



DIGITAL CRIME SCENE INVESTIGATION

Tecniche avanzate di Mobile Forensics

Fabio Massa – Cyber Crime Investigator



DIGITAL CRIME SCENE INVESTIGATION

01 VALUTAZIONE

Valutazione primaria delle potenziali sorgenti informative

02 METODOLOGIA

Pianificazione delle metodologie investigative, valutazione pratica dell'efficacia

03 ACQUISIZIONE

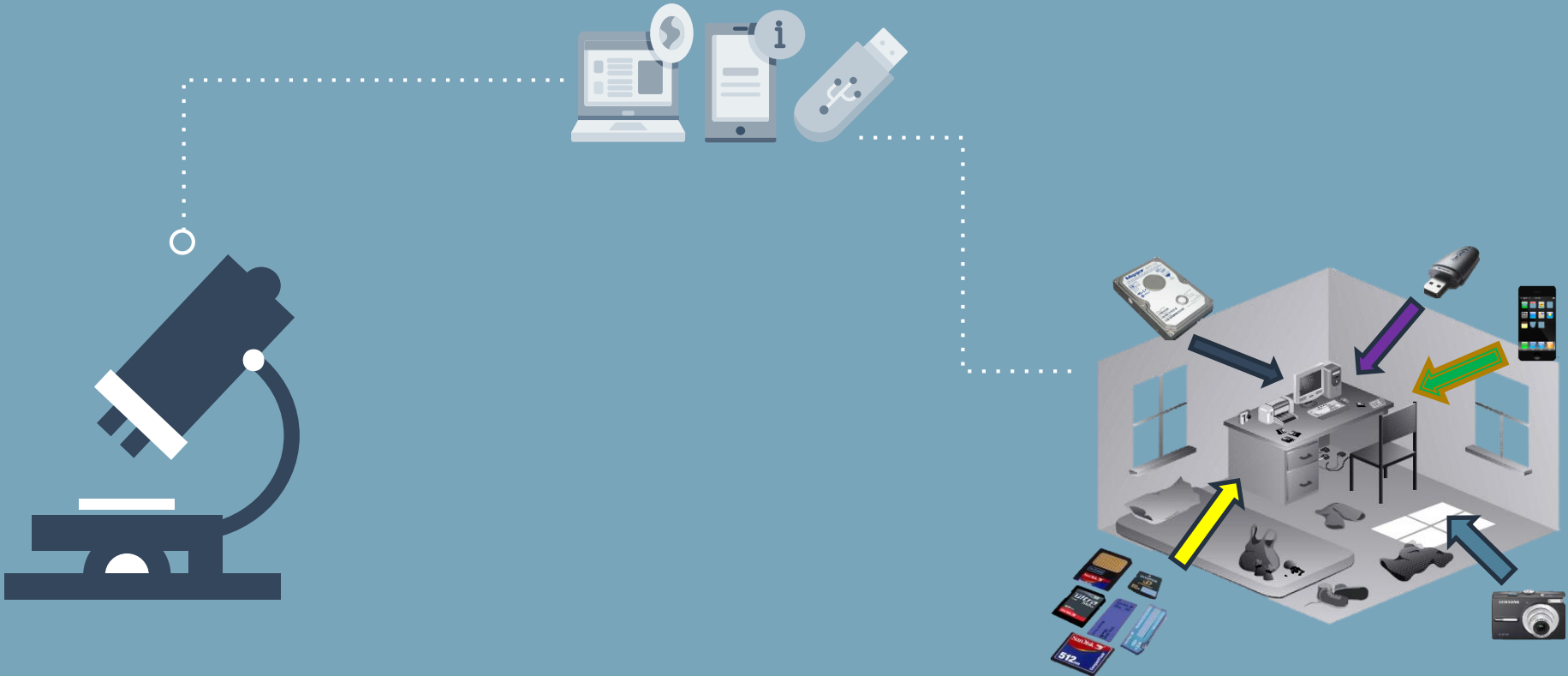
Applicazione delle tecniche investigative digitali pianificate

04 ANALISI

Analisi dei dati acquisiti, linking delle informazioni, ricostruzione digitale dei profili degli offender e delle vittime



LAW ENFORCEMENT FIRST RESPONDER DIGITAL CRIME SCENE



PHYSICAL EVIDENCE VS DIGITAL EVIDENCE

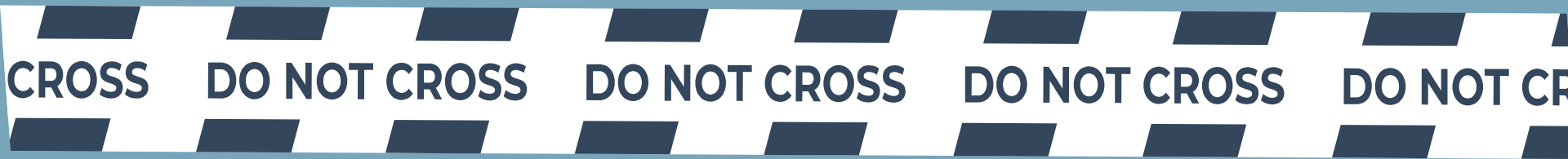


BEST PRACTICES

Acquisire le prove, senza alterare il sistema informatico in cui si trovano.

Garantire che le prove siano identiche a quelle originali.

Analizzare i dati senza che essi ne risultino alterati.



