

# COMPUTER FORENSICS

## Lezione 22: Mobile Forensics *acquisizione e analisi*



A.A. 2021/22

**Dott. Lorenzo LAURATO**

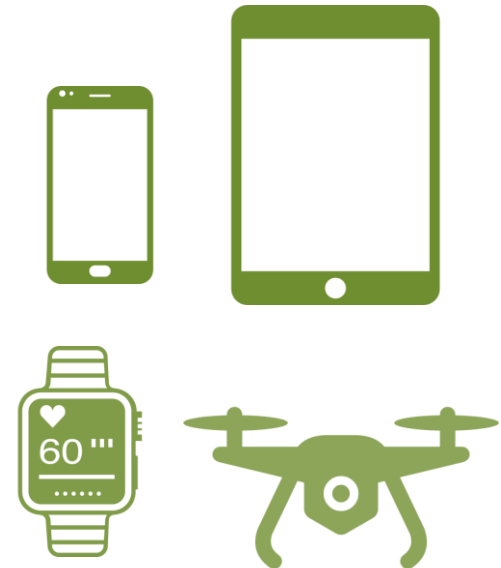
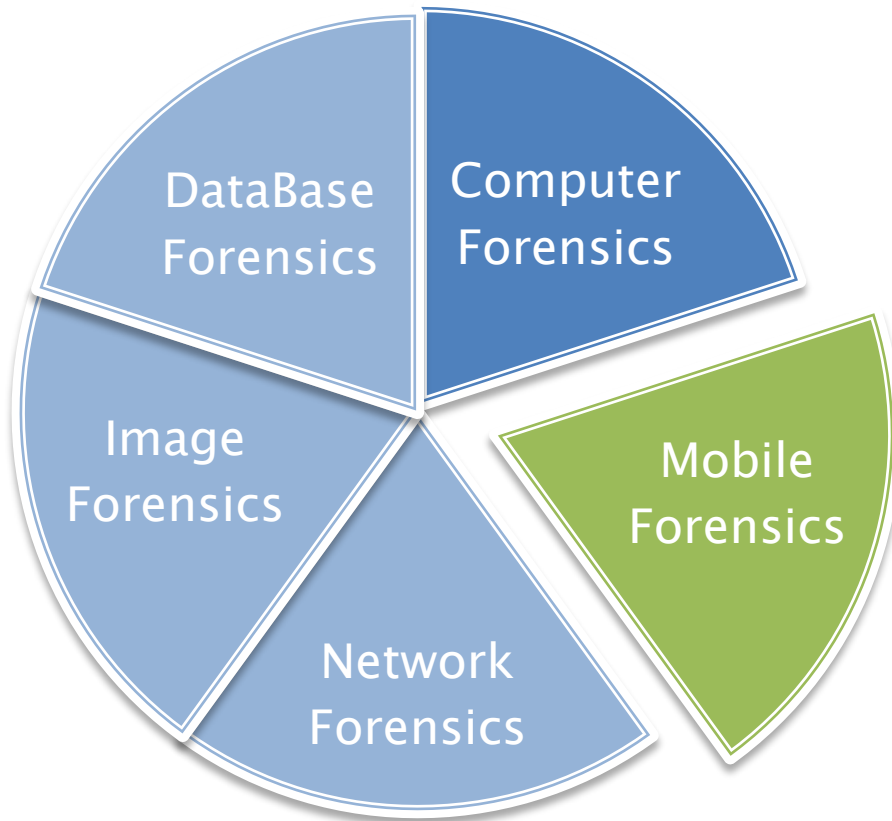


# Mobile Forensics

»» Overview

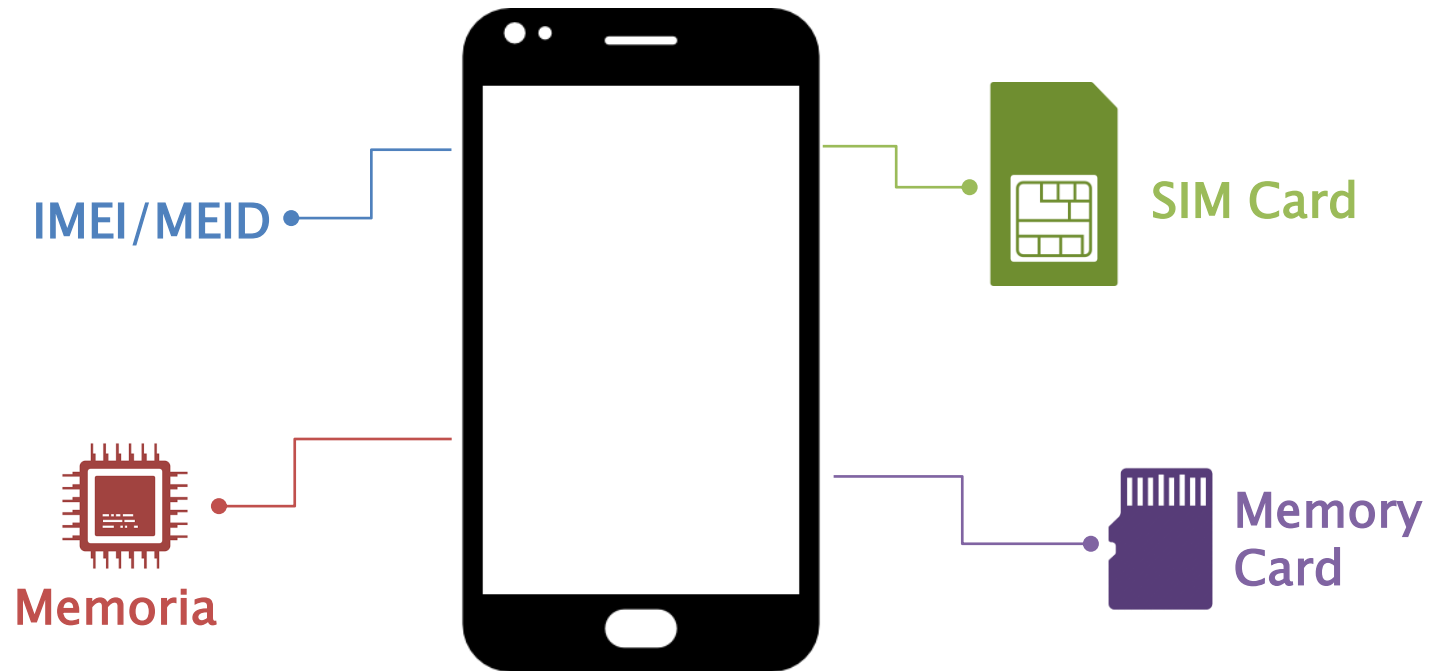


# Digital Forensics



# Mobile Forensics

## *evidence*



# Mobile Forensics

## *GSM/CDMA*

### GSM

*Global System for Mobile communications*

- ▶ **IMEI** (*International Mobile Equipment Identity*): codice univoco del dispositivo all'interno della rete mobile
- ▶ **SIM Card** (*Subscriber Identity Module*):
  - ICCID (*Integrated Circuit Card ID*): nr. seriale 19/20 cifre
  - IMSI (*International Mobile Subscriber Identity*): identificativo nella rete mobile dell'operatore

### CDMA

*Code Division Multiple Access*

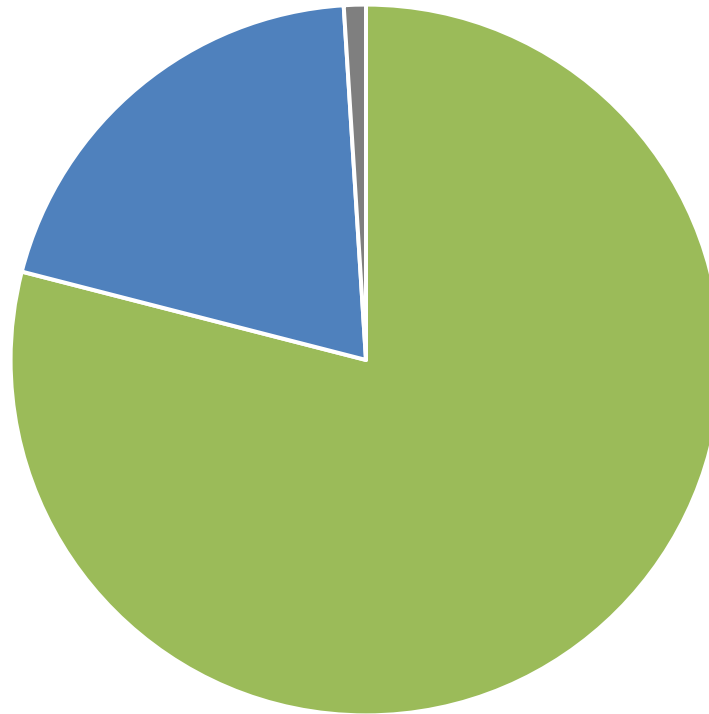
- ▶ **MEID** (*mobile equipment identifier*): codice univoco del dispositivo all'interno della rete mobile
- ▶ **NO SIM Card**

# Mobile Forensics

## *dispositivi*



O.S.



■ Android ■ Apple iOS ■ Altri



# Mobile Forensics

## *la raccolta*

- 1) Disabilitare tutte le connessioni:
  - OFF Line Mode/Airplane Mode
  - Faraday Bag
  - L'obiettivo è evitare:
    - Remote Wipe
    - Sovrascrittura di informazioni presenti



# Mobile Forensics

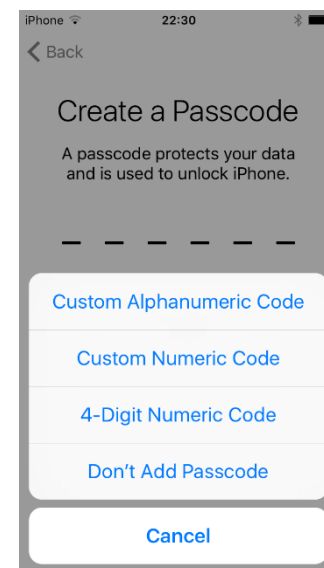
## *la raccolta*

### 2) Sbloccare il dispositivo:

#### ◦ Apple iOS:

- PassCode a 4 cifre
- PassCode a 6 cifre (default)
- PassCode > 6 cifre
- Password alfanumerica
- *Face ID/ Touch ID*

Max 10 tentativi





# Mobile Forensics

## *la raccolta*



### 2) Sbloccare il dispositivo:

#### ◦ Android OS:

- PassCode  $\geq 4$  cifre
- Password alfanumerica
- Pattern
- *Face ID/ Touch ID*
- *Password di avvio*

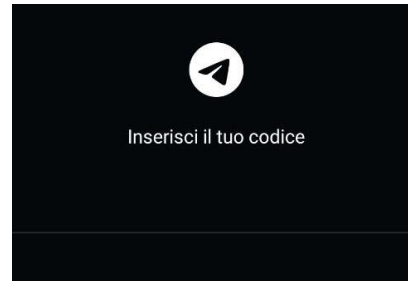
Max ? Tentativi

# Mobile Forensics

## *la raccolta*



- 2) Sbloccare il dispositivo:
- Protezione implementata dalle app



- *Applicazione di sicurezza*

# Mobile Forensics

## *la raccolta*



### 2) Sbloccare il dispositivo:

- **SIM Card:**

- PassCode 4 cifre (PIN)
  - Max 3 tentativi
- PUK: recovery code
  - 8 cifre
  - Max 10 tentativi

# Mobile Forensics

## *la raccolta*



- 3) Spegnere il dispositivo:
- Alcuni dispositivi richiedono lo sblocco

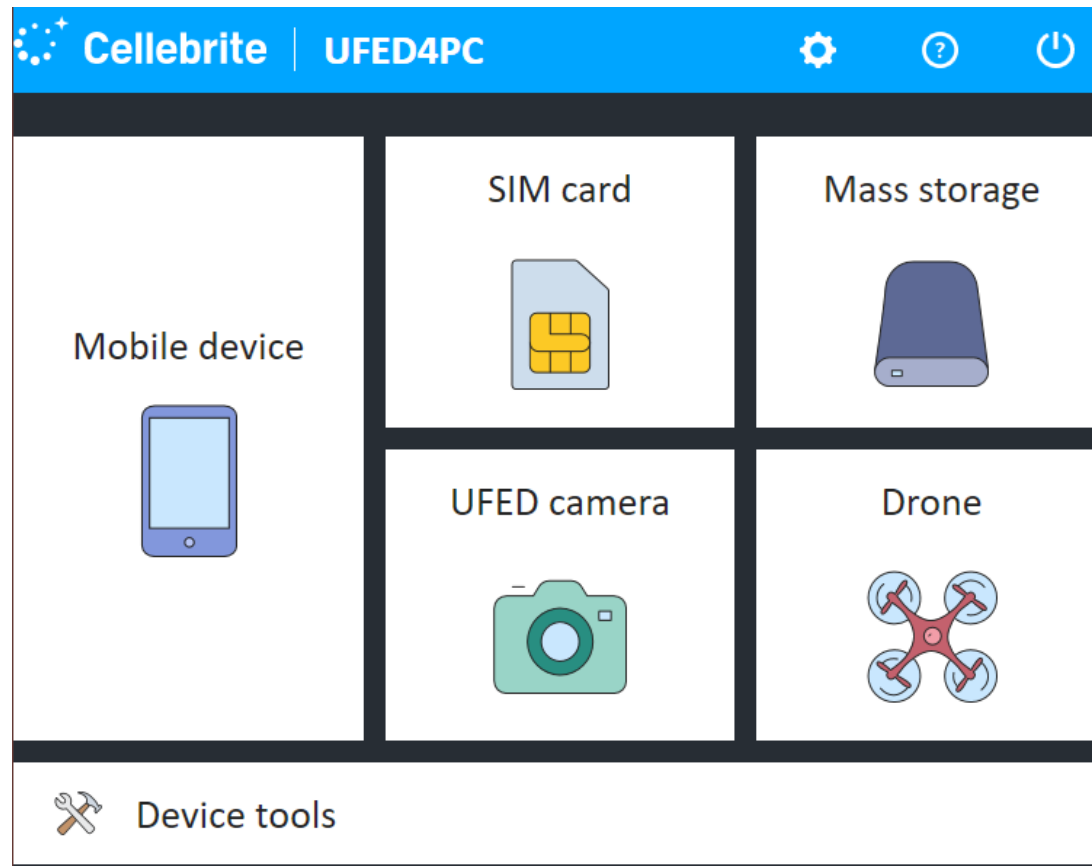
# Mobile Forensics

»» Acquisizione



# Mobile Forensics: acquisizione *strumenti*

## ► *Cellebrite UFED (Universal Forensic Extraction Device)*



# Mobile Forensics: acquisizione *strumenti*

- ▶ *Cellebrite UFED (Universal Forensic Extraction Device)*



# Mobile Forensics: acquisizione *memory card*



- ▶ *Micro SD, MiniSD, etc.*
  - *..., 16GB, 32GB, 64GB, 128GB, etc.*
  - *Foto, Video, Musica*
  - *Applicazioni*
  - *Backup*
  - *...*
- ▶ E' la prima cosa da acquisire:
  - *writeblock hardware/software*



