☑ Image file			
☑ Image file			
☑ Image file			

Details

Key Evidence | Add tag | Note

Drugs ×

Source
Type
Name
Size
Created (UTC)
Modified (UTC)
Last accessed (UTC)
Full path
Dimensions
SHA-1 Hash

Find text...

Version: 14.0.0.43 Total: 4.315 Filtered: 51 Selected: 1

You have 1 new notification

(immagine editata)

Tools

Most used tools:

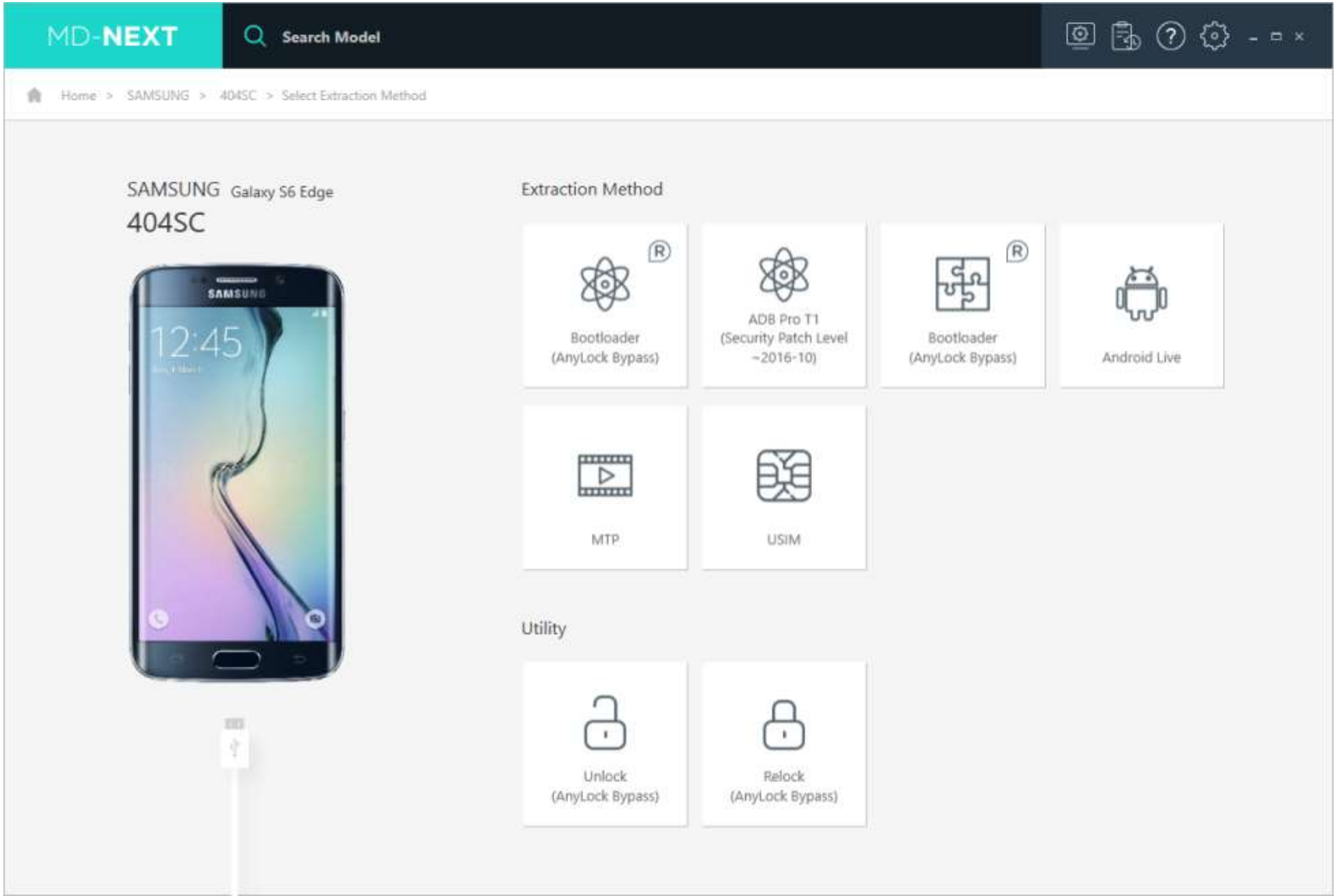
- Cellebrite UFED/Physical Analyzer
- MSAB XRY/XAMN
- Oxygen Forensic Detective
- Hancom MD-NEXT/MD-RED
- Elcomsoft Mobile Forensic Bundle
- Magnet Acquire/AXIOM
- Detego
- Autopsy
- Tsurugi Linux
- iLEAPP, ALEAPP
- APOLLO
- Andriller
- R-Studio, Amped5, X-Ways, Griffeye, DVR Examiner…