DIGITAL EVIDENCE

Una caratteristica fondamentale delle tracce digitali è l'**immaterialità**; non esistono come oggetto fisico ma sono **sequenze di bit** memorizzate su **dispositivi di archiviazione dati**. Per accedere ad una traccia occorre dunque accedere al dispositivo su cui essa è memorizzata. I dispositivi di memorizzazione sono di due tipi:

Persistenti: non necessitano di alimentazione per mantenere i dati memorizzati (Pen Drive USB, Hard Disk, schede di memoria ecc.).

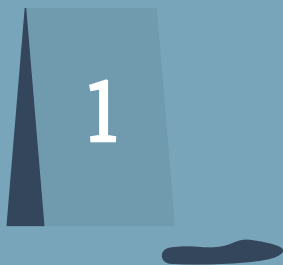
Volatili: interrotta l'alimentazione, i dati vengono persi (memoria RAM, ecc.).

CROSS DO NOT CROSS DO NOT CROSS DO NOT CROSS DO NOT CR

ON SITE INVESTIGATIONS

IDENTIFICAZIONE

Identificazione dei dispositivi e delle digital evidence da acquisire o repertare



PRESERVAZIONE

Esecuzione di tutte le possibili precauzioni per garantire l'integrità dei dati e dei dispositivi da repertare o acquisire



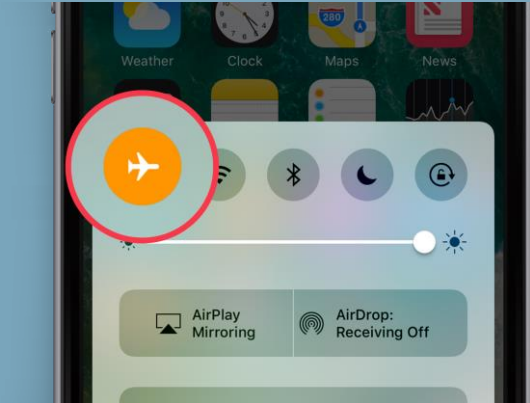
REPERTAMENTO O ACQUISIZIONE

Repertamento o acquisizione live dei dispositivi digitali di interesse investigativo



ON SITE INVESTIGATIONS

PRESERVAZIONE



MOBILE FORENSICS

ACQUISIZIONE

L'acquisizione è il processo di clonazione o copia delle prove di dati digitali da dispositivi mobili.

Il processo di acquisizione di supporti digitali e di ottenere informazioni da un dispositivo mobile e dai supporti associati è noto con precisione come "imaging".

L'immagine della prova può essere memorizzata in diversi formati che possono essere utilizzati per ulteriori analisi. Viene generato un valore hash per assicurarsi che l'immagine non venga alterata in un dato momento.



MOBILE FORENSICS

ACQUISIZIONE

L'imaging può essere eseguito con l'aiuto di diversi strumenti come Cellebrite 4PC, Cellebrite physical Analyzer, Oxygen Forensic Detective, Msab XRY, Magnet Axion, Belkasoft Evidence Center, Accessdata FTK Imager ecc.



CROSS

DO NOT CROSS

DO NOT CROSS

DO NOT CROSS

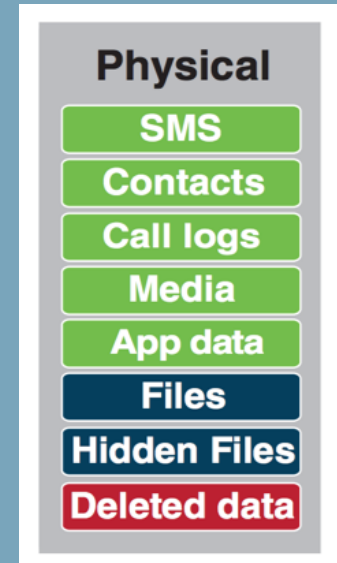
DO NOT CROSS

MOBILE FORENSICS

ACQUISIZIONE

Esistono vari metodi che possono essere utilizzati per l'estrazione dei dati dai dispositivi mobili e sono i seguenti:

1) Physical Acquisition:

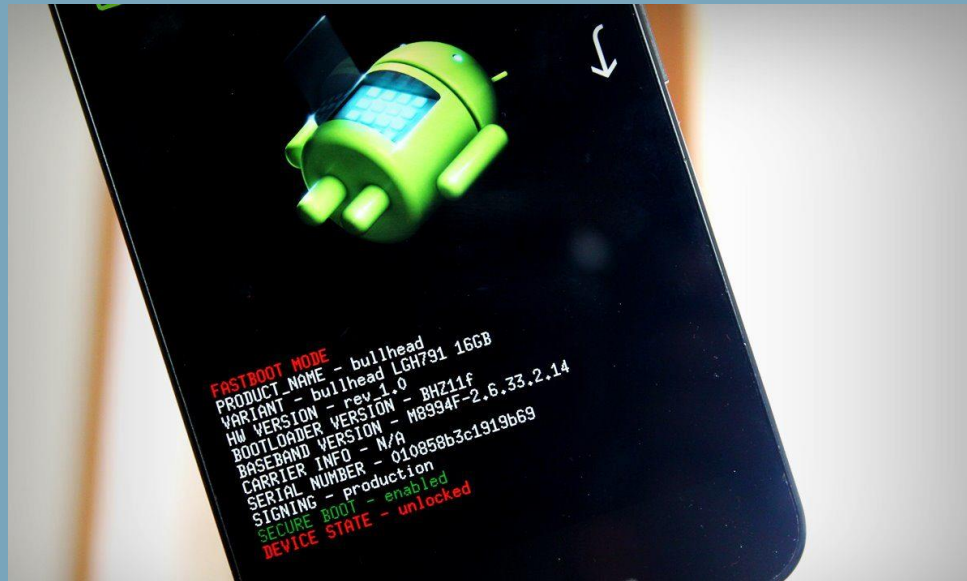


MOBILE FORENSICS

ACQUISIZIONE

Bootloader:

Il bootloader è un programma che, ogni qualvolta accendiamo un dispositivo, entra in azione ed esegue le giuste routine per avviare il sistema operativo.