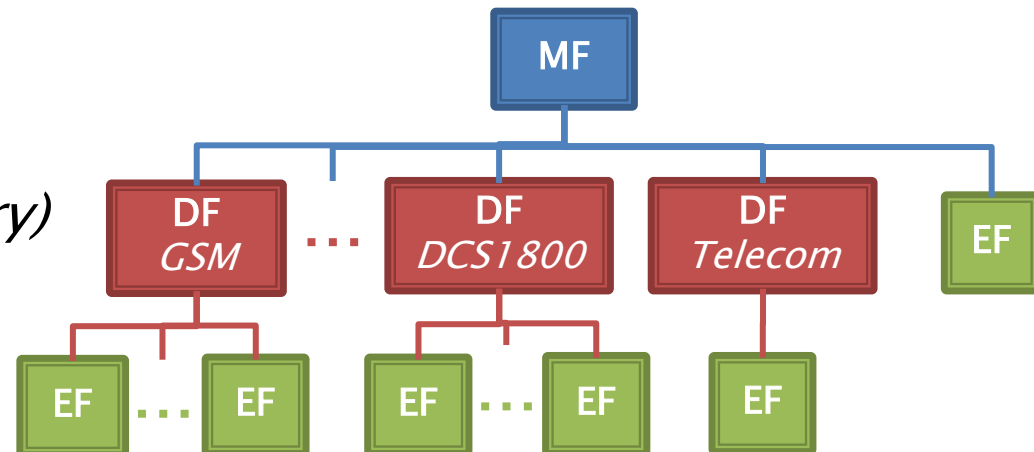
# Mobile Forensics: acquisizione

## *SIM card*



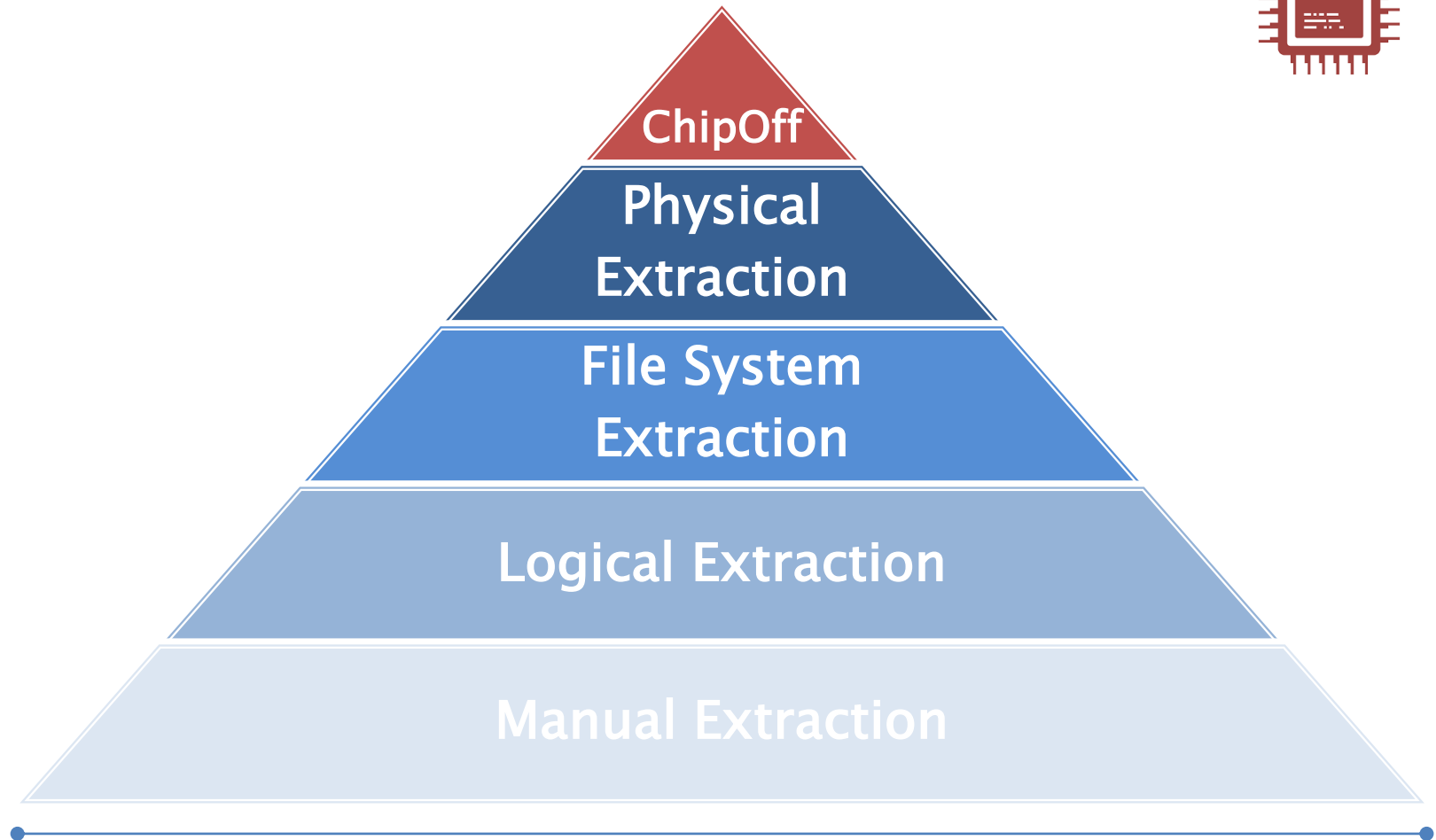
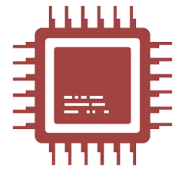
- ▶ (Mini) SIM, Micro SIM, Nano SIM
  - 16KB, 32KB, 64KB, 128KB, etc.
  - Rubrica
  - SMS
  - Identificavi: ICCID, IMSI

- ▶ Struttura:
  - Master File (*root*)
  - Dedicated File (*directory*)
  - Elementary File (*file*)



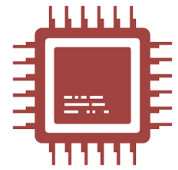
- ▶ Acquisizione:
  - *Lettore di SIM Card*













# Mobile Forensics: acquisizione *tipi*



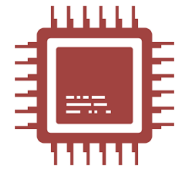
*Nr. di dispositivi supportati*













# Mobile Forensics: acquisizione *tipi*



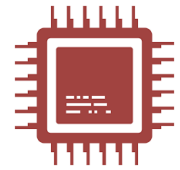
All	Vendors	Generic profiles	Recently used
<p>Sony (SonyEricsson)</p> 	<p>Sunup</p>  三普手机 专业制造	<p>Swisstone</p> 	<p>Tablets</p> 
<p>TCL</p> 	<p>TEC</p> 	<p>Tecno</p> 	<p>Telit</p> 
<p>Texet</p> 	<p>TIM</p> 	<p>T-Mobile</p> 	<p>TomTom</p> 

# Mobile Forensics: acquisizione *tipi*









<p>Sony (SonyEricsson) D5833 Xperia Z3 Compact</p> 	<p>Sony (SonyEricsson) D6503 Xperia Z2</p> 	<p>Sony (SonyEricsson) D6603 Xperia Z3</p> 	<p>Sony (SonyEricsson) D6616 Xperia Z3</p> 
<p>Sony (SonyEricsson) D6643 Xperia Z3 TV</p> 	<p>Sony (SonyEricsson) D6653 Xperia Z3</p> 	<p>Sony (SonyEricsson) D6708 Xperia Z3v</p> 	<p>Sony (SonyEricsson) D750i</p> 
<p>Sony (SonyEricsson) E2006 Xperia E4g</p> 	<p>Sony (SonyEricsson) E2104 Xperia E4</p> 	<p>Sony (SonyEricsson) E2105 Xperia E4</p> 	<p>Sony (SonyEricsson) E2303 Xperia M4 Aqua</p> 

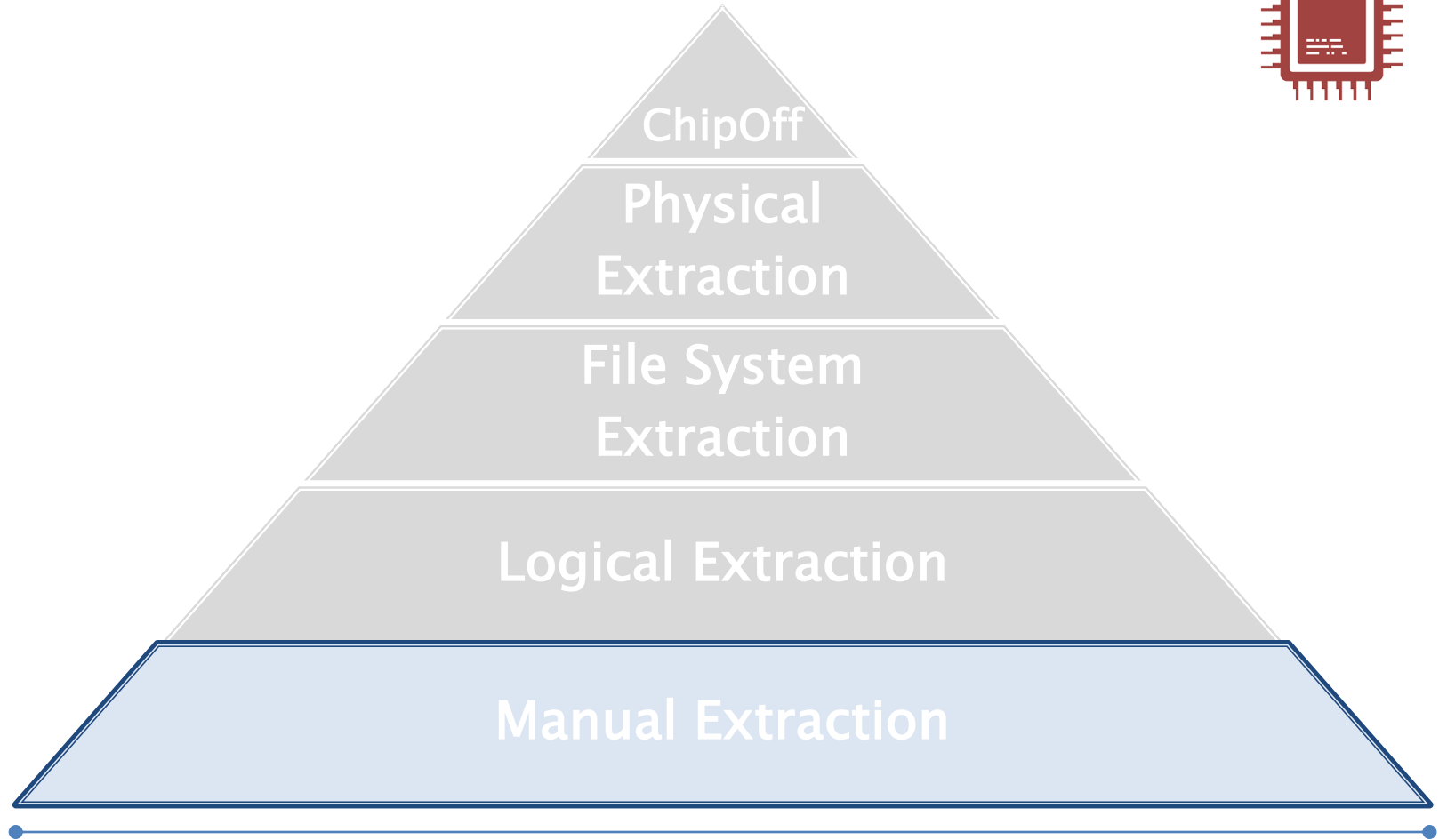
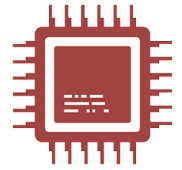
# Mobile Forensics: acquisizione *tipi*



Sony (SonyEricsson) D6603 Xperia Z3  
Cable A with black tip T-100

 Advanced Logical	 Disable/Re-Enable User Lock <small>Lock Bypass</small>	 File system	 Physical
 Camera	 Screenshot		

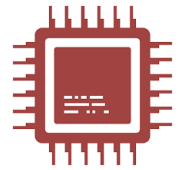
# Mobile Forensics: acquisizione



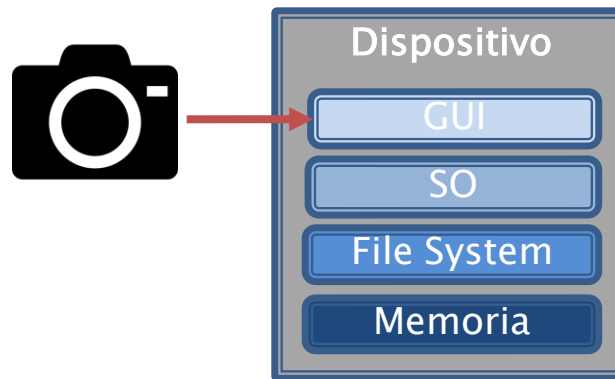
*Nr. di dispositivi supportati*

# Mobile Forensics: acquisizione

## *Manual Extraction*

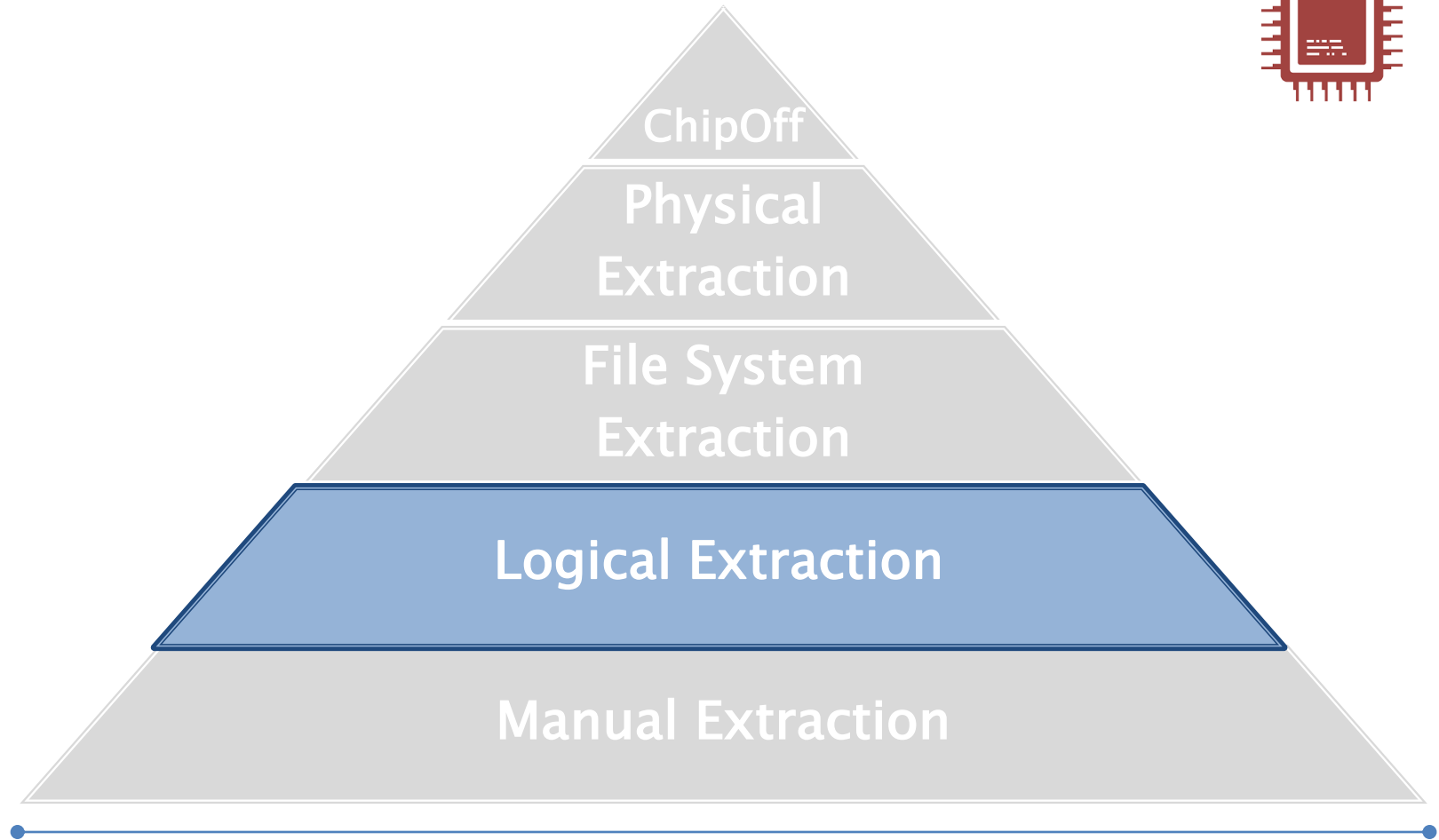
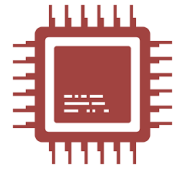


