DIGITAL CRIME SCENE INVESTIGATION

Tecniche avanzate di Mobile Forensics

Fabio Massa – Cyber Crime Investigator

02 METODOLOGIA

Pianificazione delle metodologie investigative, valutazione pratica dell'efficacia

03 ACQUISIZIONE

Applicazione delle tecniche investigative digitali pianificate

01 VALUTAZIONE

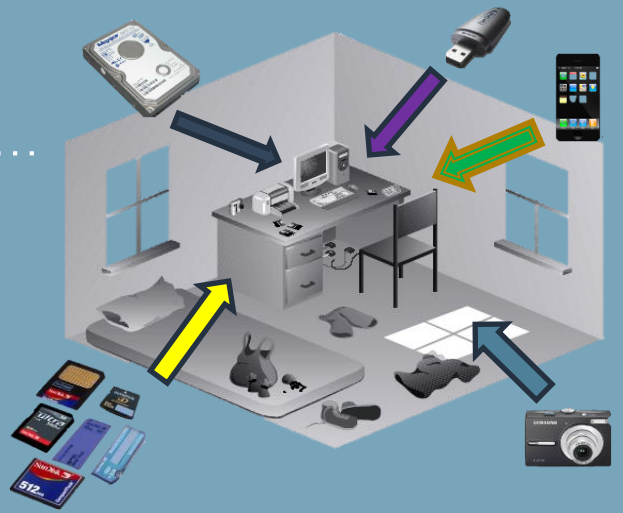
Valutazione primaria delle potenziali sorgenti informative

04 ANALISI

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

DIGITAL CRIME SCENE INVESTIGATION

LAW ENFORCEMENT FIRST RESPONDER
DIGITAL CRIME SCENE



PHYSICAL EVIDENCE VS DIGITAL EVIDENCE

BEST PRATICES

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

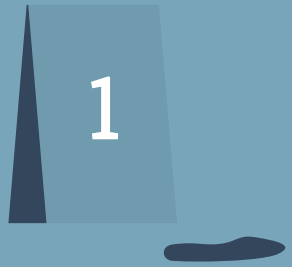
Una caratteristica fondamentale delle tracce digitali è l'**immaterialità**; non esistono come oggetto fisico ma sono **sequenze di bit** memorizzate su **dispositivi di archiviazione dati**. Per accedere ad una traccia occorre dunque accedere al dispositivo su cui essa è memorizzata. I dispositivi di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

ON SITE INVESTIGATIONS

IDENTIFICAZIONE

Identificazione dei dispositivi e delle digital evidence da acquisire o repertare



PRESERVAZIONE

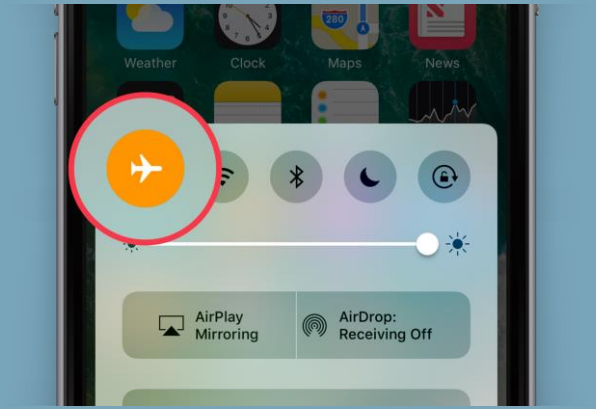
Esecuzione di tutte le possibili precauzioni per garantire l'integrità dei dati e dei dispositivi da repertare o acquisire

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

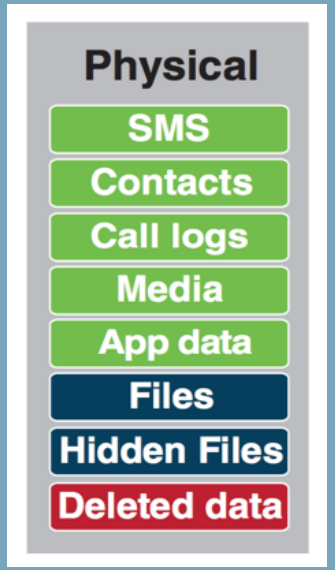
L'imaging può essere eseguito con l'aiuto di diversi strumenti come Cellebrite 4PC, Cellebrite hysical Analyzer, Oxygen Forensic Detective, Msab XRY, Magnet Axiom, Belkasoft Evidence Center, Accessdata FTK Imager ecc.