MOBILE FORENSICS

ACQUISIZIONE

Root Android:

Rootare lo smartphone, ottenere i permessi di root, diventare Superuser: ma di cosa stiamo parlando?



MOBILE FORENSICS

ACQUISIZIONE

USB DEBUG:

Android version	Steps
V 5.0 and Above	1. Goto Settings > About Phone > Build number > Tap it 7 times to become developer;
	2. Again go to Settings > Developer Options > Check and allow USB Debugging.
V 4.2,4.3 and 4.4	1. Goto Settings > About Phone > Build number > Tap it 4-5 times to become developer;
	2. Again go to Settings > Developer Options > Check and allow USB Debugging.
V 3.0 to 4.1	1. Goto Settings > Developer Options > Enable and Allow USB Debugging.
V 2.0 to 2.3	1. Go to Settings > Applications > Development > USB Debugging.

MOBILE FORENSICS

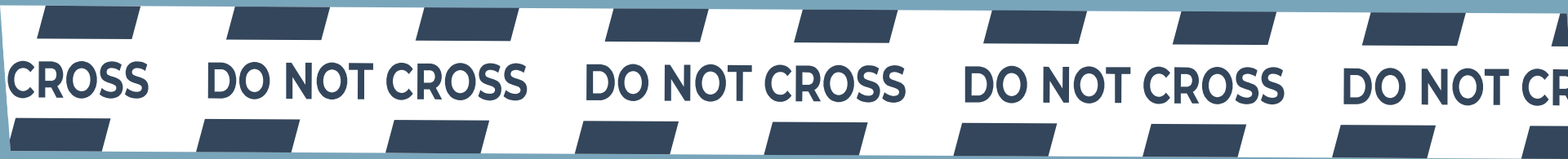
ACQUISIZIONE

Physical Acquisition:

L'acquisizione fisica è suddivisa in due sezioni:

Dumping: Durante questa fase, i dati dalla memoria fisica vengono scaricati in un formato di file esadecimale non elaborato.


Decoding: Durante questa fase, i dati grezzi vengono convertiti in un formato leggibile dall'uomo.






MOBILE FORENSICS

ACQUISIZIONE

Physical Acquisition:



Motorola CDMA MB867 Milestone X2
Cable A with purple tip T-139

<p> ADB</p>	<p> Boot Loader (Recommended) Lock Bypass</p>	<p> Physical Bypassing Lock Lock Bypass</p>
--	---	---

MOBILE FORENSICS

ACQUISIZIONE

Physical Acquisition:



Samsung CDMA SM-G930V Galaxy S7
Cable A with black tip T-100



ADB



Boot Loader (FW Flashing)

Lock Bypass



Boot Loader
(Recommended)

Lock Bypass



Decrypting EDL ADB

MOBILE FORENSICS

ACQUISIZIONE



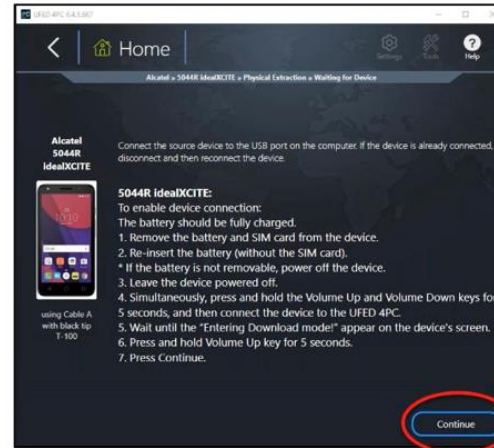
Qualcomm - Emergency Download Mode (EDL)

EDL extraction test – encrypted Alcatel 5044R

After removing the SIM and reinserting the battery, follow the button procedure as instructed. When done correctly, the download screen will appear and then turn black after the final step. Press “Continue” when the button becomes active.



Cellebrite



Utilizzo della modalità EDL. Fonte: webinar su Cellebrite

MOBILE FORENSICS

ACQUISIZIONE



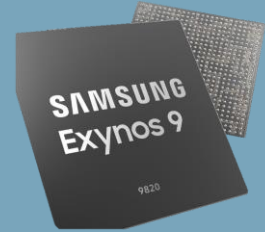
Emergency Download Mode (EDL)

TEST POINT



MOBILE FORENSICS

ACQUISIZIONE



Physical Acquisition: Samsung Device

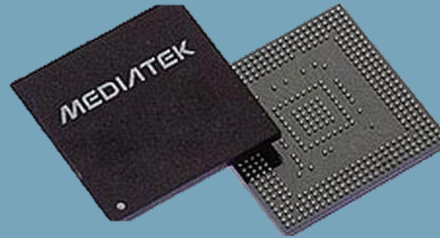
Il principale ostacolo all'estrazione dei dati dai dispositivi Samsung è che i dati dell'utente sono crittografati per impostazione predefinita. Qualsiasi moderno smartphone Samsung utilizza la crittografia con una chiave protetta dall'hardware, che non può essere disabilitata. I dispositivi Samsung rilasciati prima del 2019 utilizzano la crittografia full-disk (FDE).