- ▶ repertazione fotografica del contenuto
  - *Interagire con la GUI*



- ▶ **Svantaggi:**
  - Processo lungo
  - Rischio modifica/cancellazione dei dati
  - Visualizzazione limitata delle informazioni
- ▶ **Limiti:**
  - Display non funzionante
  - Codice di sblocco

# Mobile Forensics: acquisizione

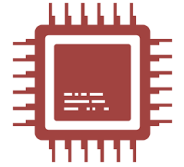


*Nr. di dispositivi supportati*

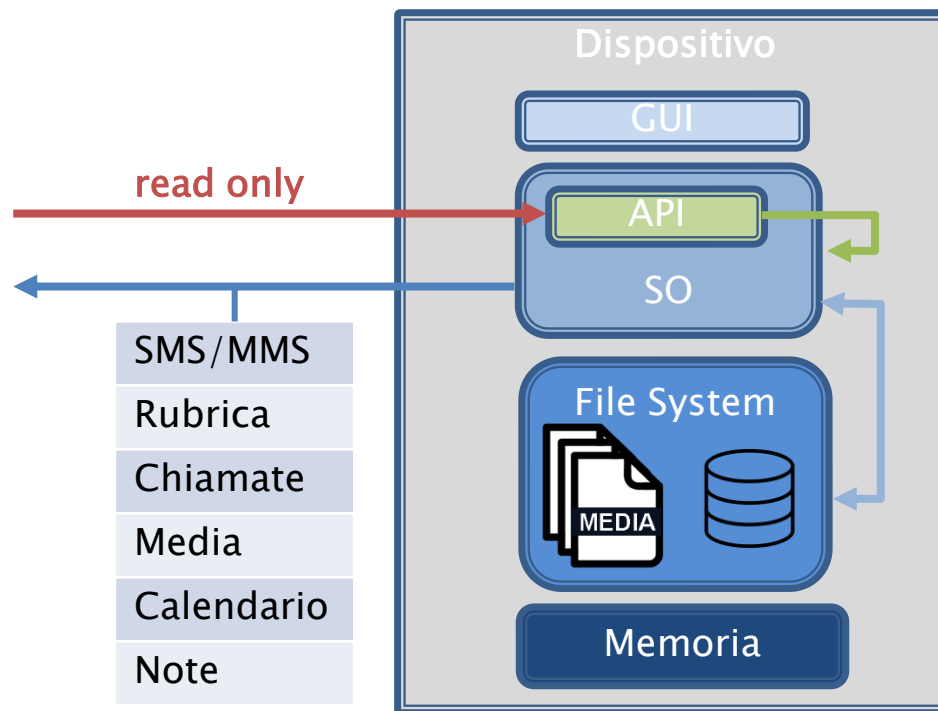


# Mobile Forensics: acquisizione

## *Logical Extraction*

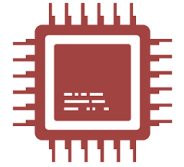


- Estrazione dei dati tramite API del dispositivo



# Mobile Forensics: acquisizione

## *Logical Extraction*

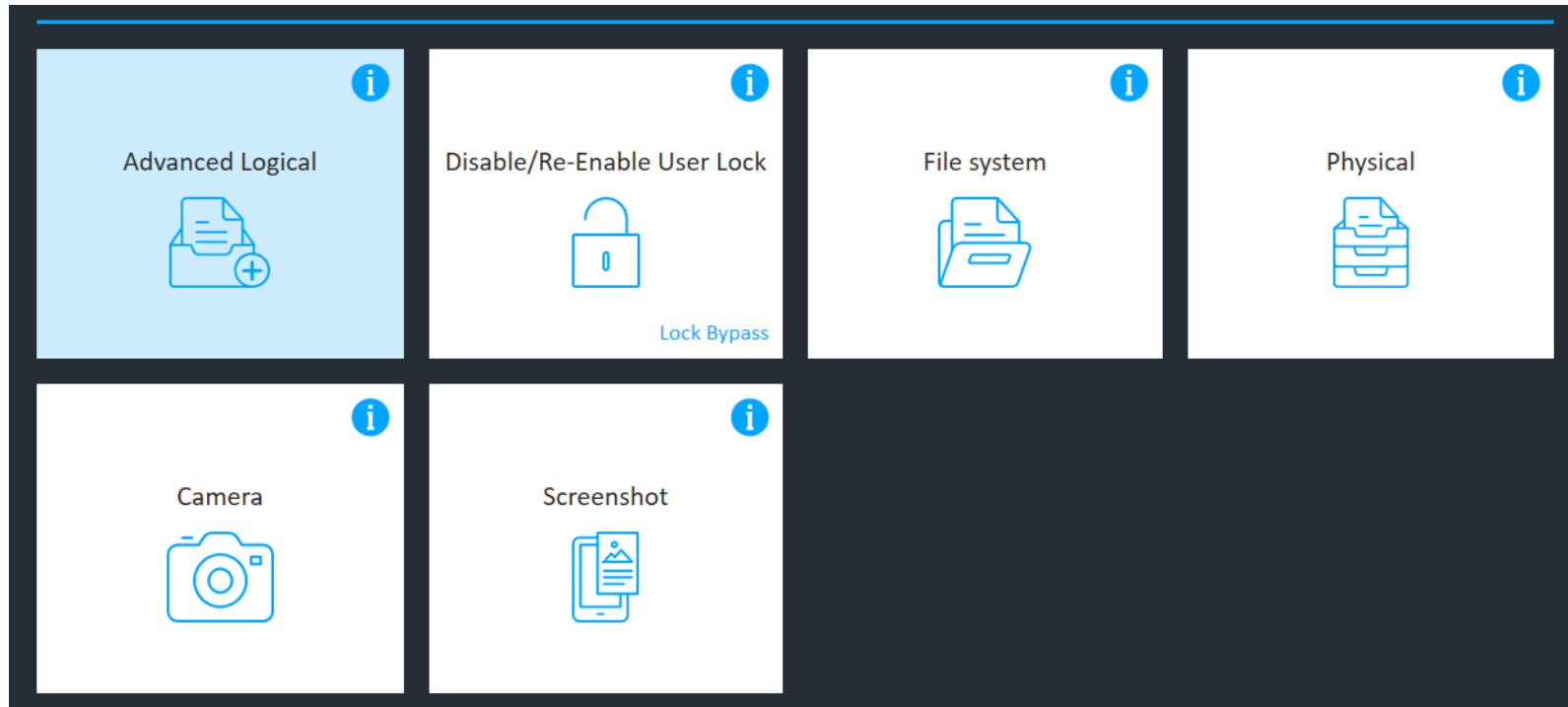
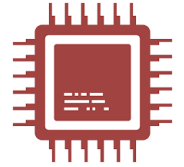


### ► Limiti:

- I risultati dipendono dall'API
  - Parziali:
    - solo alcune informazioni di un dato
    - solo alcuni dati: nessun dato di app di terze parti
- Codice di sblocco

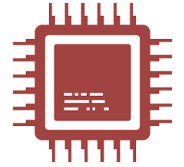
# Mobile Forensics: acquisizione

## *Logical Extraction*




# Mobile Forensics: acquisizione




## *Logical Extraction*




Sony (SonyEricsson) D6603 Xperia Z3  
Cable A with black tip T-100















---

 Extract from

 Device	 SIM	 Memory Card
--	---	---

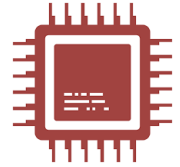
---

 Choose data types to extract ☐ All

 Contacts	 SMS	 MMS	 Calendar
 Pictures	 Audio/Music	 Videos	 Ringtones
 Call Logs	 Files	 Email	 IM
 Browsing Data	 User Dictionary		

# Mobile Forensics: acquisizione

## *Logical Extraction*



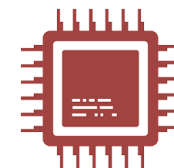
- Attachments
- Audio
- Images
- Ringtones
- Backup 2016\_05\_20 (001).cal
- Backup 2016\_05\_20 (001).clog
- Backup 2016\_05\_20 (001).MMS
- Backup 2016\_05\_20 (001).PBB
- Backup 2016\_05\_20 (001).SMS**

- PA Logical.ufd
- Report.html
- Report.xml
- Report\_AudioSection.html
- Report\_CalendarSection.html
- Report\_CallLogsSection.html
- Report\_ContactsSection.html
- Report\_DatabasesSection.html
- Report\_ImagesSection.html
- Report\_MMSSection.html
- Report\_RingtonesSection.html
- Report\_SMSSection.html
- Report\_VideoSection.html

```
Type(1)=0
Source(1)=1
Folder(1)=1
SMSC(12)=+12063130057
Number(12)=+14782279373
Date(6)=150826
Time(6)=100039
Body(261)=Señor El Chappo, The new lab is up and running. The U.S. Coast Guard
intercepted the last shipment on our submarine. We only lost 10,000 kilos. This will
not interfere with our profit margin. The U.S. Economy is supports our business model
very well!! Jorge
Status(1)=1
GmtOffset(4)=-300
Name(12)=Valio Jorge
#4
Type(1)=0
Source(1)=1
Folder(1)=1
SMSC(12)=+12063130055
Number(12)=+14782279373
Date(6)=150826
Time(6)=103400
Body(65)=Señor El Chapo, We are preparing the weapons for your escape.
Status(1)=1
GmtOffset(4)=-300
Name(12)=Valio Jorge
```