MOBILE FORENSICS

ACQUISIZIONE

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

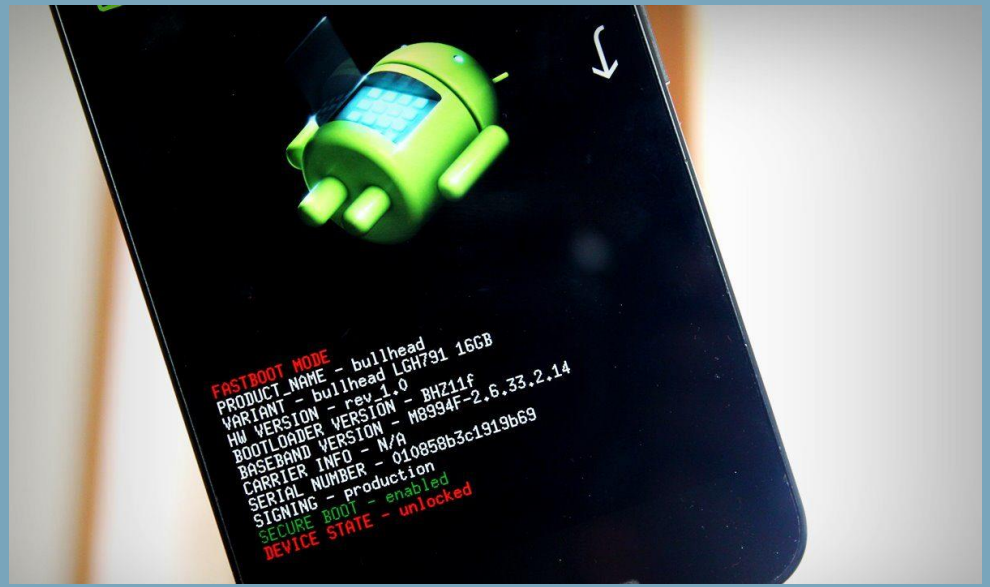
1) **Physical Acquisition**:



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:

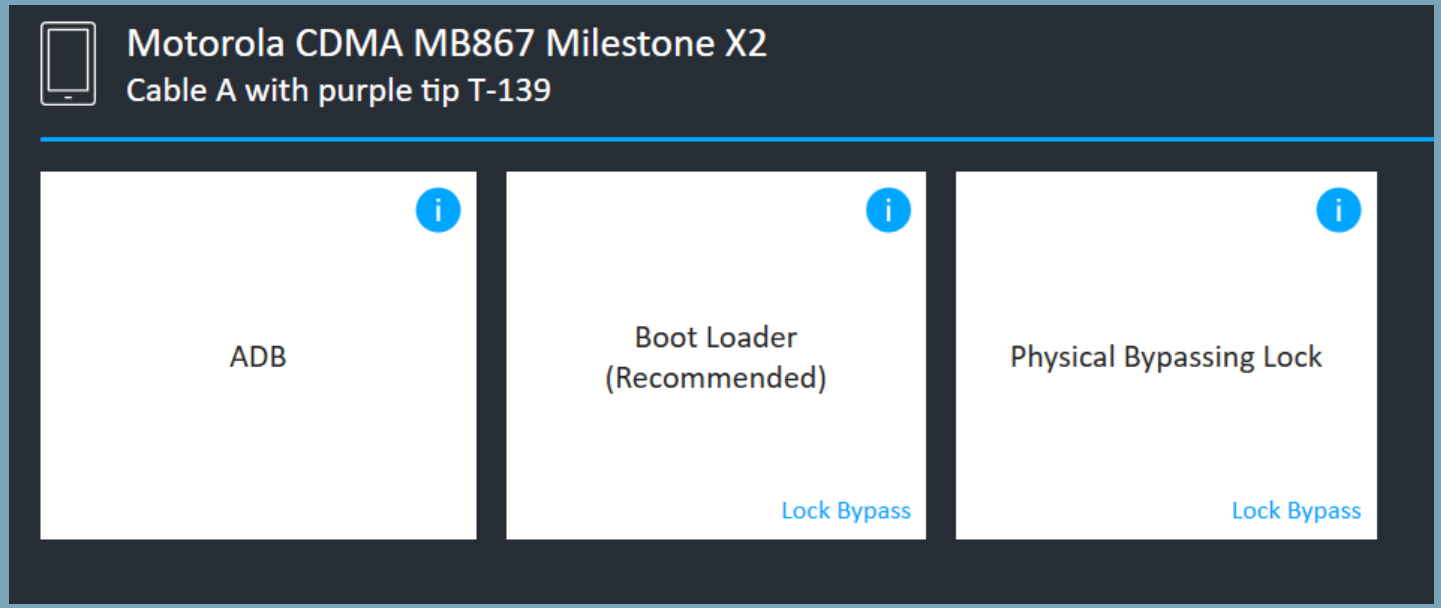
Dumping: Durante questa fase, i dati dalla memoria fisica vengono scaricati in un formato di file esadecimale non elaborato.

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

MOBILE FORENSICS

ACQUISIZIONE

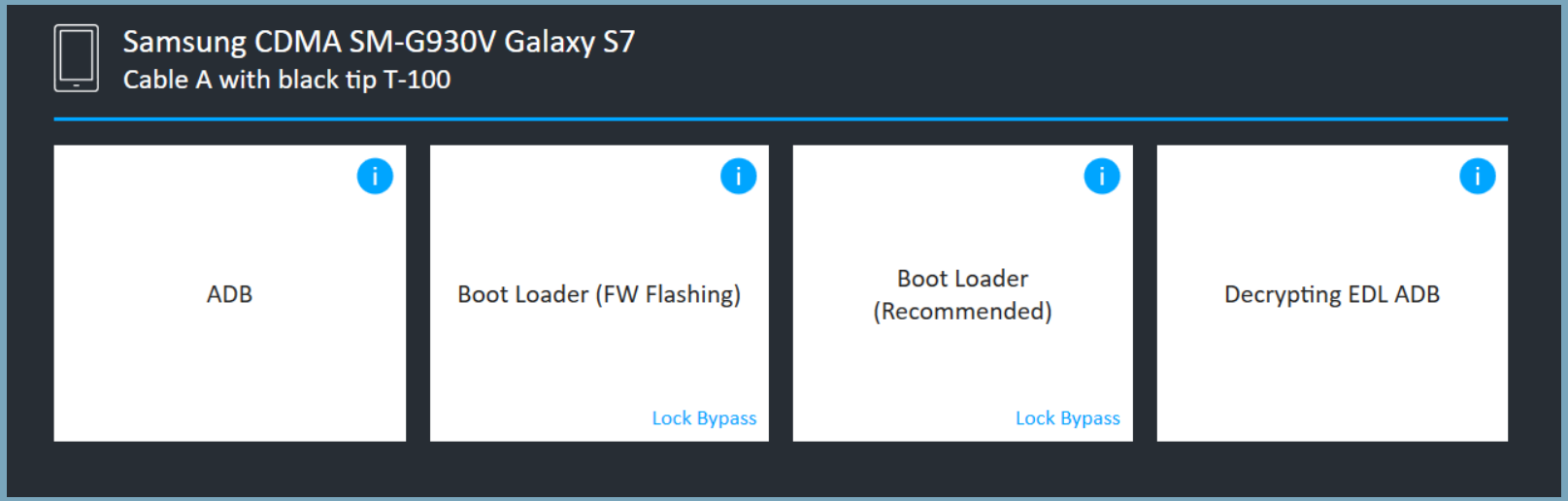
Physical Acquisition:



MOBILE FORENSICS

ACQUISIZIONE

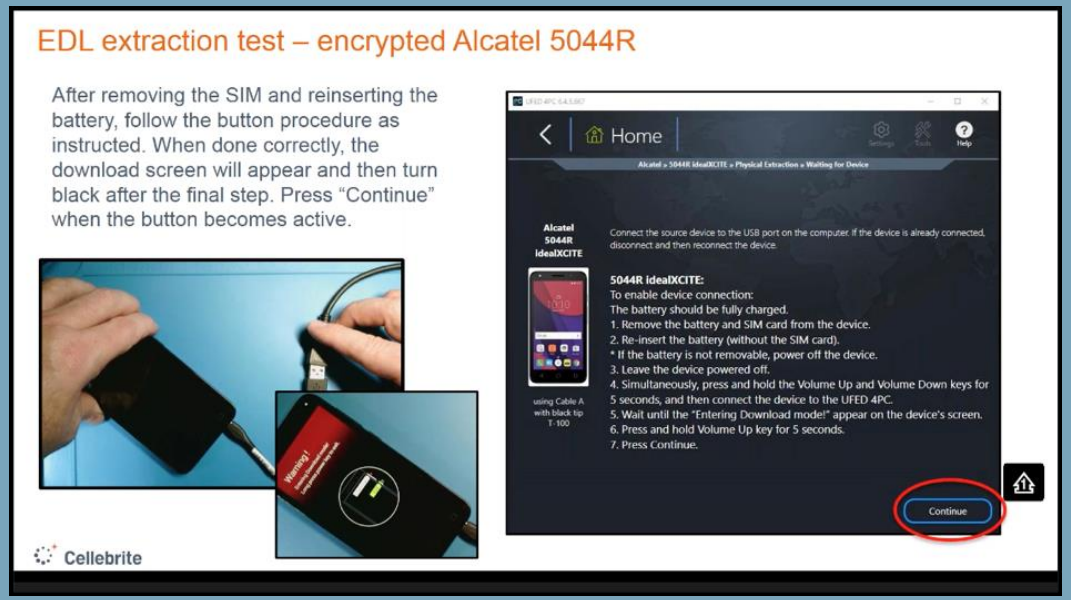
Physical Acquisition:



MOBILE FORENSICS

ACQUISIZIONE

Qualcomm - Emergency Download Mode (EDL)



Utilizzo della modalità EDL. Fonte: webinar su Cellebrite

MOBILE FORENSICS

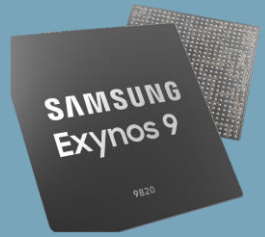
ACQUISIZIONE

Emergency Download Mode (EDL)

TEST POINT

MOBILE FORENSICS

ACQUISIZIONE



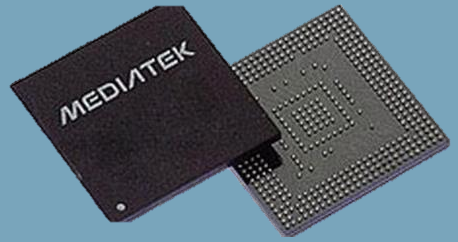
Physical Acquisition:
Samsung Device

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).