CROSS DO NOT CROSS DO NOT CROSS DO NOT CROSS DO NOT CR

MOBILE FORENSICS

ACQUISIZIONE

Physical Acquisition:
Device basati su processori Mediatek

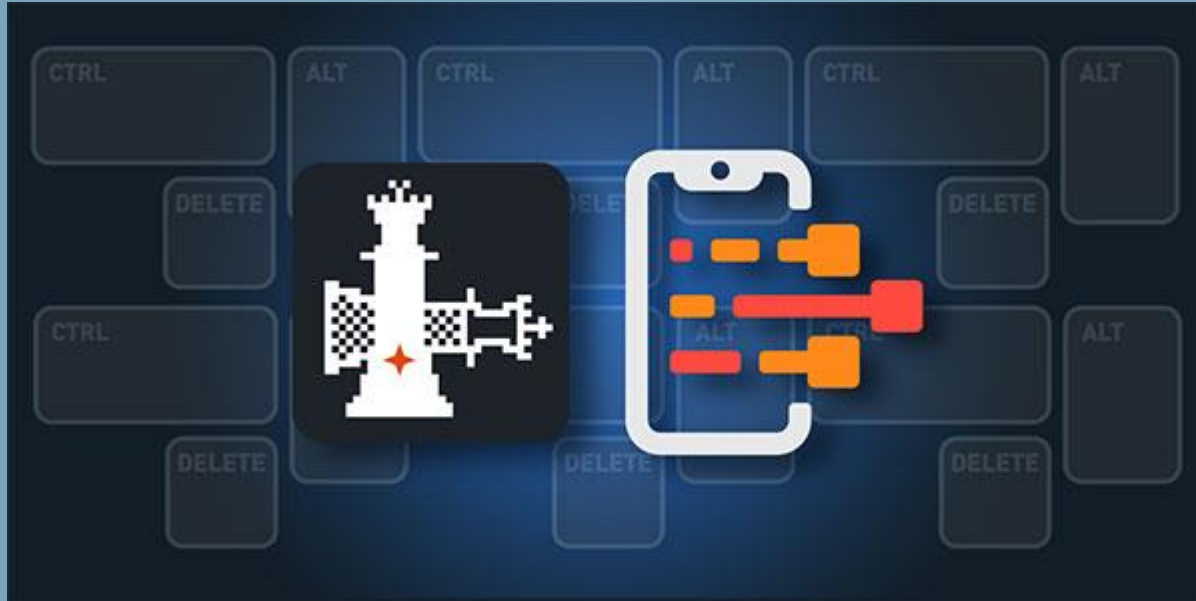


CROSS DO NOT CROSS DO NOT CROSS DO NOT CROSS DO NOT CROSS

MOBILE FORENSICS

ACQUISIZIONE

Full File System Acquisition: Apple Device



MOBILE FORENSICS

ACQUISIZIONE

**Full File System Acquisition:
Apple Device CheckM8 BootROM exploit**




Apple iPhone 7 (A1778)

USB cable 210 or Original Cable

File System

Full File System

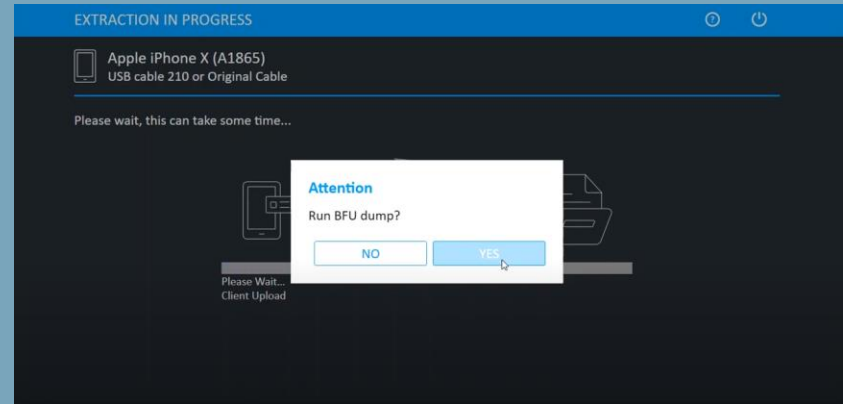
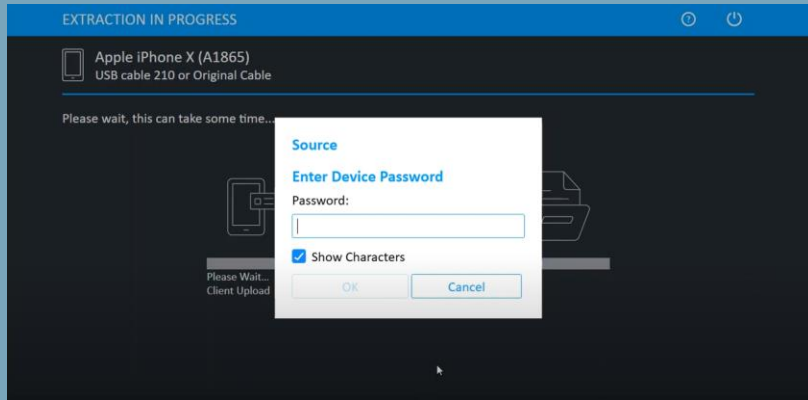
Full File System (checkm8) 

MOBILE FORENSICS

ACQUISIZIONE

Full File System Acquisition: Apple Device CheckM8 BootROM exploit

BFU (Before First Unlock)