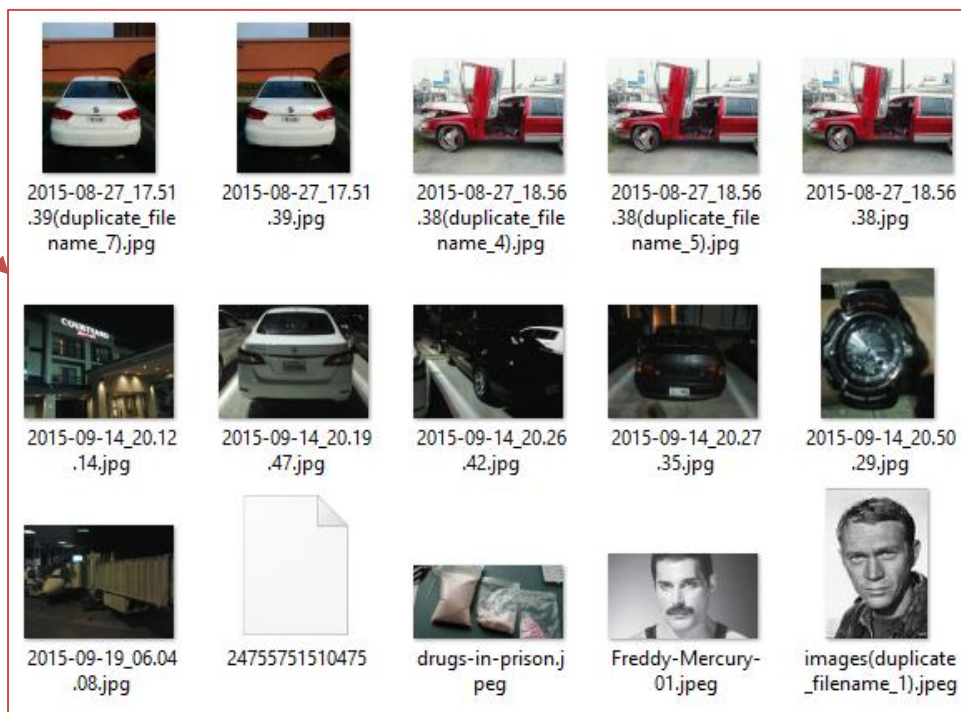
# Mobile Forensics: acquisizione

## *Logical Extraction*

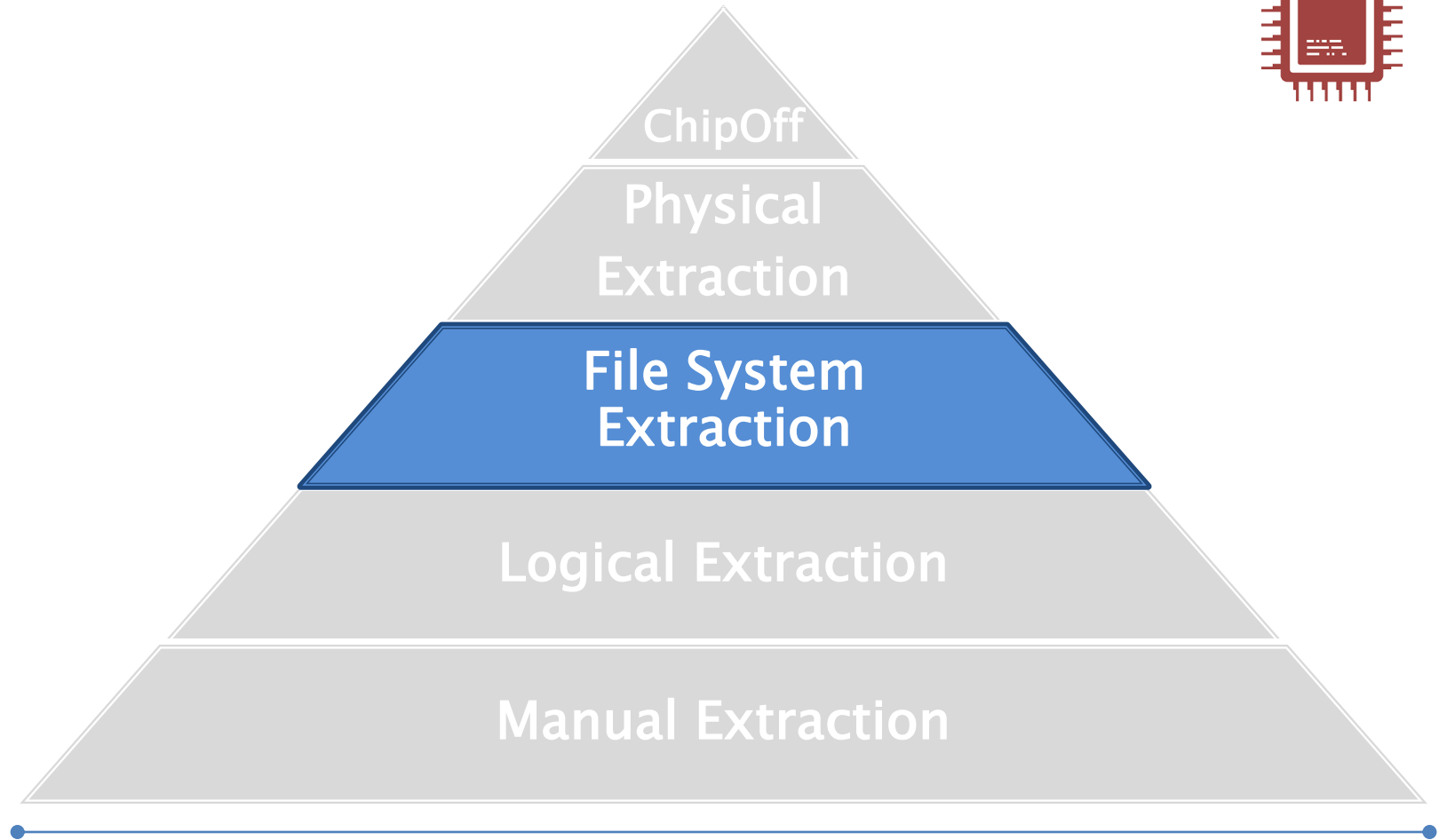
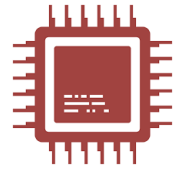


- Attachments
- Audio
- Images
- Ringtones

- Backup 2016\_05\_20 (001).cal
- Backup 2016\_05\_20 (001).clog
- Backup 2016\_05\_20 (001).MMS
- Backup 2016\_05\_20 (001).PBB
- Backup 2016\_05\_20 (001).SMS
- PA Logical.ufd
- Report.html
- Report.xml
- Report\_AudioSection.html
- Report\_CalendarSection.html
- Report\_CallLogsSection.html
- Report\_ContactsSection.html
- Report\_DatabasesSection.html
- Report\_ImagesSection.html
- Report\_MMSSection.html
- Report\_RingtonesSection.html
- Report\_SMSSection.html
- Report\_VideoSection.html



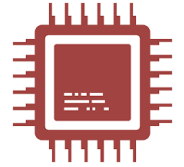
# Mobile Forensics: acquisizione



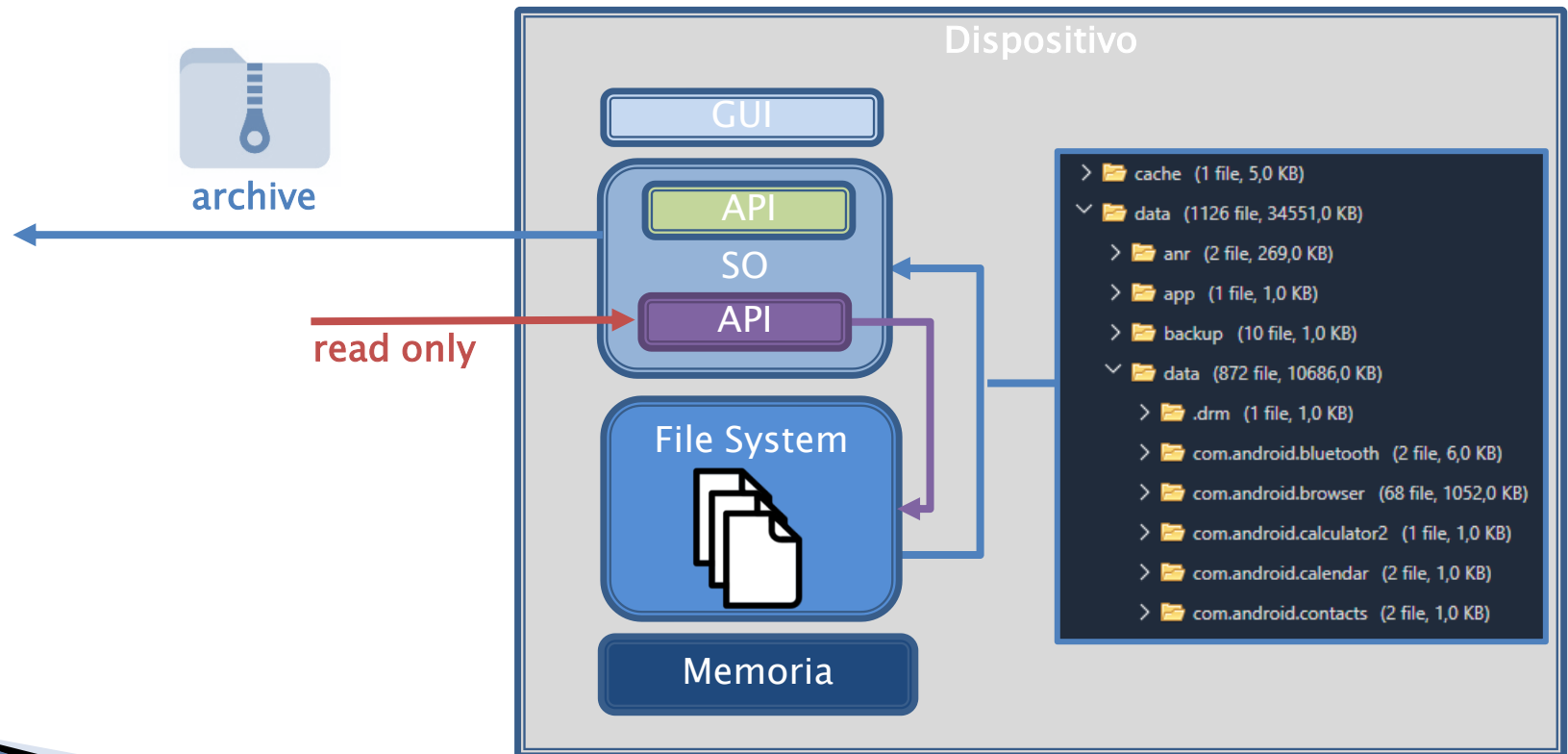
*Nr. di dispositivi supportati*

# Mobile Forensics: acquisizione

## *File System Extraction*



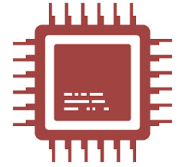
- Estrazione dei file tramite API del dispositivo





# Mobile Forensics: acquisizione

## *File System Extraction*



### ► Risultato:

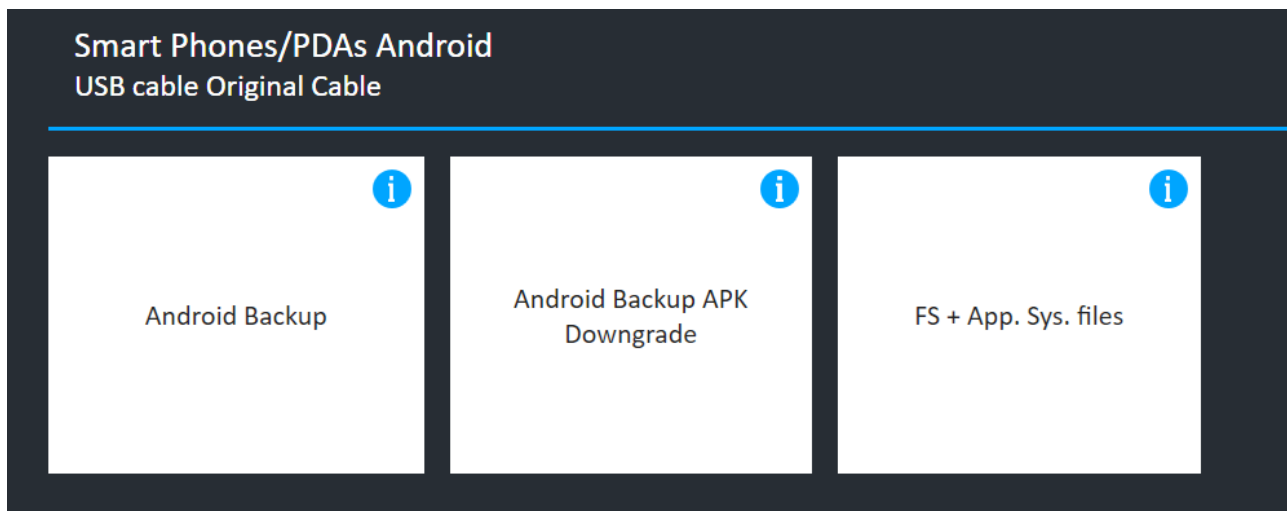
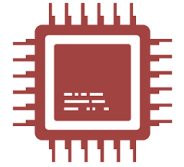
- L'output va processato per visualizzare i dati contenuti:
  - I dati sono contenuti in DB SQLite
  - Possibilità di visualizzare dati cancellati (entry dei DB)

### ► Limiti:

- I risultati dipendono dai permessi con cui vengono fatte le richieste:
  - File System Completo: tutta la struttura della live partition.
  - File System Parziale: solo determinate porzioni

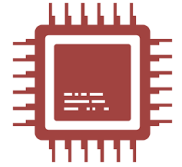
# Mobile Forensics: acquisizione

## *File System Extraction*



# Mobile Forensics: acquisizione

## *File System Extraction*



Smart Phones/PDAs Android  
USB cable Original Cable

Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device.

### **Android:**

#### **Important:**

Verify that the device's Internet connectivity is disabled (Wi-Fi and mobile data) by entering into Airplane mode.

This method is supported for devices running Android version 4.1 and above and with Developer options enabled.

To enable the Developer options, go to Menu → Settings → About (information) → tap the "Build number" 7 times until it's enabled.

Under Developer options → enable the Android/USB debugging and Stay awake (if available).

#### **Notice:**

After pressing "Continue" the extraction will start automatically, DO NOT press anything.

If the extraction does not start you will be prompted to select "Back up my data" on the device.

#### **Note:**

On some devices the "Back up my data" button may be disabled.

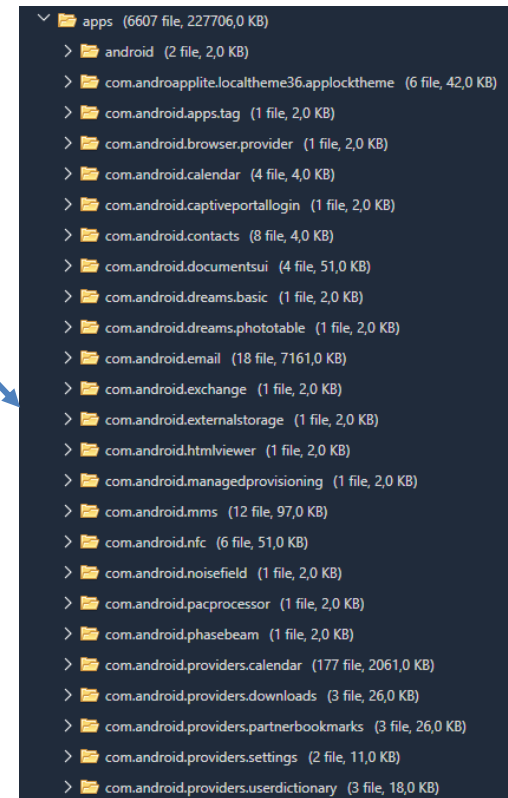
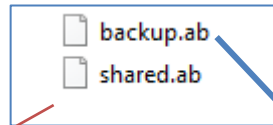
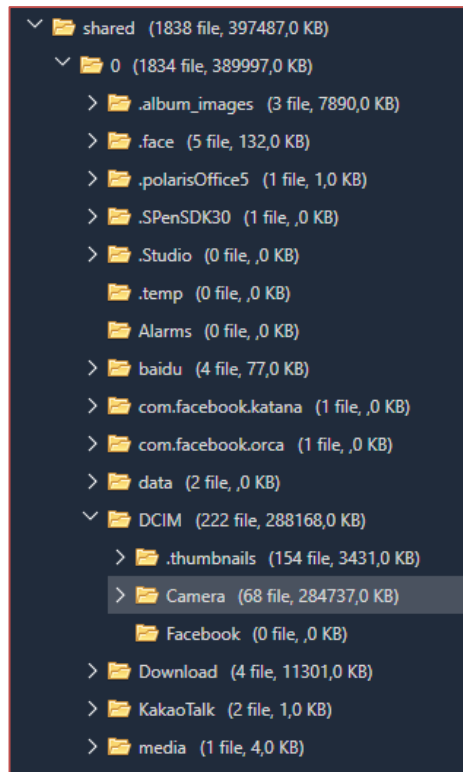
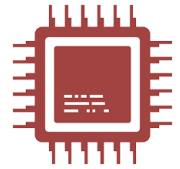
To enable it, enter a password and then press the "Back up my data" button.

To decode the extraction, this password will also be required in Physical Analyzer.