MOBILE FORENSICS

ACQUISIZIONE

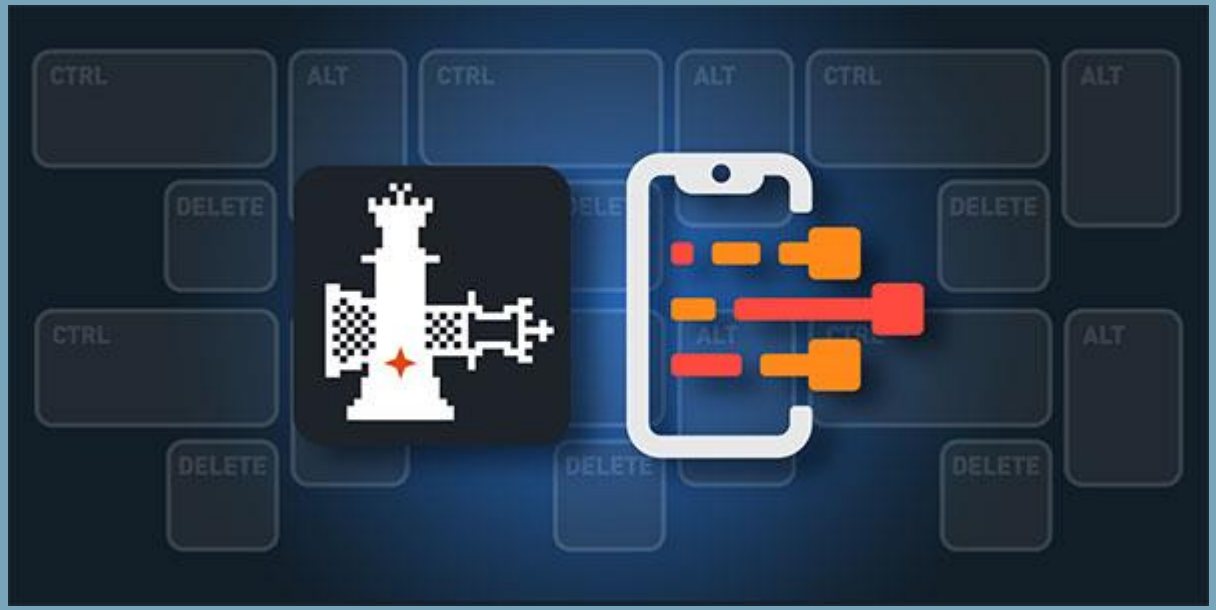
Physical Acquisition:
Device basati su processori Mediatek



MOBILE FORENSICS

ACQUISIZIONE

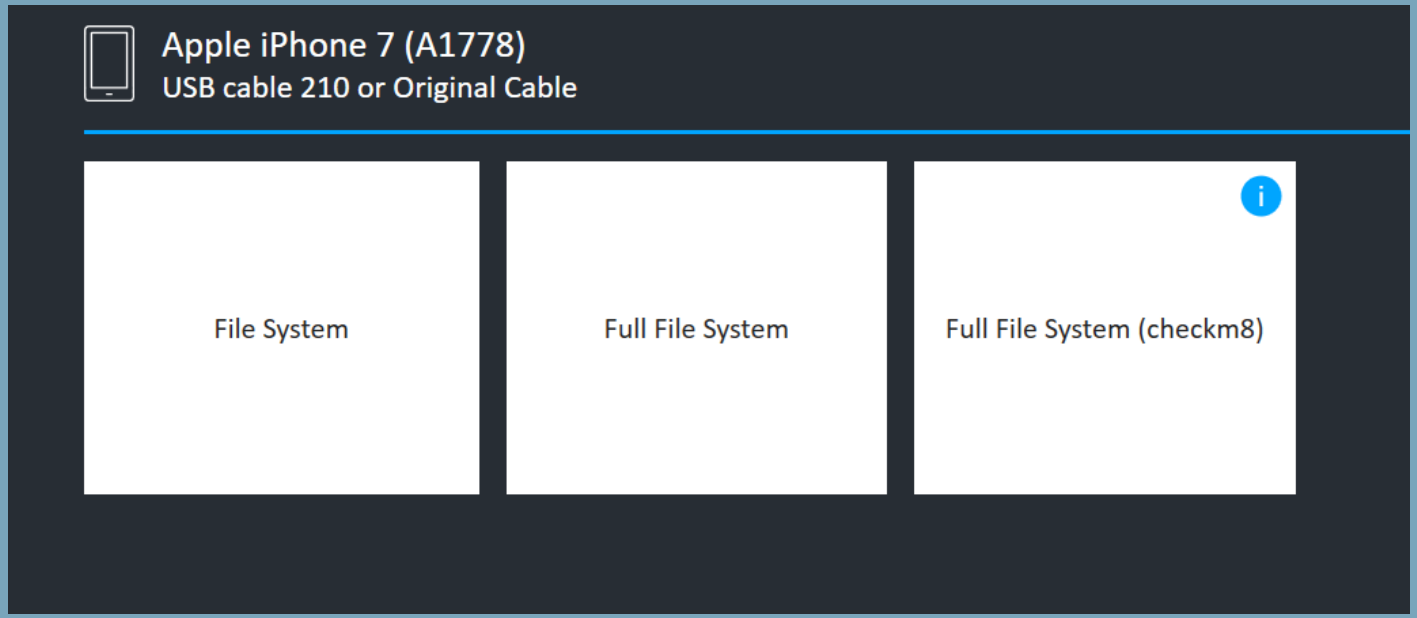
Full File System Acquisition:
Apple Device