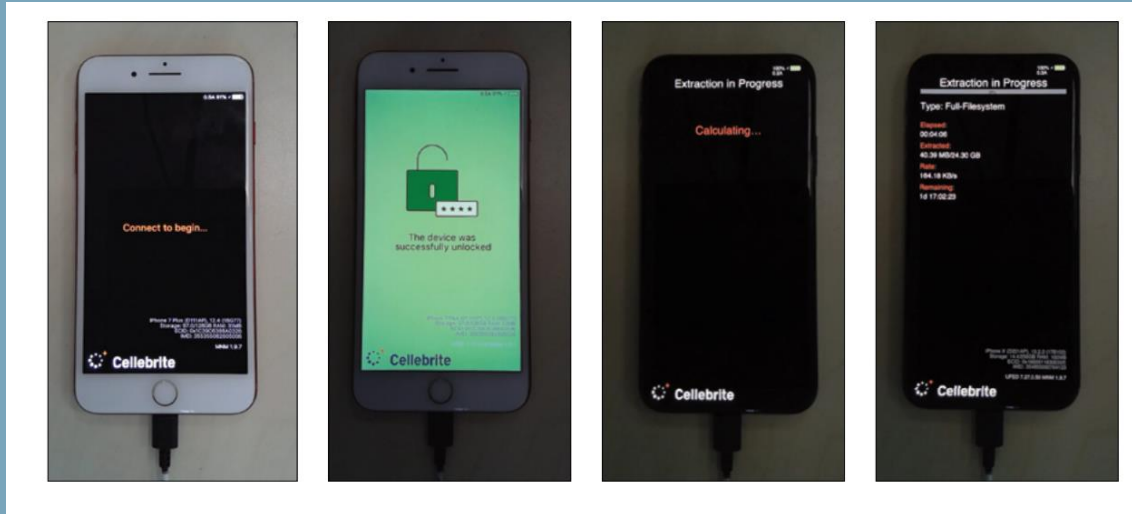


MOBILE FORENSICS

ACQUISIZIONE

**Full File System Acquisition:
Apple Device CheckM8 BootROM exploit**

AFU (After First Unlock)



MOBILE FORENSICS

ACQUISIZIONE

Apple Full File System Acquisition:

Device Content

[6 data sources can be extracted using UFED Cloud Analyzer](#)

Phone Data

Activities	25361	Application Usage	1820 (7)	Applications Usage...	9198 (57)	Bluetooth Devices	799 (5)
Calendar	434	Call Log	337 (2)	Cell Towers	1403	Chats	955 (4)
Contacts	4050 (59)	Cookies	2011 (3)	Device Events	11202	Device Locations	51591 (157)
Device Notifications	1	Emails	31472	Installed Applications	803 (2)	Log Entries	2700
MMS Messages	6	Notes	4	Passwords	1212	Recordings	4
Searched Items	561 (183)	SMS Messages	1200	User Accounts	22	User Dictionary	9261
Web Bookmarks	8	Web History	1667 (841)	Wireless Networks	29704		

Data Files

Applications	44 (1)	Archives	314 (16)	Audio	2902	Configurations	146717
Databases	1618	Documents	1461 (190)	Exchange	120 (3)	Images	57383 (130)
Text	3155 (6)	Uncategorized	67424 (32)	Videos	141 (5)		

MOBILE FORENSICS

ACQUISIZIONE

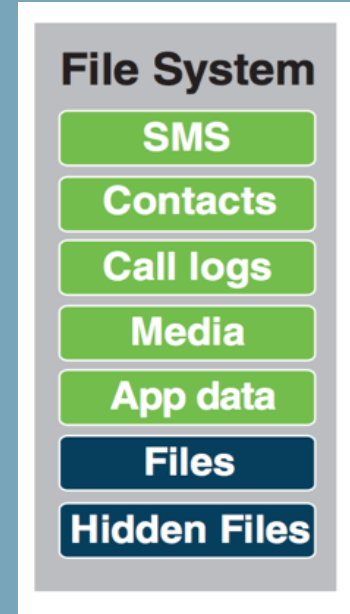
Apple BFU:

Name	Creation date	Modification date	Token	
com.apple.account.DeviceLocator.token (4C26B00...	11.09.13 02:57:00	05.03.15 22:32:41	AQAAAABU-K6O_rzKzko...	
com.apple.account.FindMyFriends.find-my-friends-...	17.09.14 11:24:12	05.03.15 22:32:40	AQAAAABU-K6OgjM-tIka...	
com.apple.account.DeviceLocator.token (2462990...	05.03.15 22:37:17	03.04.15 15:43:38	AQAAAABVHorQ6SBbZU...	
com.apple.account.FindMyFriends.find-my-friends-...	05.03.15 22:37:17	03.04.15 15:43:37	AQAAAABVHorQLndgKC...	
com.apple.account.DeviceLocator.token (AE0AA26...	03.04.15 15:45:23	03.04.15 15:54:24	AQAAAABVHo1WdTWSg...	
com.apple.account.FindMyFriends.find-my-friends-...	03.04.15 15:45:23	03.04.15 15:54:23	AQAAAABVHo1W7UviQj...	
com.apple.account.FindMyFriends.find-my-friends-...	08.09.16 07:43:37	23.08.19 05:59:54	EAAaaaaABLwIAAAAAAF1...	
com.apple.account.DeviceLocator.token (vkatalov...	08.09.16 07:43:40	23.08.19 05:59:55	EAAaaaaABLwIAAAAAAF1...	
com.apple.account.DeviceLocator.find-my-iphone-...	08.09.16 07:43:40	23.08.19 05:59:55	EAAaaaaABLwIAAAAAAF1...	
iCloud HomeKit Identifier (564819206)	30.11.16 04:15:43	30.11.16 04:15:43	4382DA20-42F8-47E8-9...	5