Other helpful tools:

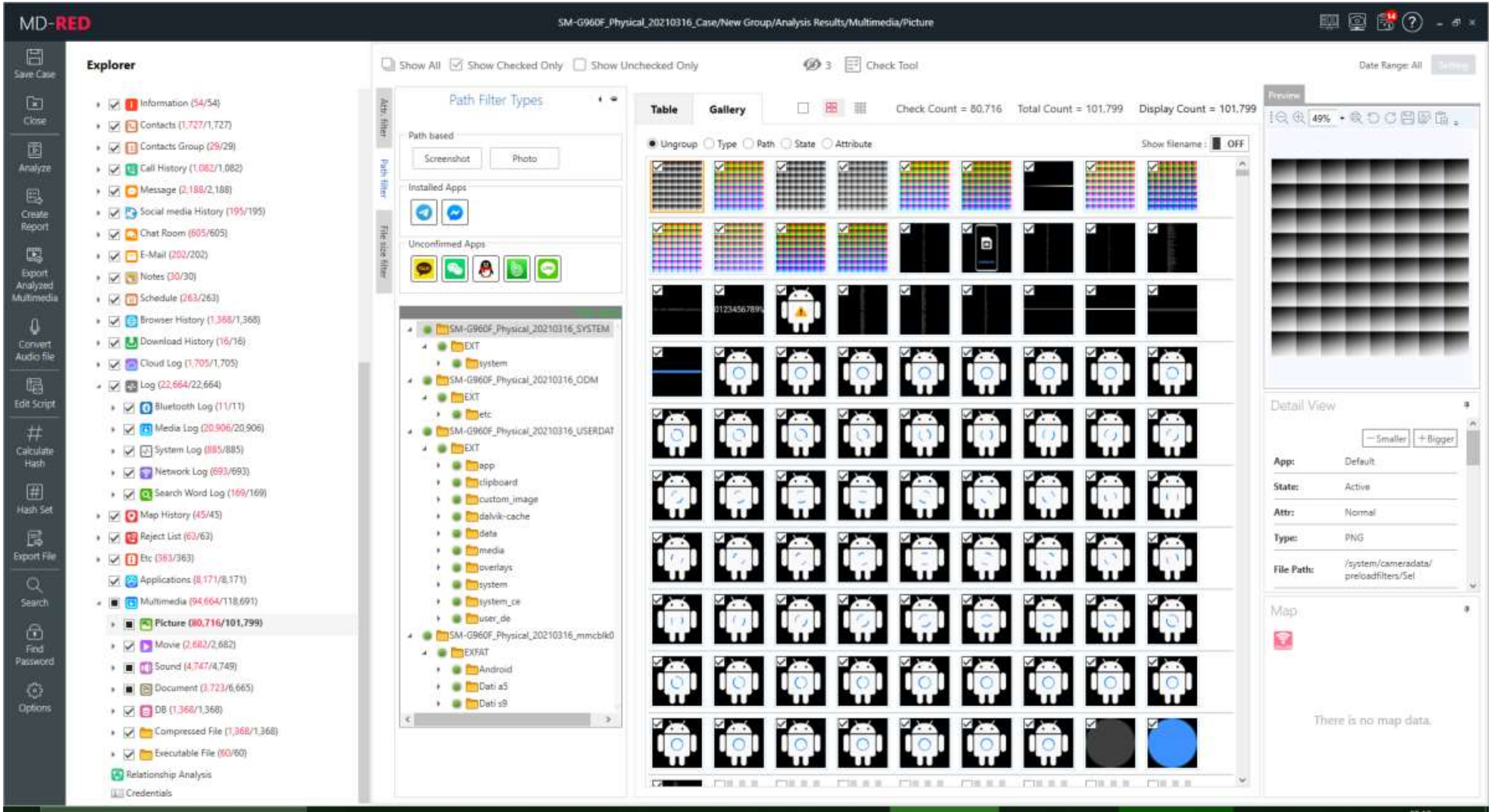
- 3uTools
- Libimobiledevice
- iMobiledevice
- iBackupbot
- iPhone Backup Extractor
- iFunBox
- iTools
- iExplorer
- HiSuite
- kobackupdec
- MiPCSuite
- Odin
- ADBGui
- ABE
- DARGui
- DrFone
- Plisteditor
- DB Browser