MOBILE FORENSICS

ACQUISIZIONE

Full File System Acquisition:
Apple Device CheckM8 BootROM exploit

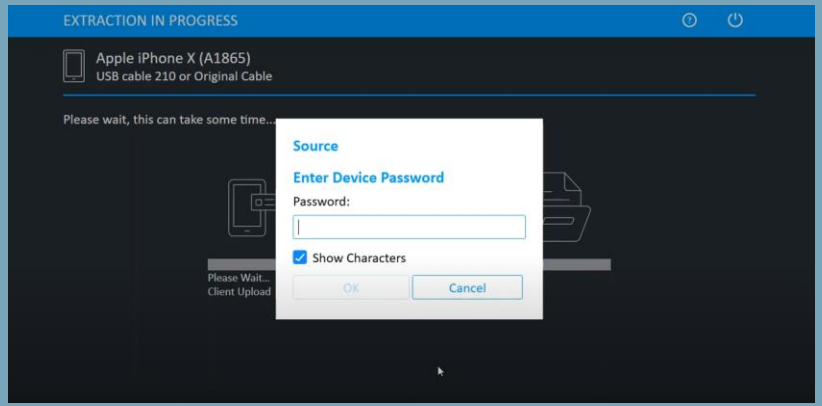


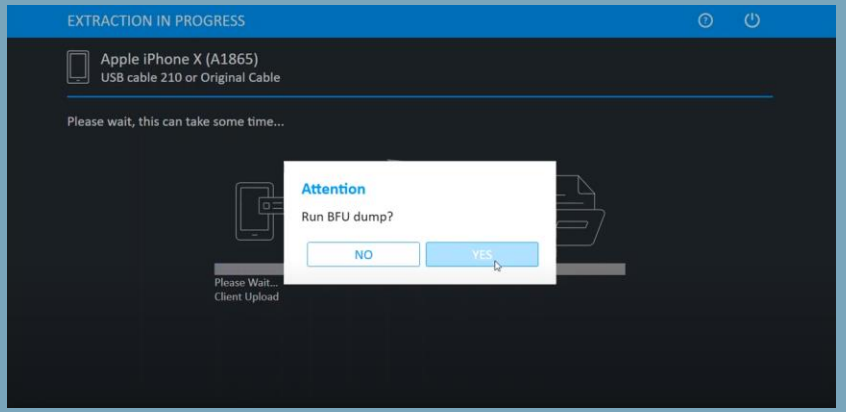
MOBILE FORENSICS

ACQUISIZIONE

Full File System Acquisition:
Apple Device CheckM8 BootROM exploit

BFU (Before First Unlock)