MOBILE FORENSICS

ACQUISIZIONE

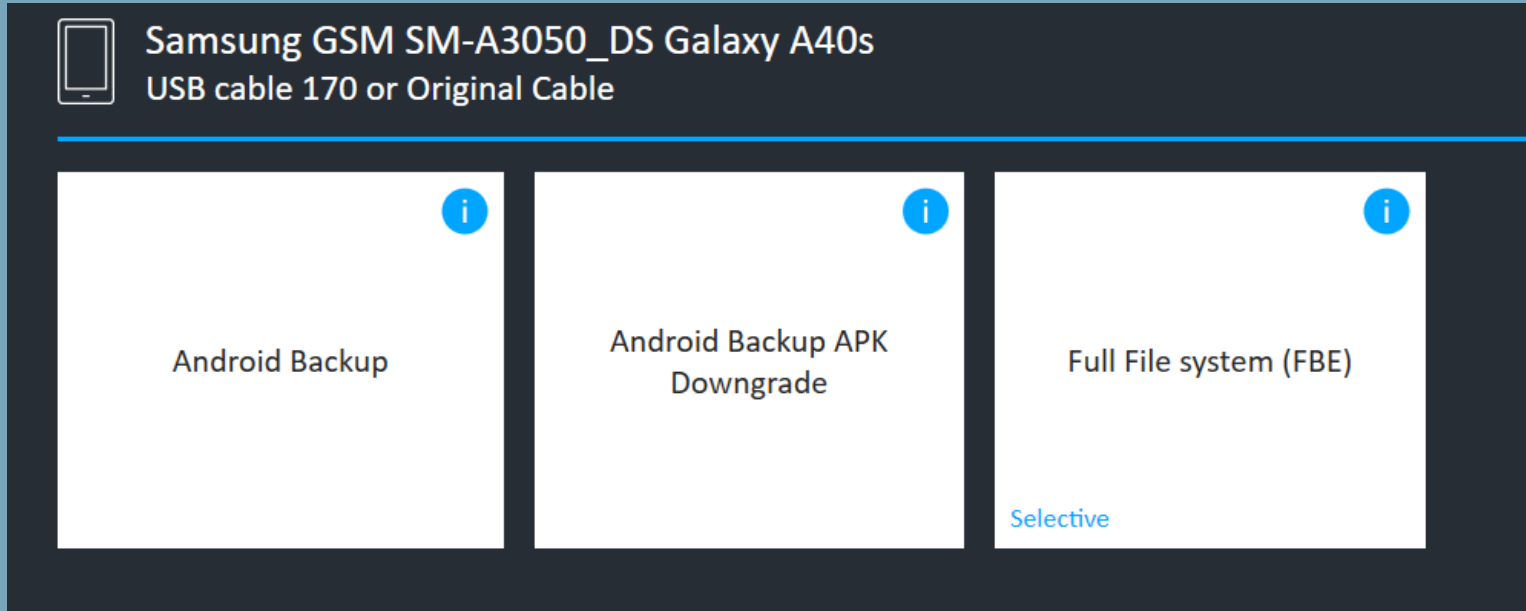
2) File system acquisition:



MOBILE FORENSICS

ACQUISIZIONE

2) File system acquisition:



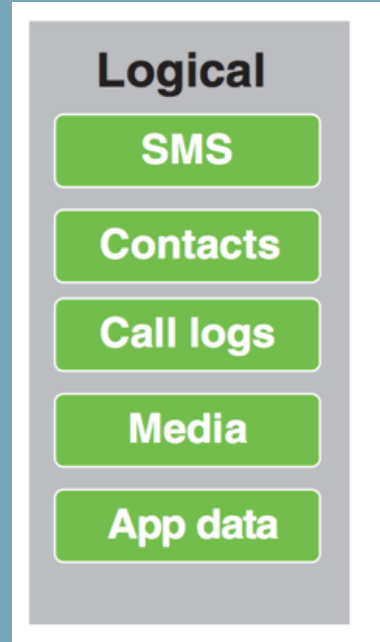
The screenshot shows a software interface for mobile forensic acquisition. At the top, it identifies the device as a Samsung GSM SM-A3050_DS Galaxy A40s and lists the required connection as USB cable 170 or Original Cable. Below this, there are three main acquisition options, each with an information icon (i) in the top right corner:

- Android Backup**: A simple text option.
- Android Backup APK Downgrade**: A text option for acquiring backup APKs.
- Full File system (FBE)**: A text option for full file system extraction, with a **Selective** option available below it.

MOBILE FORENSICS

ACQUISIZIONE

3) Logical Acquisition :