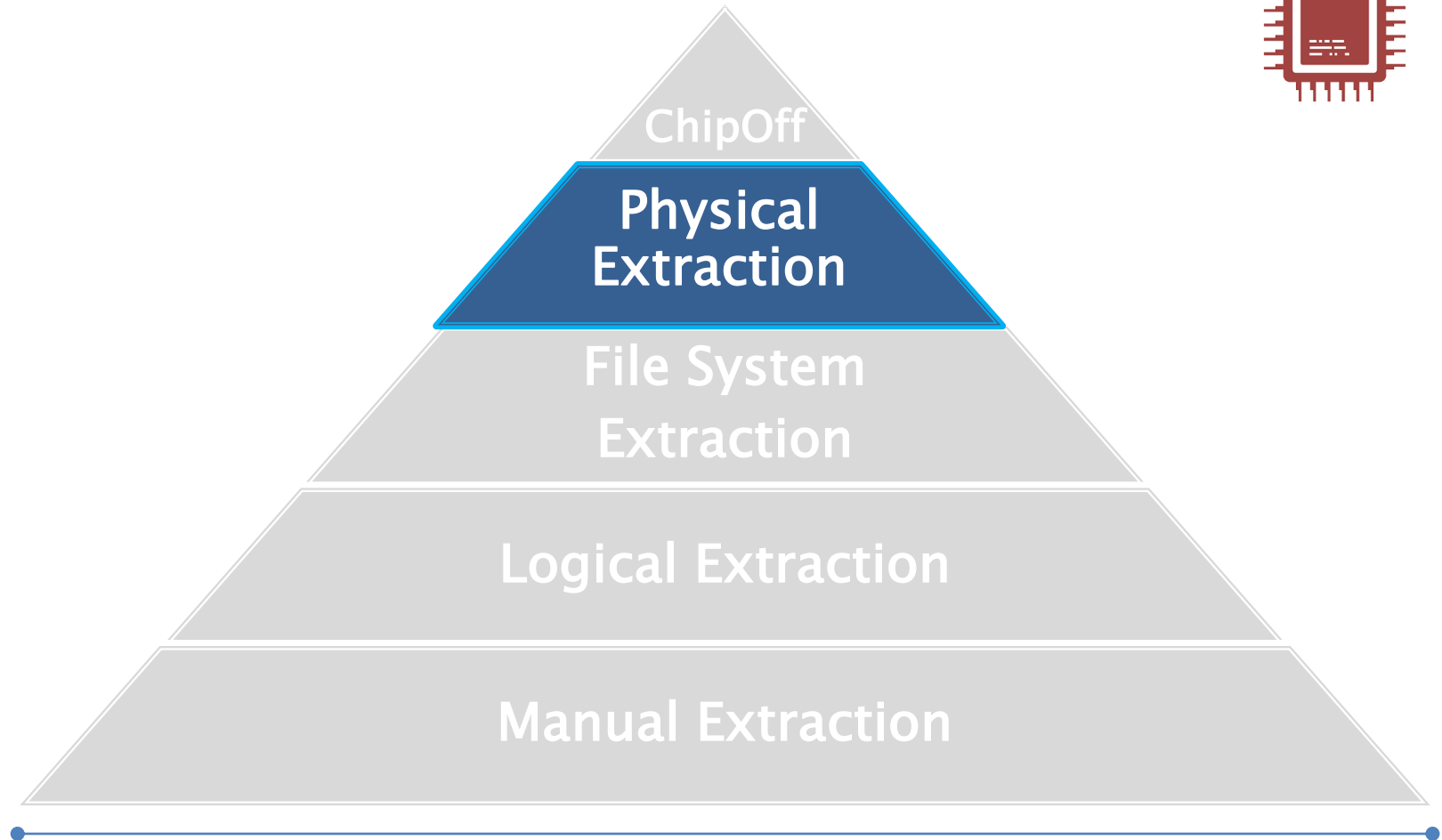
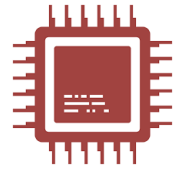
On some devices, the "Back up my data" button is not clearly visible, and you may need to press the bottom-right corner of the device's screen to continue.

# Mobile Forensics: acquisizione

## *File System Extraction*



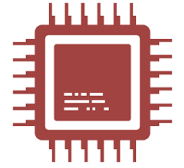
# Mobile Forensics: acquisizione



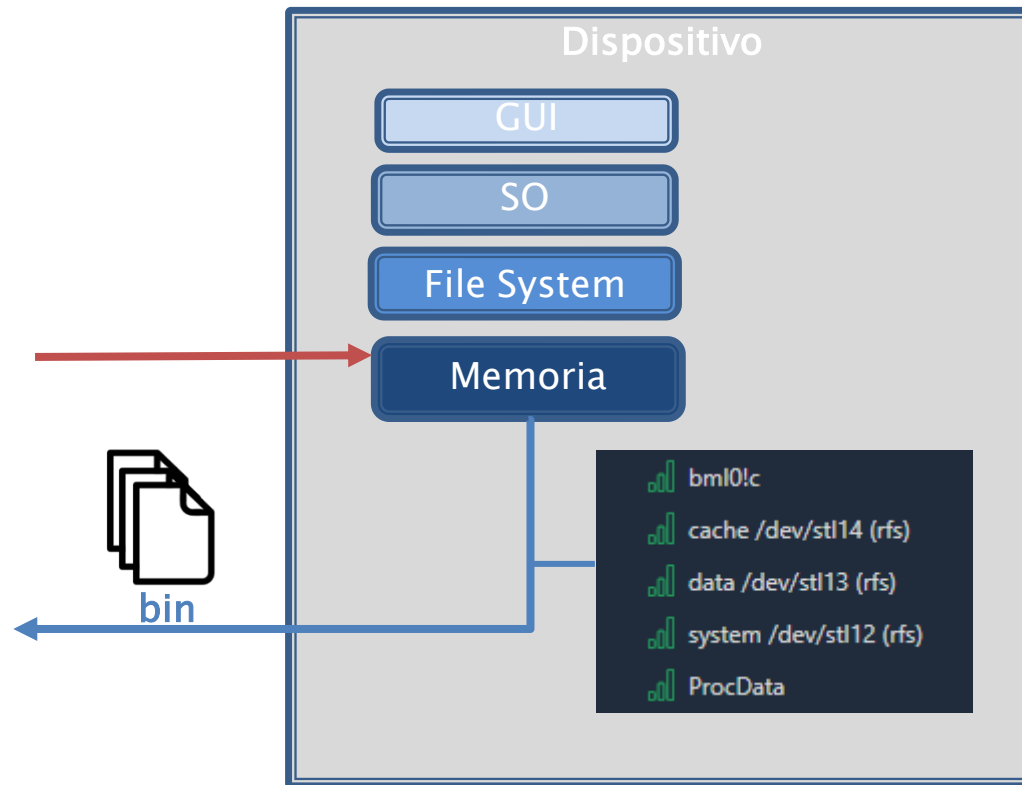
*Nr. di dispositivi supportati*

# Mobile Forensics: acquisizione

## *Physical Extraction*

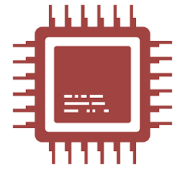


- Copia bit-a-bit della memoria del dispositivo

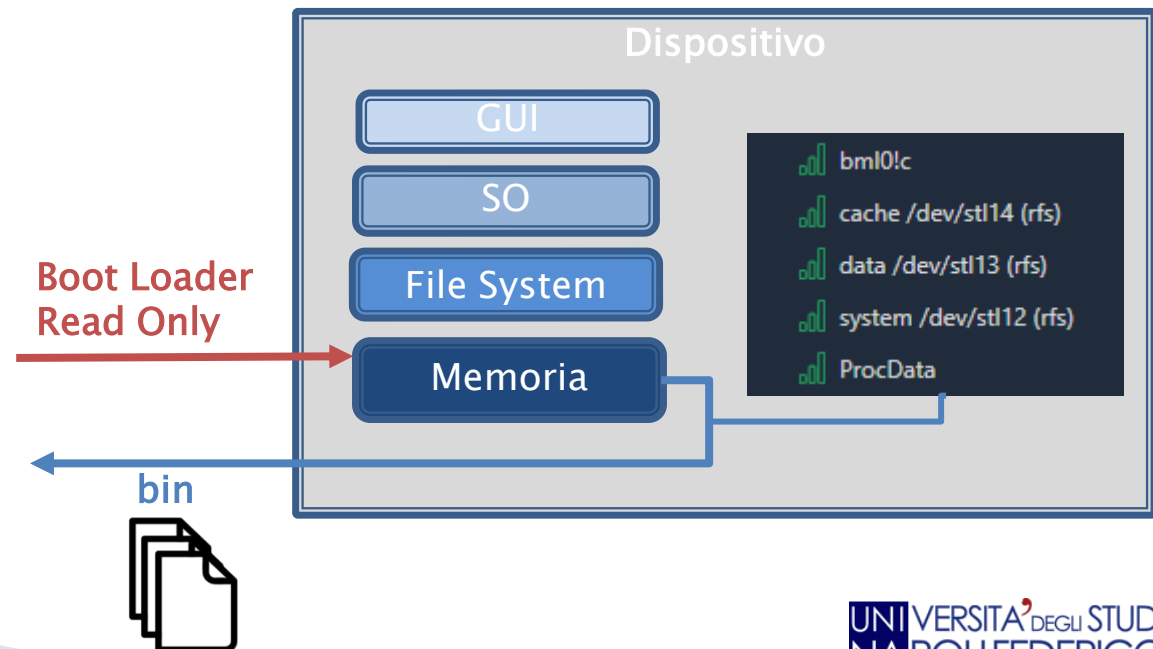


# Mobile Forensics: acquisizione

## *Physical Extraction*

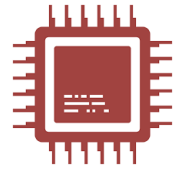


- ▶ Copia bit-a-bit della memoria del dispositivo:
  - **Boot loader:** codice immesso nella fase di avvio del dispositivo per avviare l'estrazione dati
    - Bug del firmware\Chipset

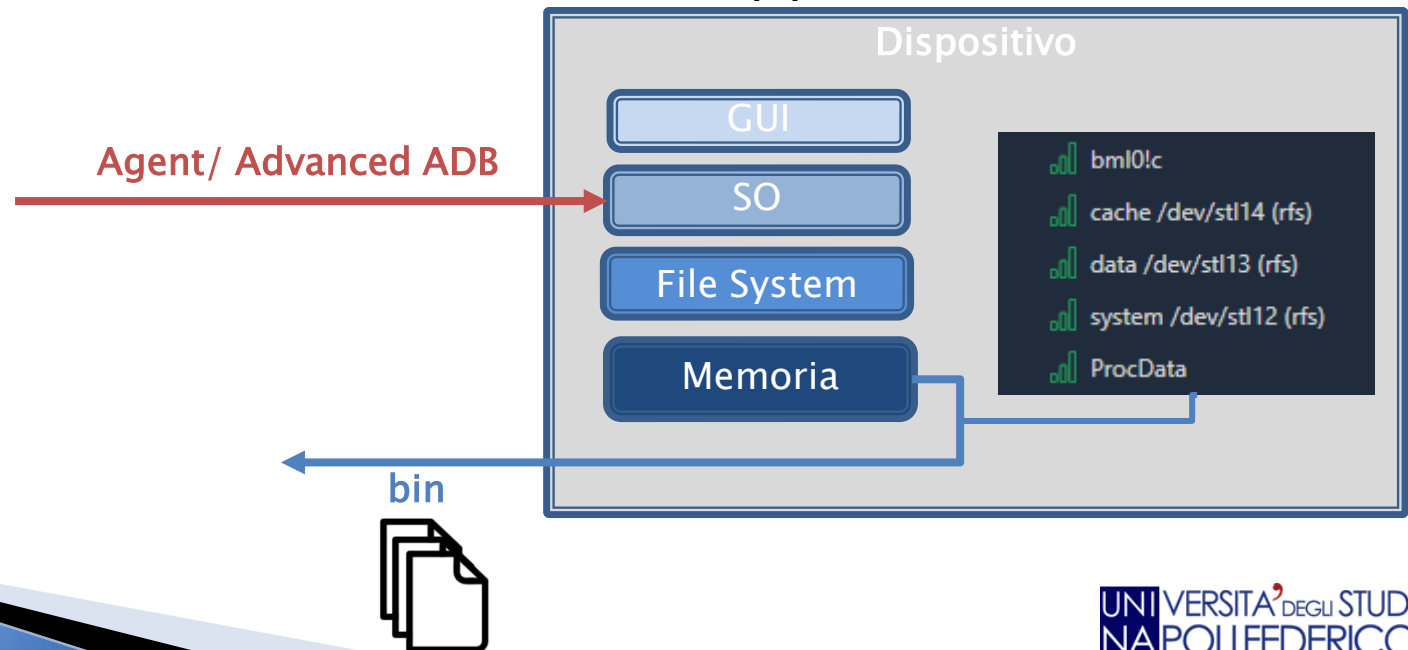


# Mobile Forensics: acquisizione

## *Physical Extraction*



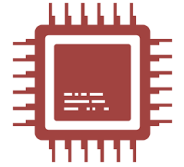
- ▶ Copia bit-a-bit della memoria del dispositivo:
  - **Agent:** tool installato nel S.O.
    - Bug nel S.O.
  - **Advanced ADB** (*Android Debug Bridge*):
    - Bug nel S.O. (Android  $\leq 7.1$  & security patch  $\leq 11/2016$ )





# Mobile Forensics: acquisizione

## *Physical Extraction*



### ► Risultato:

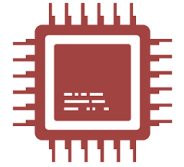
- L'output va processato per visualizzare i dati contenuti
- Recupero di file cancellati (carving)








### ► Limiti:

- Produttore del dispositivo
- Chipset
- Versione del S.O.
- Patch di sicurezza

# Mobile Forensics: acquisizione

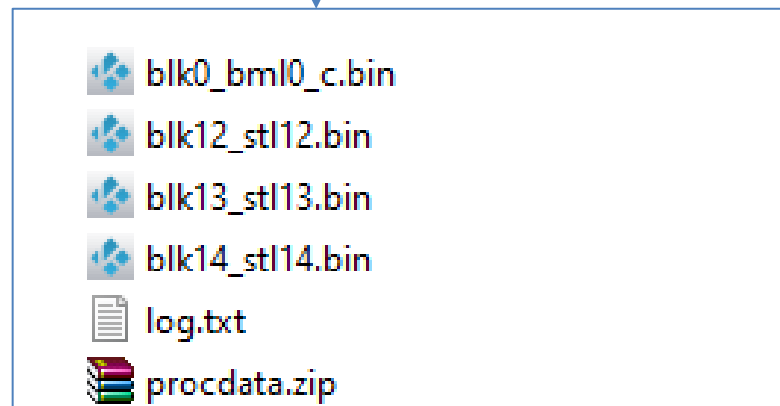
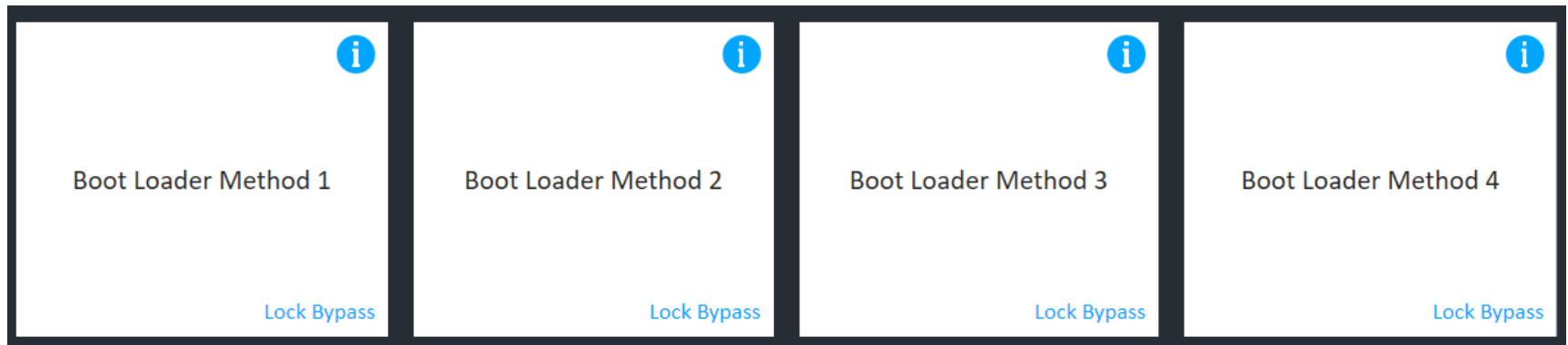
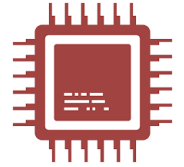
## *Physical Extraction*