…

Hancom MD-NEXT



Hancom MD-RED



MD-RED SM-G960F_Physical_20210316_Case/New Group/Analysis Results/Multimedia/Picture

Explorer

- ☑ Information (54/54)
- ☑ Contacts (1,727/1,727)
- ☑ Contacts Group (29/29)
- ☑ Call History (1,082/1,082)
- ☑ Message (2,188/2,188)
- ☑ Social media History (195/195)
- ☑ Chat Room (605/605)
- ☑ E-Mail (202/202)
- ☑ Notes (30/30)
- ☑ Schedule (263/263)
- ☑ Browser History (1,368/1,368)
- ☑ Download History (16/16)
- ☑ Cloud Log (1,705/1,705)
- ☑ Log (22,664/22,664)
  - ☑ Bluetooth Log (11/11)
  - ☑ Media Log (20,906/20,906)
  - ☑ System Log (885/885)
  - ☑ Network Log (693/693)
  - ☑ Search Word Log (169/169)
- ☑ Map History (45/45)
- ☑ Reject List (63/63)
- ☑ Etc (363/363)
- ☑ Applications (8,171/8,171)
- ■ Multimedia (94,664/118,691)
  - ■ **Picture (80,716/101,799)**
  - ☑ Movie (2,682/2,682)
  - ■ Sound (4,747/4,749)
  - ■ Document (3,723/6,665)
  - ☑ DB (1,368/1,368)
  - ☑ Compressed File (1,368/1,368)
  - ☑ Executable File (60/60)
- Relationship Analysis
- Credentials

□ Show All ☑ Show Checked Only □ Show Unchecked Only 3 Check Tool Date Range: All

Path Filter Types

Path based

Screenshot Photo

Installed Apps

Unconfirmed Apps

- SM-G960F_Physical_20210316_SYSTEM
  - EXT
    - system
- SM-G960F_Physical_20210316_ODM
  - EXT
    - etc
- SM-G960F_Physical_20210316_USERDAT
  - EXT
    - app
    - clipboard
    - custom_image
    - dalvik-cache
    - data
    - media
    - overlays
    - system
    - system_ce
    - user_de
- SM-G960F_Physical_20210316_mmcblk0
  - EXFAT
    - Android
    - Dati a5
    - Dati s9