MOBILE FORENSICS

ACQUISIZIONE

Dispositivi mobili non convenzionali

Esempio Samsung Gear 3 smartwatch

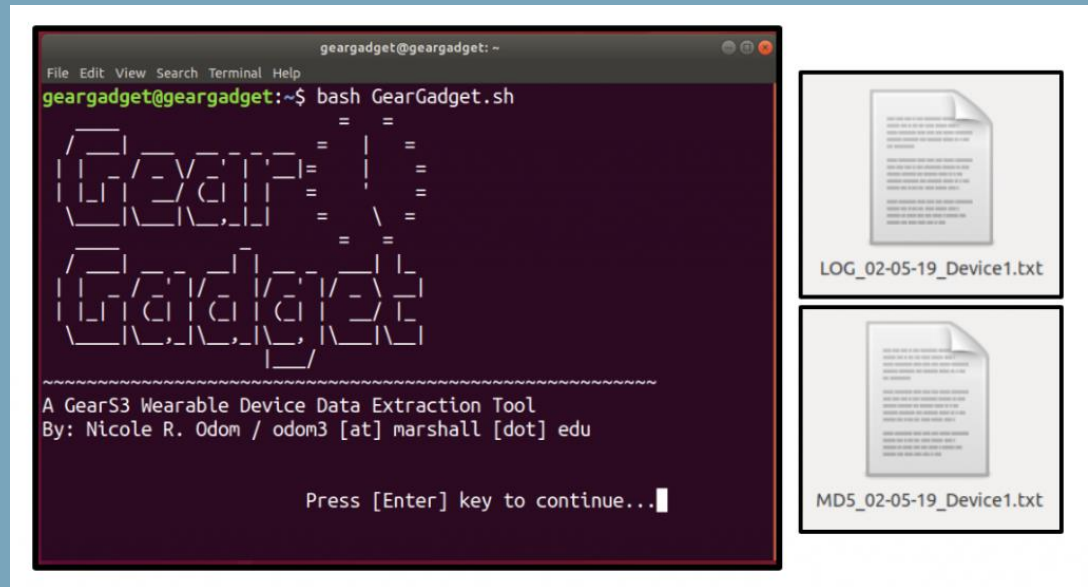


MOBILE FORENSICS

ACQUISIZIONE

Dispositivi mobili non convenzionali

Samsung Gear 3 smartwatch



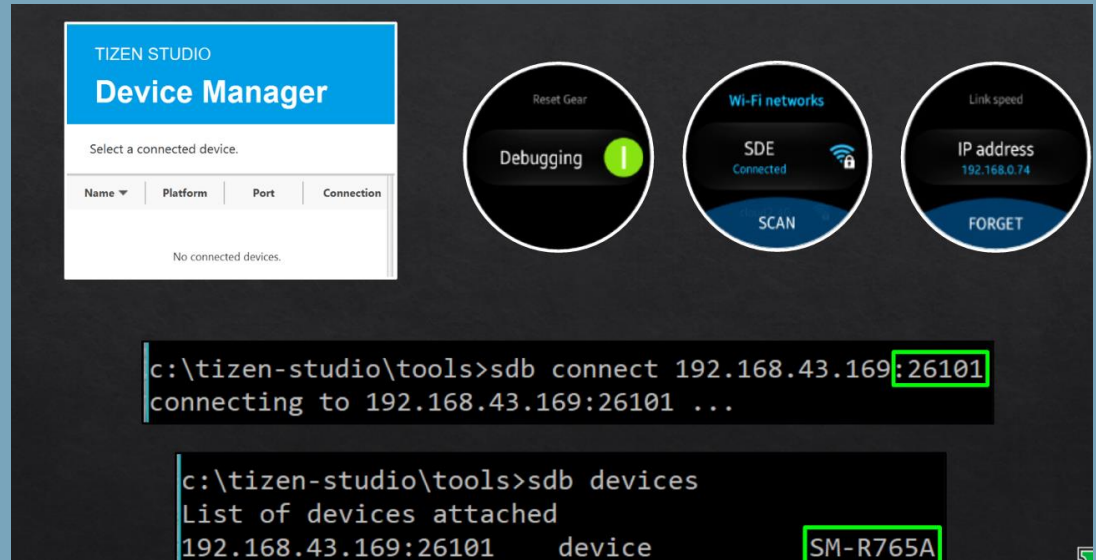
The image displays a terminal window on a Linux system. The terminal title is "geargadget@geargadget: ~". The prompt is "gargadget@geargadget:~\$". The user has entered the command "bash GearGadget.sh". The script outputs a stylized ASCII art logo for "GearGadget" with a grid of equals signs. Below the logo, it reads: "A GearS3 Wearable Device Data Extraction Tool" and "By: Nicole R. Odom / odom3 [at] marshall [dot] edu". At the bottom of the terminal, it says "Press [Enter] key to continue...". To the right of the terminal, there are two file icons representing log files: "LOG_02-05-19_Device1.txt" and "MD5_02-05-19_Device1.txt".

MOBILE FORENSICS

ACQUISIZIONE

Dispositivi mobili non convenzionali

Samsung Gear 3 smartwatch



The screenshot displays the Tizen Studio interface and a terminal window. The Tizen Studio Device Manager window shows a table with columns for Name, Platform, Port, and Connection, and a message indicating no connected devices. The terminal window shows the command `sdb connect 192.168.43.169:26101` being executed, followed by the output `connecting to 192.168.43.169:26101 ...`. A second terminal window shows the command `sdb devices` being executed, followed by the output `List of devices attached` and a table with columns for IP address and device name, showing `192.168.43.169:26101 device SM-R765A`.

TIZEN STUDIO
Device Manager

Select a connected device.

Name	Platform	Port	Connection
No connected devices.			

Reset Gear
Debugging ⓘ

Wi-Fi networks
SDE Connected
SCAN

Link speed
IP address 192.168.0.74
FORGET

```
c:\tizen-studio\tools>sdb connect 192.168.43.169:26101
connecting to 192.168.43.169:26101 ...
```

```
c:\tizen-studio\tools>sdb devices
List of devices attached
192.168.43.169:26101 device SM-R765A
```