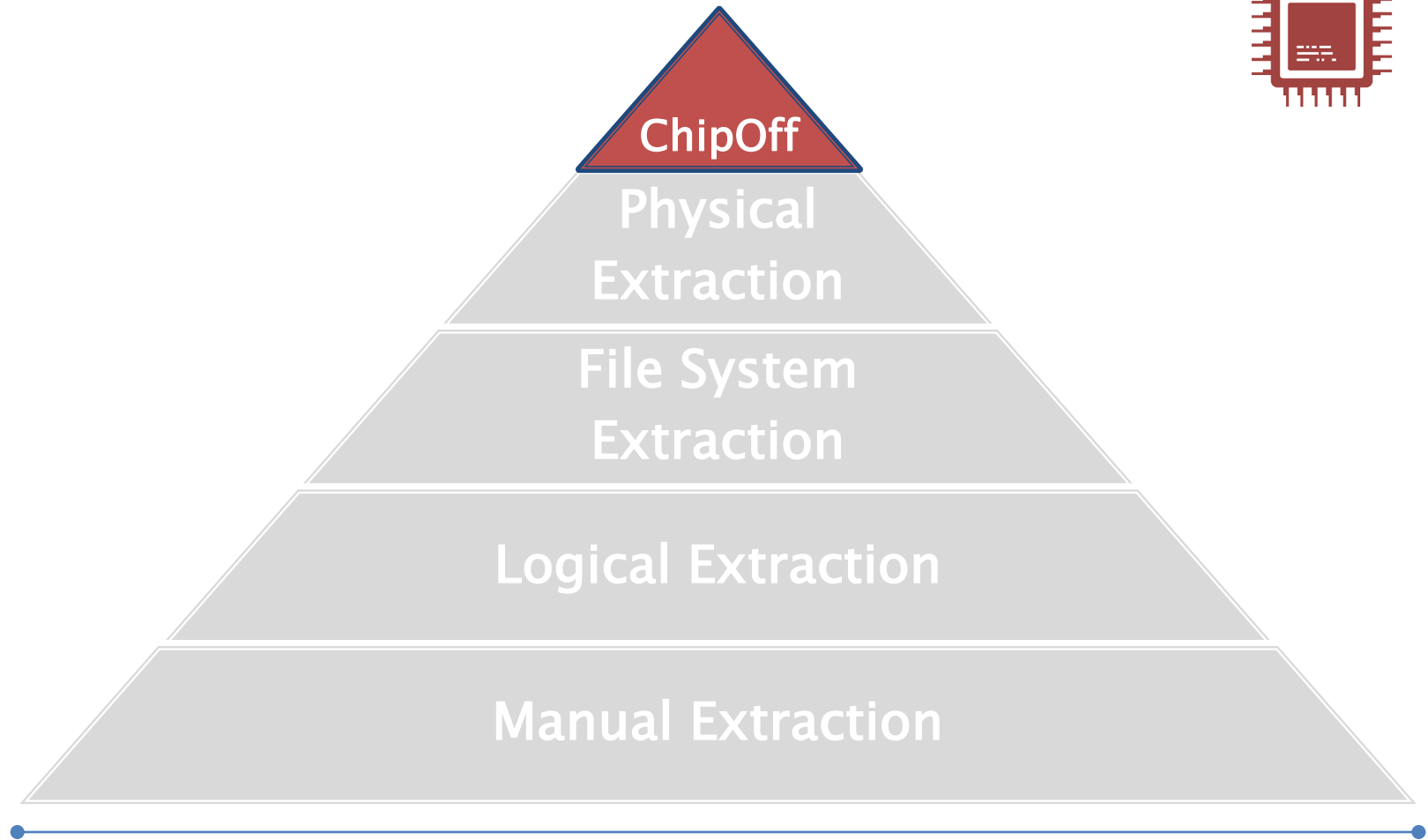
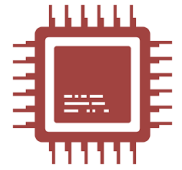
All	Vendors	Generic profiles	Recently used
Android 	Qualcomm 	Decrypting Qualcomm 	MTK 
Decrypting MTK 	Decrypting LG MTK 	MTK Live 	Android Bluetooth 

# Mobile Forensics: acquisizione

## *Physical Extraction*



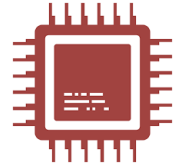
# Mobile Forensics: acquisizione



*Nr. di dispositivi supportati*

# Mobile Forensics: acquisizione

## *Chip Off*



- ▶ Estrazione fisica del chip dalla scheda madre
  - Distruzione del dispositivo
- ▶ Limiti:
  - Dispositivo cifrato

# Mobile Forensics

»» Analisi



# Mobile Forensics: analisi *i sistemi operativi*

## ▶ O.S. Android:

- Migliaia di produttori e modelli
- Kernel linux: OpenSource
- App

## ▶ Apple iOS:

- Pochi modelli
- Closed
- App

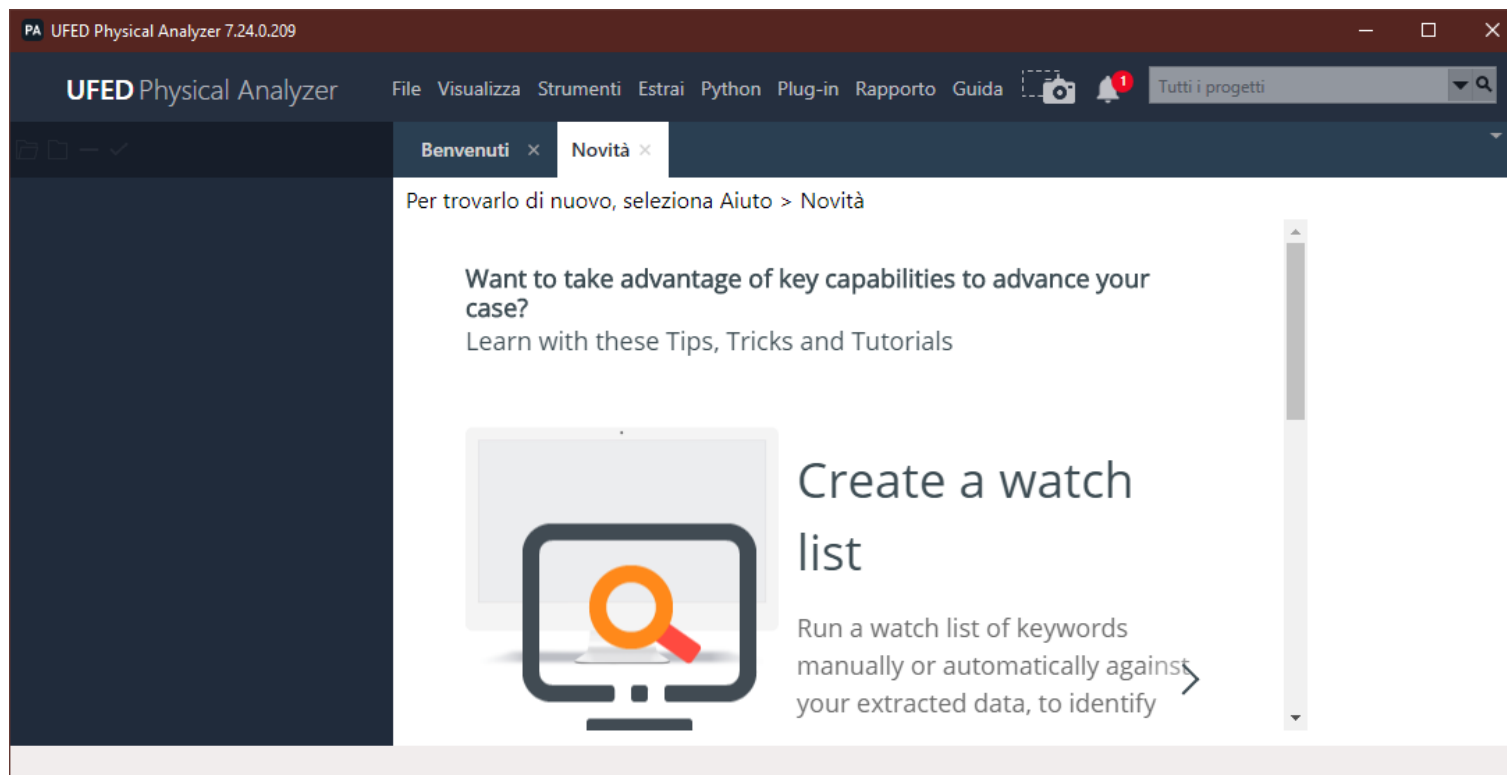
# Mobile Forensics: analisi *App*

- ▶ Estendono la funzionalità del S.O.
- ▶ Rappresentano le principali interazioni con l'utente:
  - Produzione di dati
- ▶ Hanno un proprio dominio