Table Gallery

Check Count = 80,716 Total Count = 101,799 Display Count = 101,799

● Ungroup ○ Type ○ Path ○ State ○ Attribute Show filename : OFF

Preview

49%

Detail View

− Smaller + Bigger

App: Default

State: Active

Attr: Normal

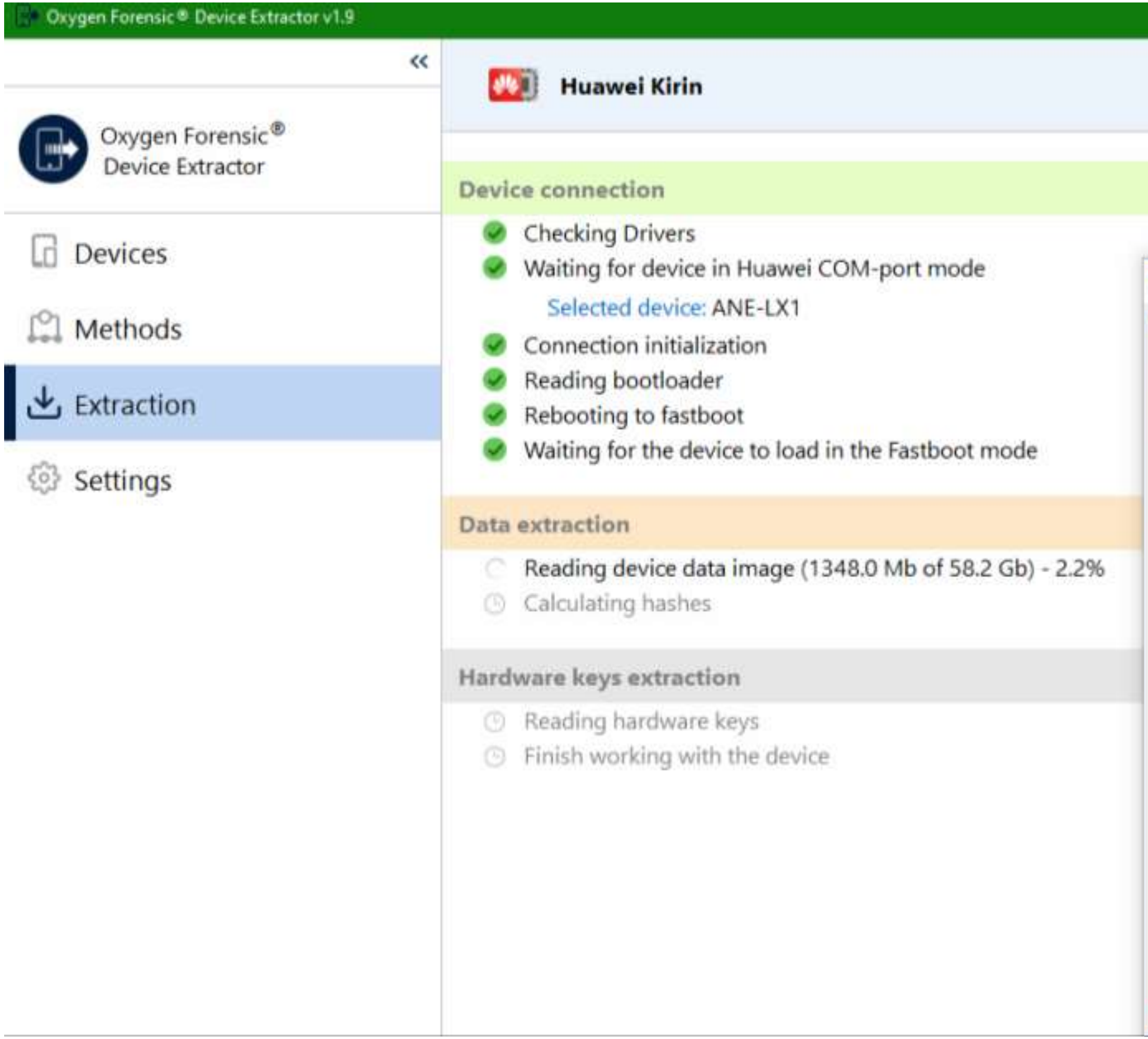
Type: PNG

File Path: /system/cameradata/preloadfilters/Sel

Map

There is no map data.