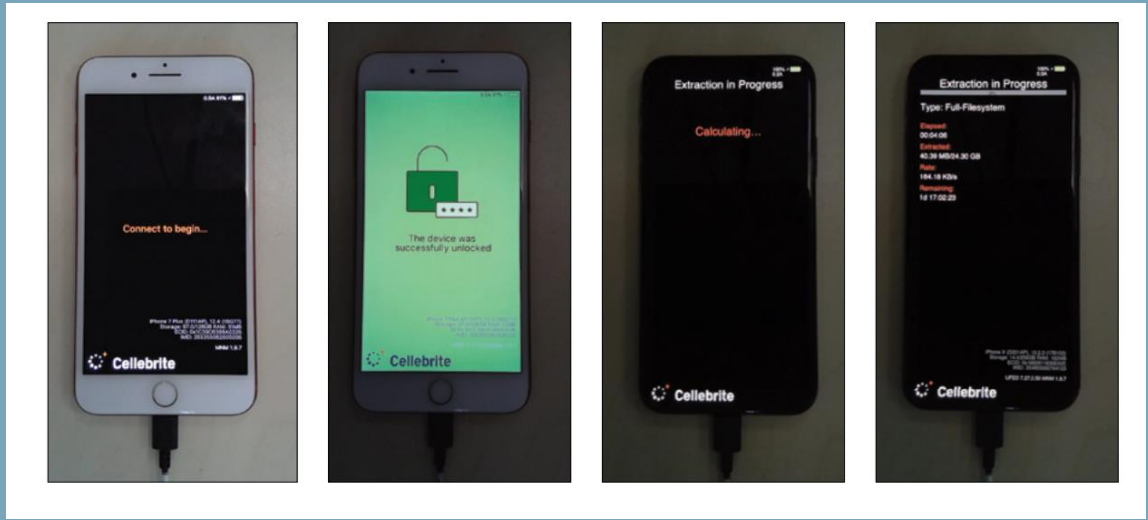


MOBILE FORENSICS

ACQUISIZIONE

Full File System Acquisition:
Apple Device CheckM8 BootROM exploit

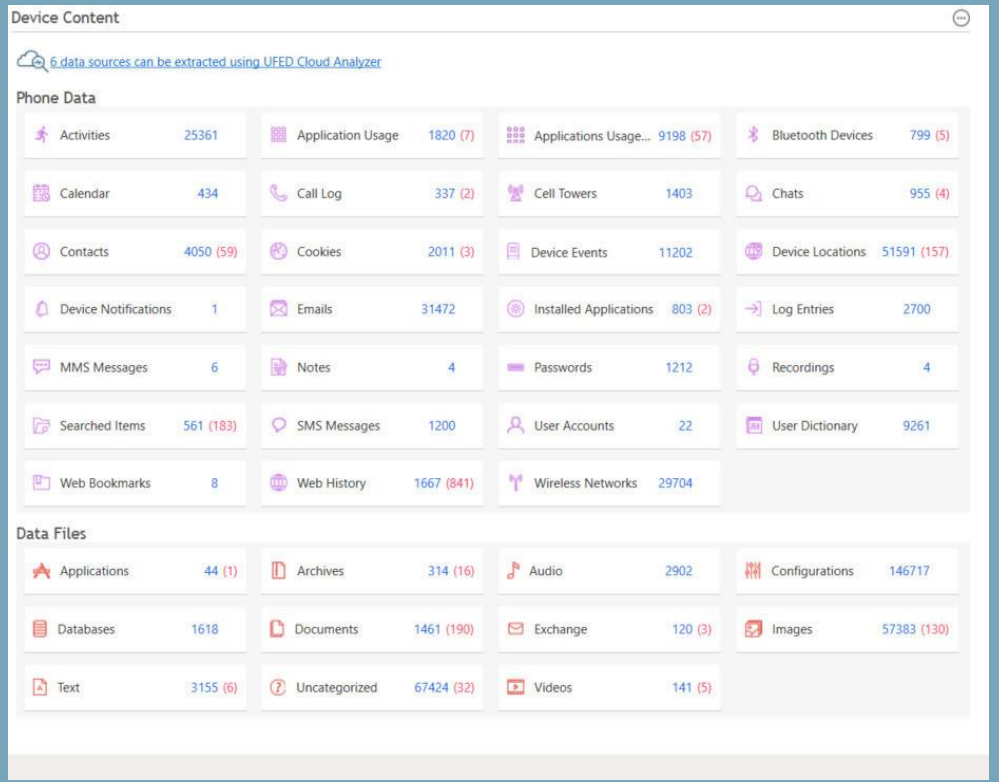
AFU (After First Unlock)