MOBILE FORENSICS

ACQUISIZIONE

Dispositivi mobili non convenzionali

Samsung Gear 3 smartwatch

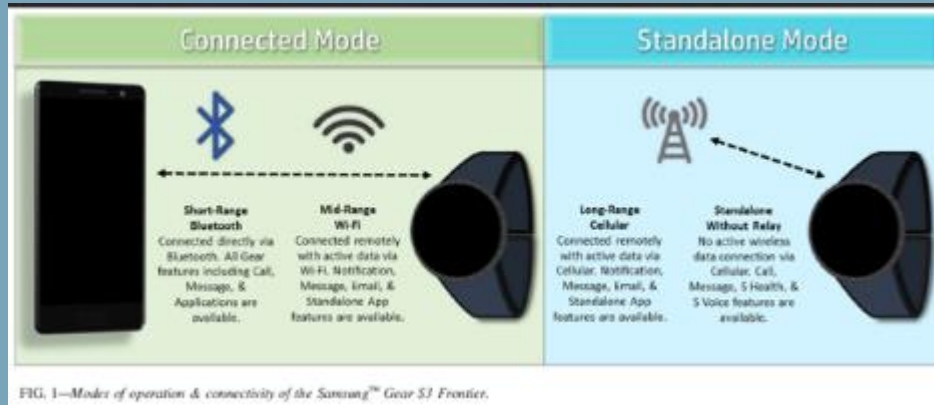
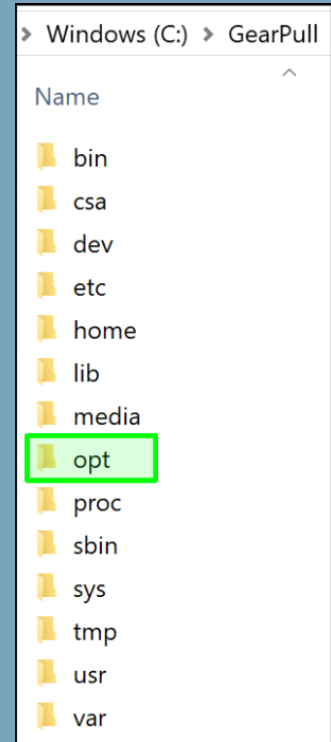


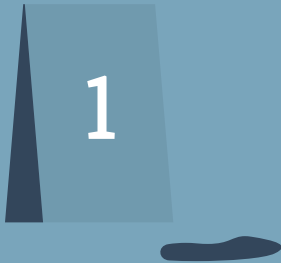
FIG. 1—Modes of operation & connectivity of the Samsung™ Gear S3 Frontier.



LAB INVESTIGATIONS

ACQUISIZIONE

Valutazione ed esecuzione dell'acquisizione dei dispositivi post mortem



ANALISI

Analisi e ricostruzione delle evidenze digitali prodotte dalle operazioni tecniche di acquisizione



REFERTO TECNICO

Valutazione dei risultati e conclusioni mediante produzione di accurati report investigativi



LAB INVESTIGATIONS



AccessData®

- Analizzare le informazioni al fine di ricavare potenziali fonti probatorie di interesse investigativo è l'aspetto più complesso, richiede esperienza, elevate capacità tecniche e conoscenze informatiche avanzate costantemente aggiornate.

LAB INVESTIGATIONS

REFERITO TECNICO

- Fase di produzione del report contenente le risultanze dell'analisi.
- Tradurre le informazioni tecniche in informazioni pratiche comprensibili per il giudice o il pubblico ministero.

Computer Forensic Analysis Report

MEMORANDUM FOR (Client POC Name), (Client Organization Name) **Date:** (Report Date)

FROM: (Investigator Name), (Investigator Title)
(Investigating Organization Name)
(Investigating Organization Address)

SUBJECT: Cyber Forensic Investigation Analysis Report
Person of Interest (POI) / Subject(s) Name: John M. Smith
Born: (Date of birth of POI) (Additional identifiers of POI may be added)
Case Number: (Place case number)

1. Support Requested

(Client POC), (Client Organization) requested the examination of the submitted digital media seized as a result of suspected criminal behavior related to the theft and subsequent sale of company proprietary information. The request asked that the submitted media be examined for any evidence related to the theft and/or sale of proprietary information, particularly cancer preventing trial medicines, and the existence of possible co-conspirators who participated in, or facilitated the unlawful activity.

2. Status: Pending (or closed)

3. Summary of Findings

The examination of submitted media, which was conducted during the period of (start date) and (end date) resulted in the discovery of numerous image files depicting transporting of proprietary information indicated in the Request for Analysis. A number of the image files also showed the suspect, (POI's last name), in possession of the materials. Additionally, a review of Internet activity resulted in the discovery of a number of instances where the suspect's computer was used to access Internet auction sites in an attempt to sell proprietary information. While the suspect received numerous email correspondences from individuals apparently responding to his auction advertisements and participated in newsgroup conversations regarding the sale of proprietary information, little information was found which indicates the existence of a conspiracy between the suspect and any other individuals in this activity.

Released by _____
(Investigator's Name)
Computer Forensic Analyst

ACCERTAMENTI TECNICI URGENTI NON RIPETIBILI

L'Art. 360 c.p.p. (Accertamenti Tecnici Non Ripetibili) prevede che, quando gli accertamenti previsti dall'artt. 359 riguardano persone, cose o luoghi il cui stato è soggetto a modificazione, il P.M. avvisa, senza ritardo, la persona sottoposta alle indagini, la persona offesa dal reato e i difensori del giorno, dell'ora e del luogo fissati per il conferimento dell'incarico e della facoltà di nominare consulenti tecnici. I difensori nonché i consulenti tecnici eventualmente nominati, hanno diritto di assistere al conferimento dell'incarico, di partecipare agli accertamenti e di formulare osservazioni o riserve.



The image displays two X-ray views of a human neck and upper chest. The left view is a lateral (side) view, showing the cervical spine, the skull, and the upper thoracic region. The right view is an anterior (front) view, showing the skull, the larynx, the trachea, and the upper thoracic region. A ruler is visible on the left side of the lateral view and on the right side of the anterior view, providing a scale for the images. The text "Result analysis" is overlaid in the center of the image.

Result analysis

THANKS

fabio.massa@angif.it