Hardware interventions



Oxygen Forensic® Device Extractor v1.9

Huawei Kirin

Device connection

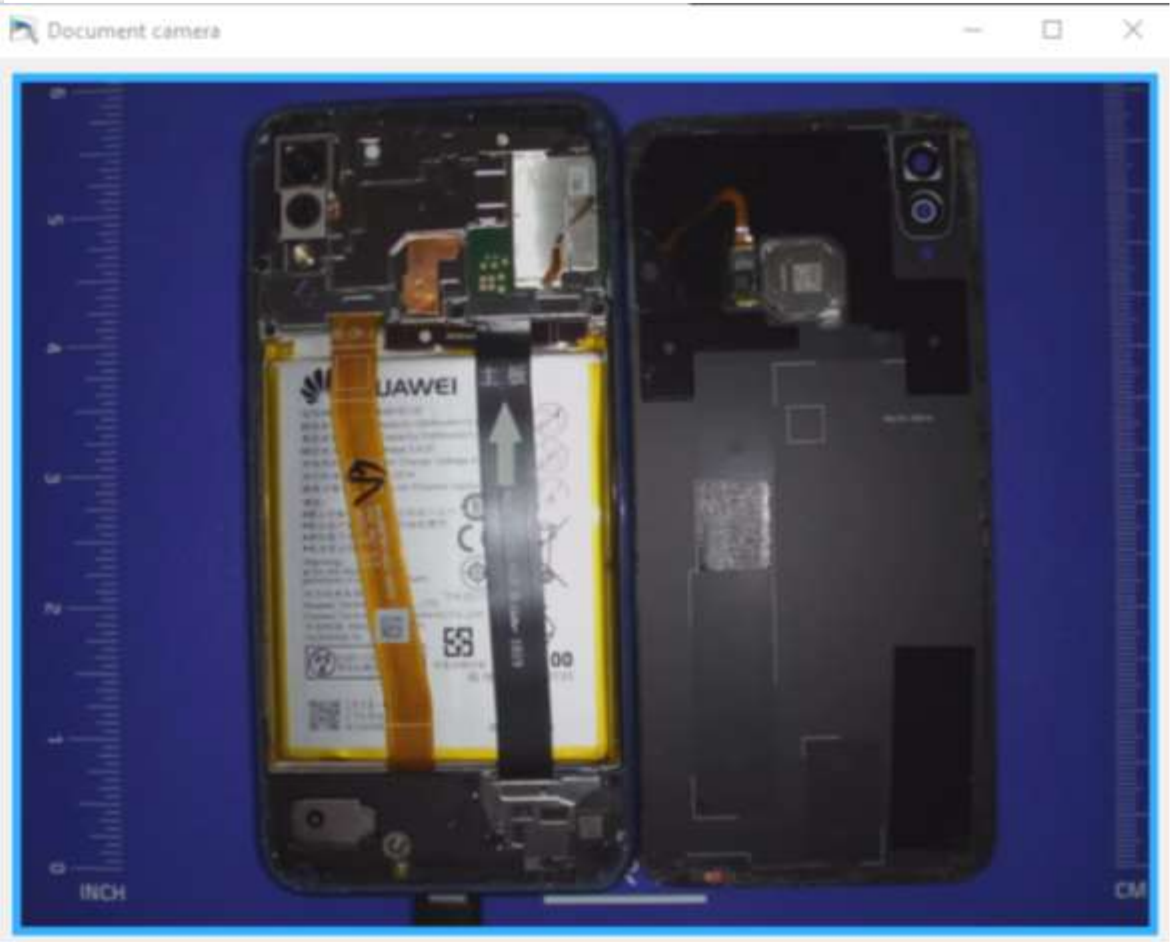
- ✓ Checking Drivers
- ✓ Waiting for device in Huawei COM-port mode
  - Selected device: ANE-LX1
- ✓ Connection initialization
- ✓ Reading bootloader
- ✓ Rebooting to fastboot
- ✓ Waiting for the device to load in the Fastboot mode

Data extraction

- ○ Reading device data image (1348.0 Mb of 58.2 Gb) - 2.2%
- ○ Calculating hashes