# Mobile Forensics: analisi *Strumenti*

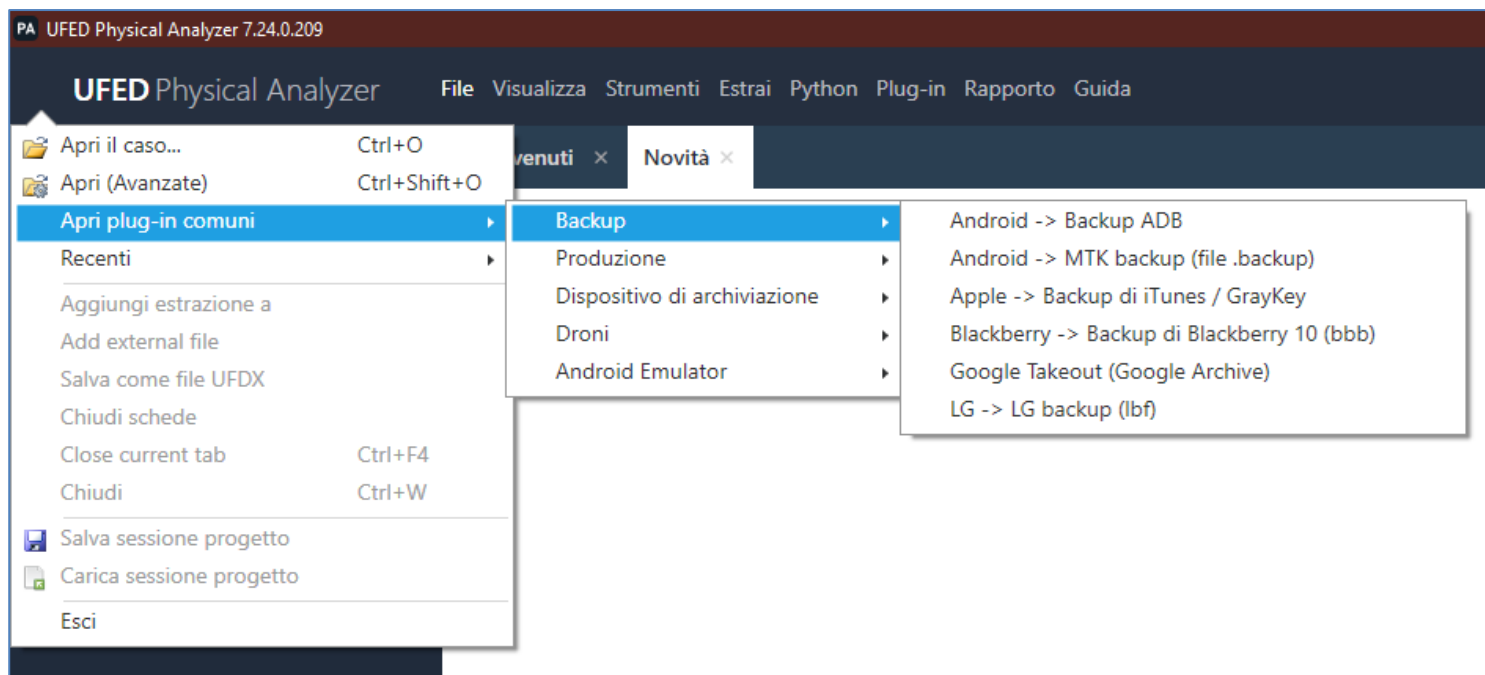
## ► UFED Physical Analyzer



# Mobile Forensics: analisi

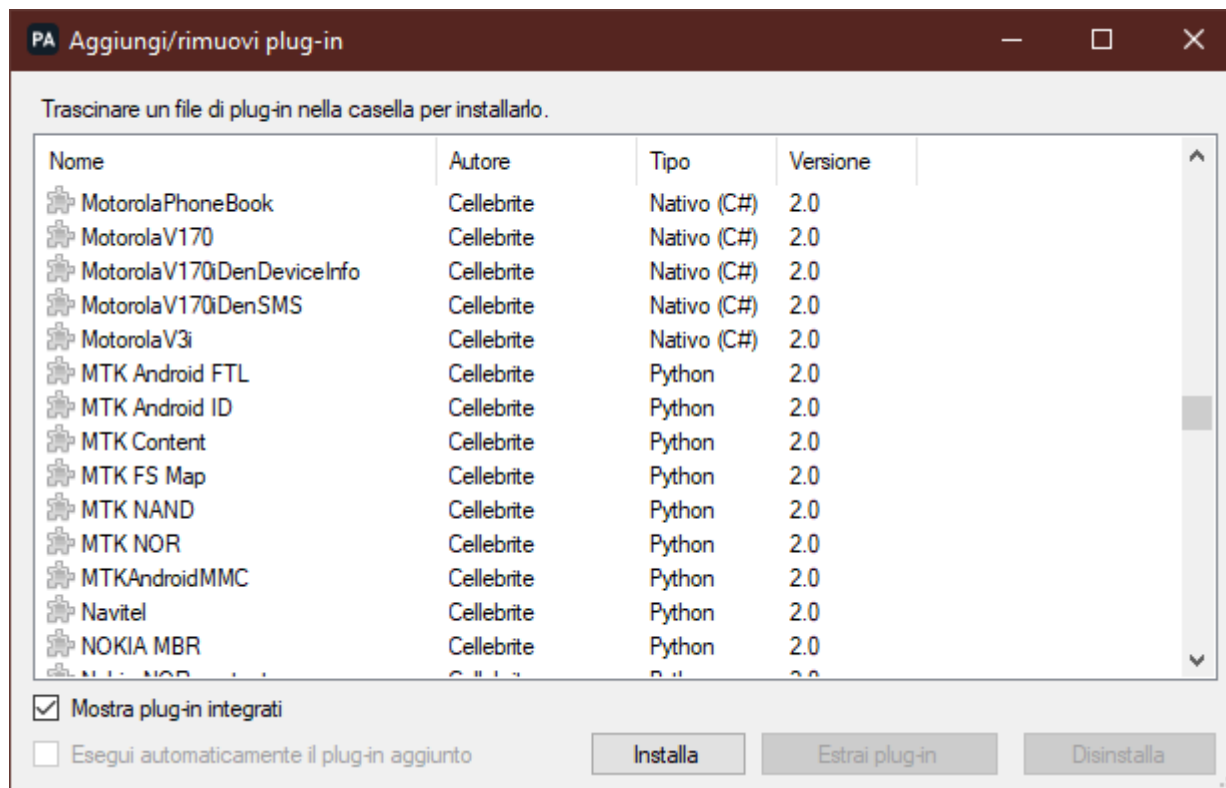
## *Strumenti*

### ► Analisi di backup

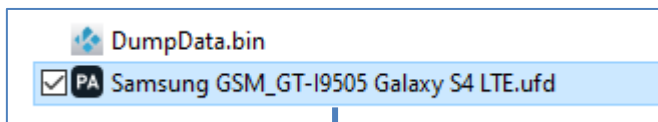


# Mobile Forensics: analisi *plugin*

## ► Modulare: plugin



# Mobile Forensics: analisi *plugin*

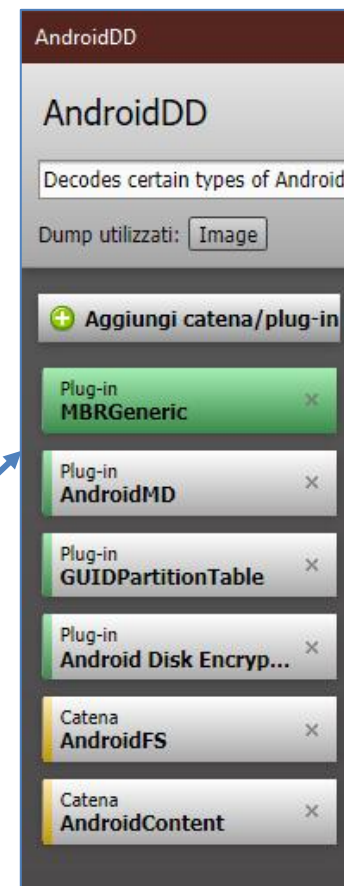


```
[Dumps]
Image=DumpData.bin

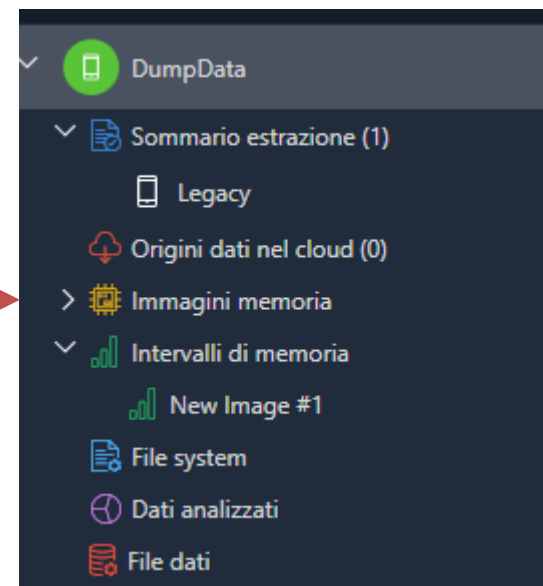
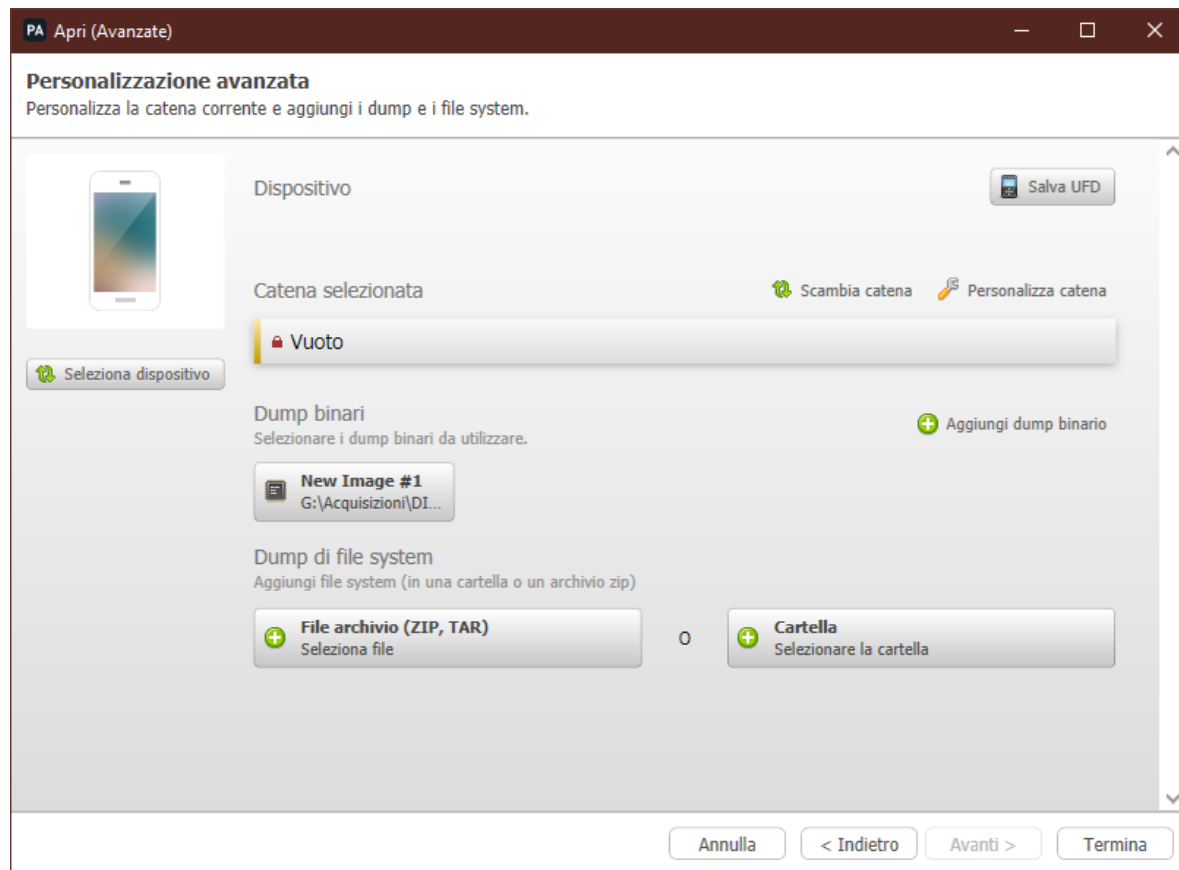
[ExtractionStatus]
ExtractionStatus=Success

[General]
ConnectionType=Cable No. 133
Date=11/09/2018 14:01:24 (+2)
Device=SAMI9505
EndTime=11/09/2018 15:40:29 (+2)
ExtractionType=Physical
FullName=GT-I9505 Galaxy S4 LTE
GUID=6A3819DD-09DE-45BF-AF29-0F2A324A6BD5
InternalBuild=4.7.7.845
MachineName=NB-SEAMAN85
Model=GT-I9505 Galaxy S4 LTE
UfdVer=1.2
UnitId=1482376414
UserName=
Vendor=Samsung GSM
Version=7.5.0.845

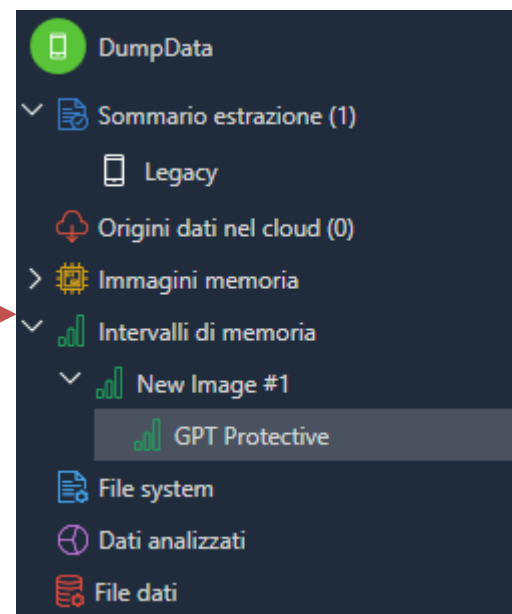
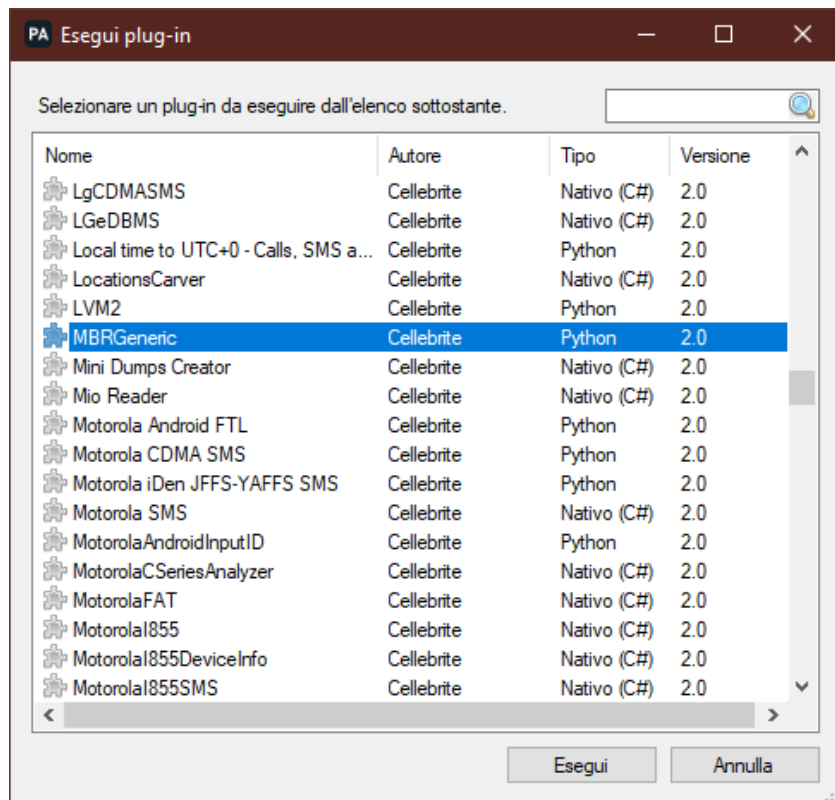
[Image]
ExtractionMethod=SAMSUNG_ODIN
```



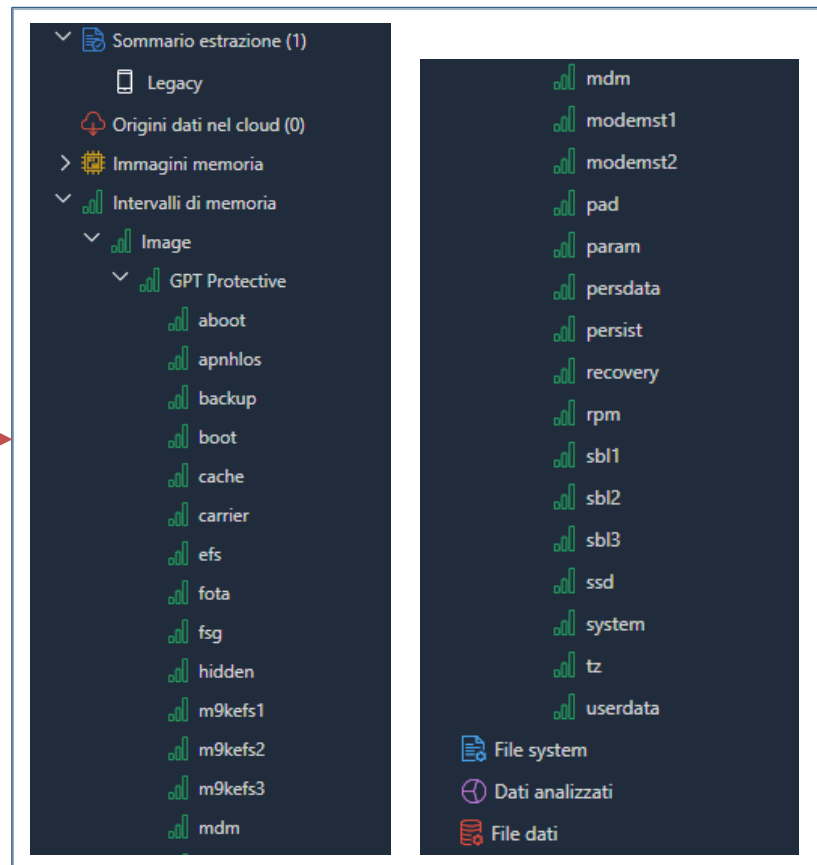
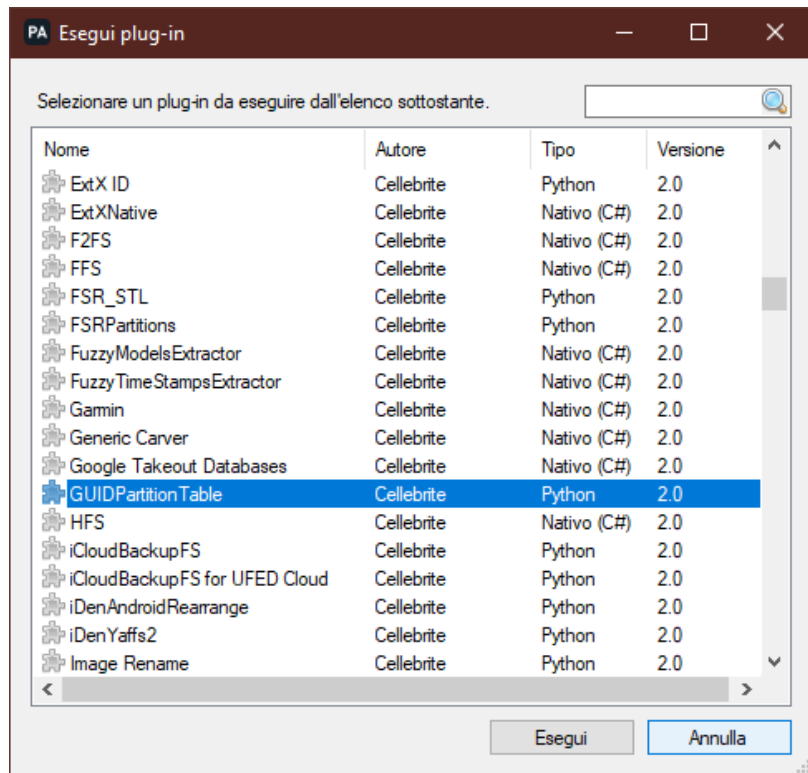
# Mobile Forensics: analisi *plugin*