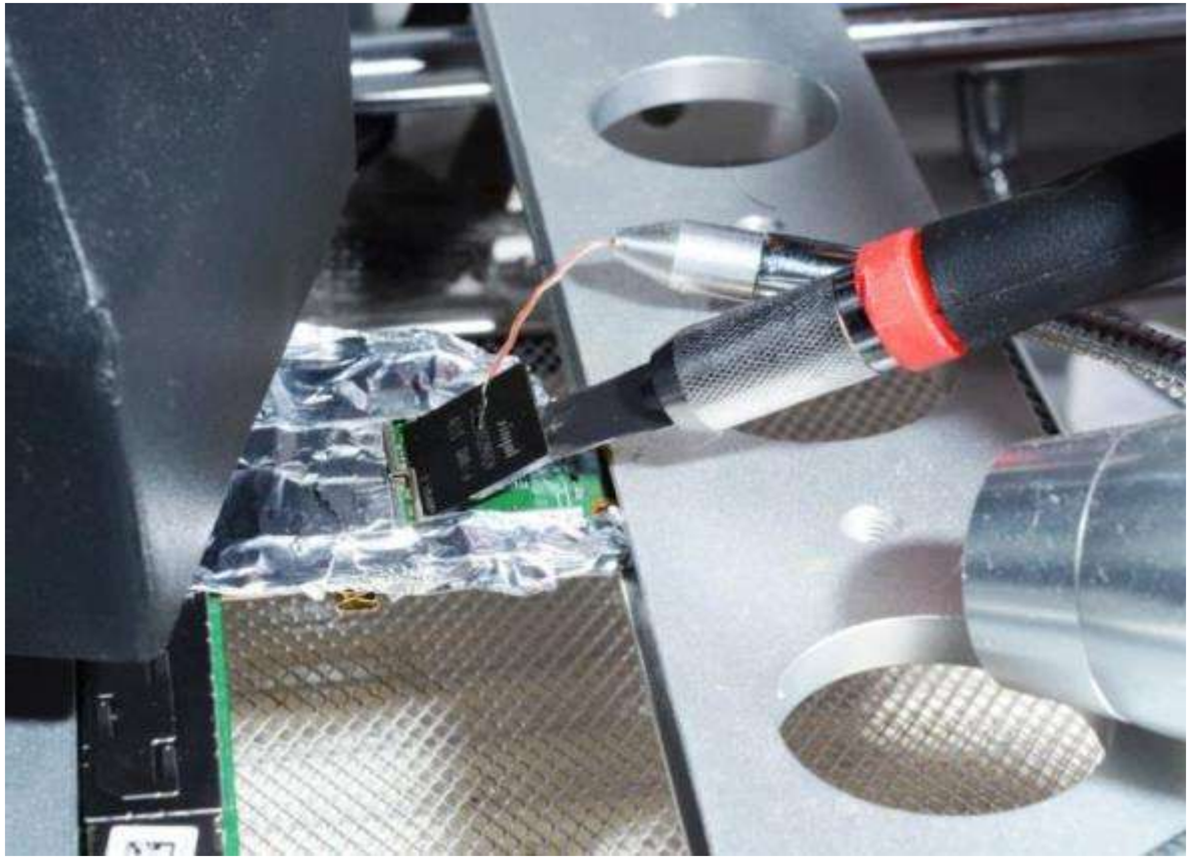
Hardware keys extraction

- ○ Reading hardware keys
- ○ Finish working with the device



Extreme measures

- Cleanroom to recover hard drives
- Chip-off of embedded memories



Resources reserved to LE

Keep in touch

Davide Rebus Gabrini

e-mail: davide.gabrini@unipv.it

GPG Public Key: www.tipiloschi.net/rebus.asc
KeyID: 0x176560F7

For more bullshit click on

www.tipiloschi.net

facebook.com/gabrini

twitter.com/therebus

it.linkedin.com/in/rebus

- **Rebus' Digest**
  newsletter on cybercrime, hacking, digital forensics…
- **EventiLoschi**
  public calendar of public conferences