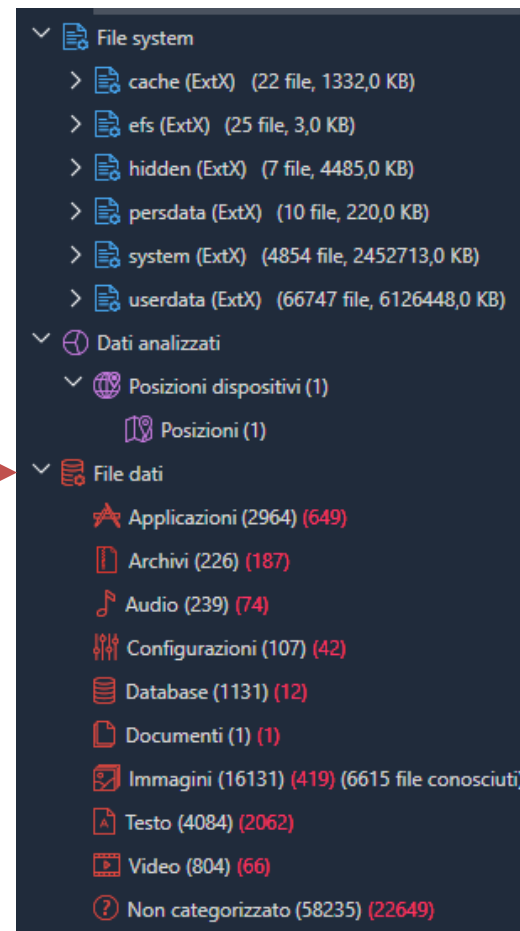
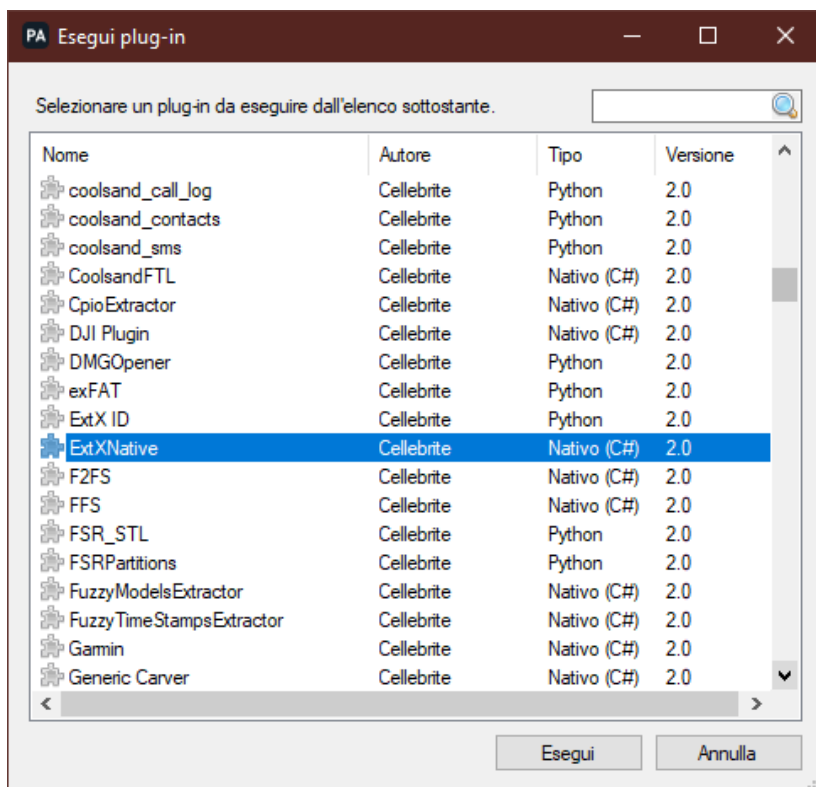
# Mobile Forensics: analisi *plugin*



# Mobile Forensics: analisi *plugin*

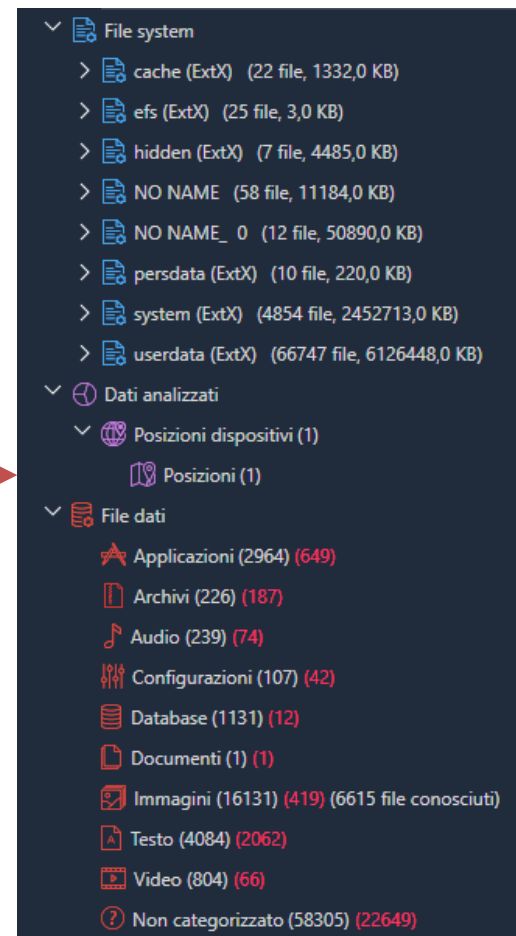
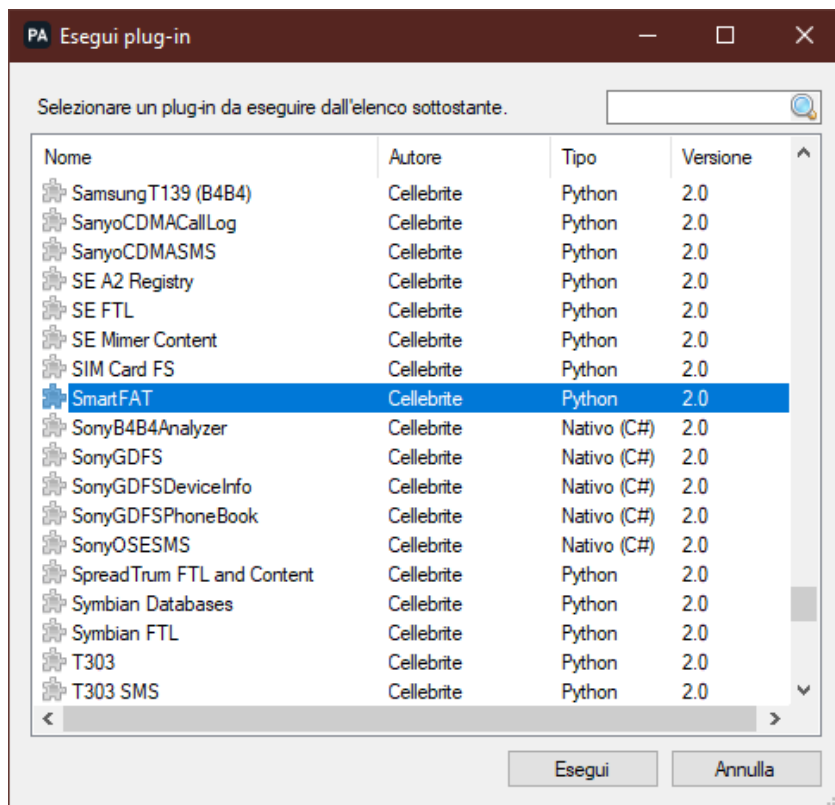


# Mobile Forensics: analisi *plugin*

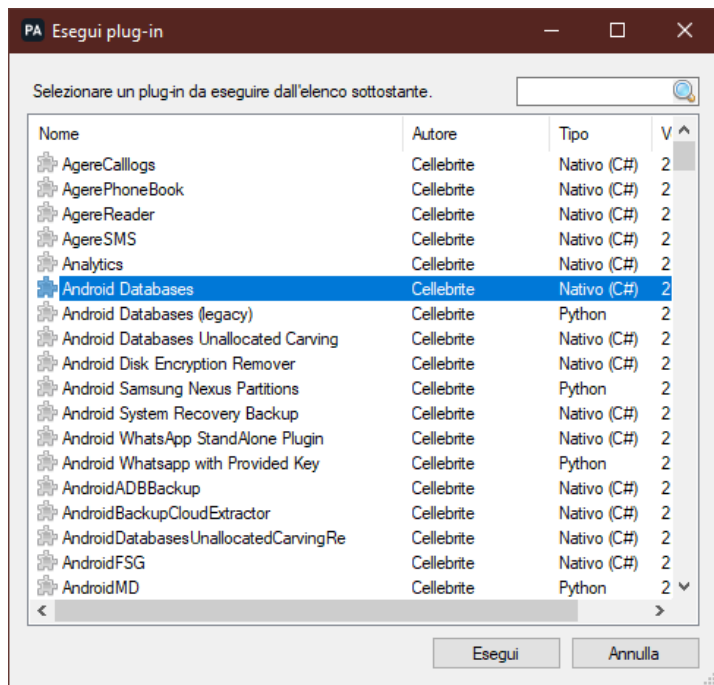




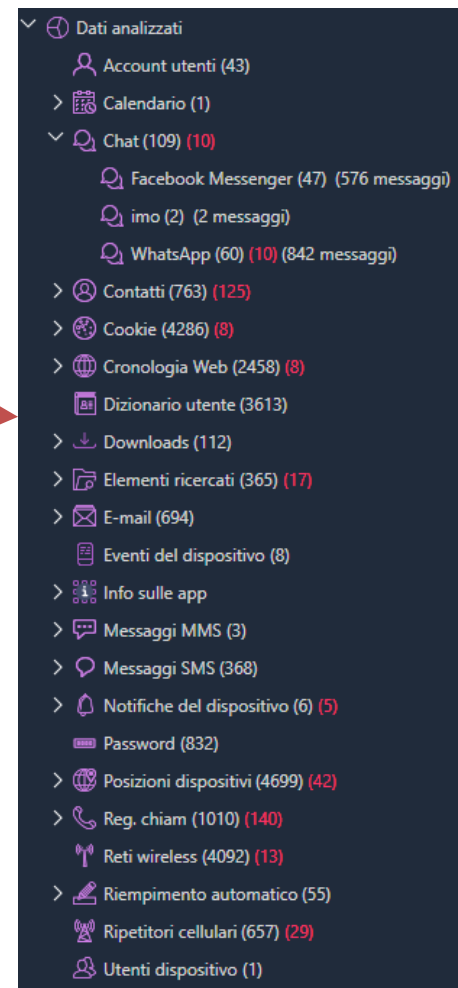
# Mobile Forensics: analisi *plugin*



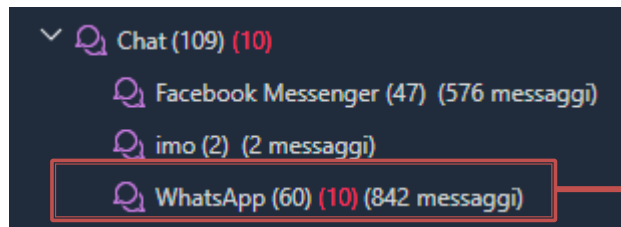
# Mobile Forensics: analisi *plugin*



04:16 Running plugin Android Databases (debug=False)  
04:16 Parsing GooglePlay  
04:16 Parsing Permissions  
04:16 Parsing App Usage  
04:16 Parsing App Usage  
04:16 Parsing AndroidID  
04:16 Parsing Build Prop  
04:16 Parsing Keystore  
04:16 Parsing ChatOn\_3.5.839  
04:16 Parsing Calendar  
04:16 Parsing providers\_settings  
04:16 Parsing S Note  
04:16 Parsing Google+\_6.5.0.104456905  
04:16 Parsing DropBox\_102.2.2  
04:16 Parsing AnalyzeMedia  
04:16 Parsing WiFi  
04:16 Parsing WiFi\_12.8.74 (020308-204998136)  
04:16 Parsing Accounts



# Mobile Forensics: analisi *plugin*



#							Partecipanti	↓ Ora inizio	Ultima attività
40					4	2	491725...@s.whatsapp.net 491521...@s.whatsapp.net Habib... (proprietario)	19/11/2016 20:04(UTC+0)	19/11/2016 22:11(UTC+0)
41					7	1	491521...@s.whatsapp.net Habib... (proprietario)	06/09/2016 21:41(UTC+0)	21/11/2016 23:57(UTC+0)
42			5		8	2	4915739...@s.whatsapp.net 4915210...@s.whatsapp.net kanistafa... (proprietario) Habib... (proprietario)	28/08/2016 17:19(UTC+0)	14/10/2016 19:20(UTC+0)
43			16		28	2	491573...@s.whatsapp.net 4915210...@s.whatsapp.net Habib... (proprietario)	24/08/2016 18:19(UTC+0)	27/12/2016 22:22(UTC+0)
44			46		49	2	4915214...@s.whatsapp.net 4915210...@s.whatsapp.net +491521... Habib... (proprietario)	22/08/2016 16:11(UTC+0)	04/10/2017 20:29(UTC+0)
45					6	1	4915210...@s.whatsapp.net ... (proprietario)	12/08/2016 11:24(UTC+0)	15/08/2016 16:49(UTC+0)
46			2		9	2	447481...@s.whatsapp.net 491521...@s.whatsapp.net Rafi... Habib... (proprietario)	10/08/2016 07:44(UTC+0)	23/05/2017 19:39(UTC+0)
47					27	2	4915788...@s.whatsapp.net 4915210...@s.whatsapp.net Queen... Habib... (proprietario)	08/08/2016 12:10(UTC+0)	15/08/2016 16:52(UTC+0)

# Mobile Forensics: analisi *plugin*

Numero righe	↑ Nome ▼
1	_jobqueue-WhatsAppJo...
1948	axolotl.db
6	chatsettings.db
0	chatsettingsbackup.db
3	Cookies
7713	emojidictionary.db
1	google_app_measureme...
1	hsmpacks.db
1	location.db
2	media.db
1206	msgstore.db
399	wa.db
3	Web Data
0	web_sessions.db



## SSRI Lorenzo Laurato s.r.l.



Via Coroglio nr. 57/D (BIC- Città della Scienza)  
80124 Napoli



Tel. 081.19804755

Fax 081.19576037



lorenzo.laurato@unina.it

lorenzo.laurato@ssrilab.com



[www.docenti.unina.it/lorenzo.laurato](http://www.docenti.unina.it/lorenzo.laurato)

[www.computerforensicsunina.forumcommunity.net](http://www.computerforensicsunina.forumcommunity.net)