MOBILE FORENSICS

ACQUISIZIONE

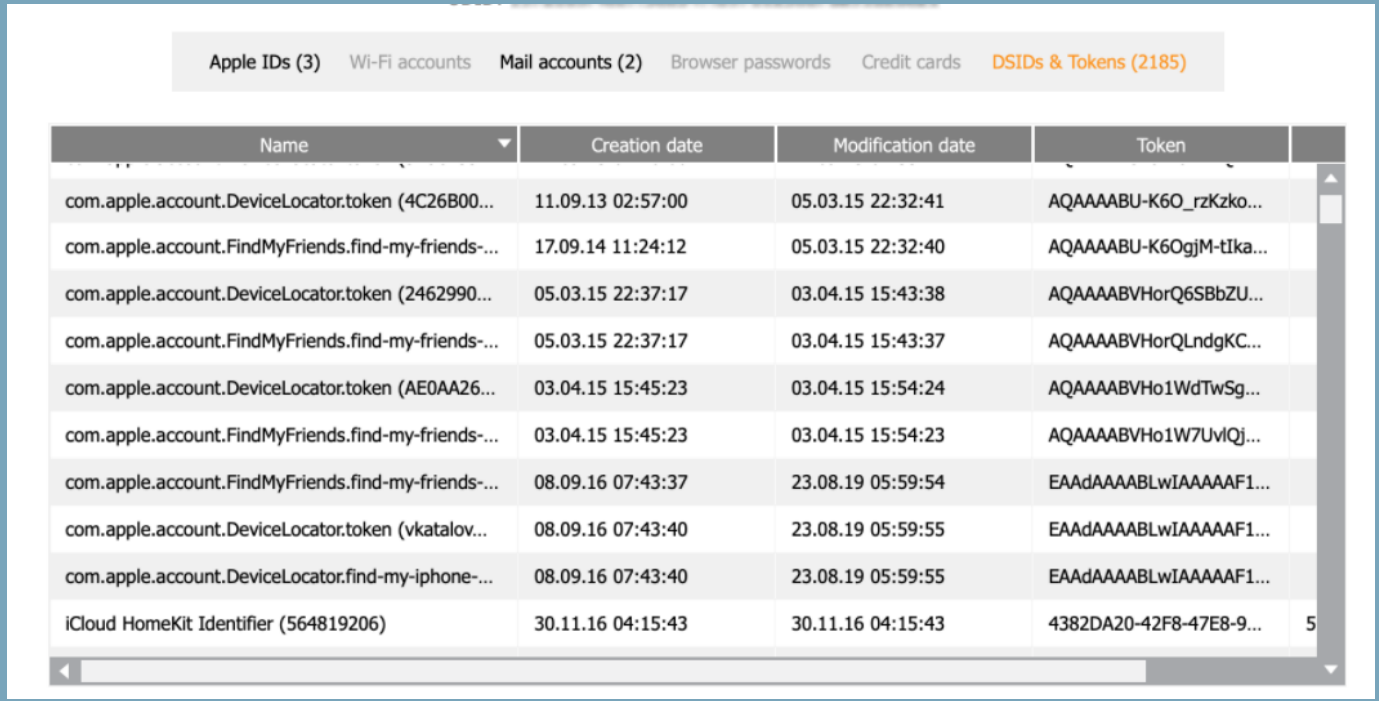
Apple Full File System Acquisition:



MOBILE FORENSICS

ACQUISIZIONE

Apple BFU:



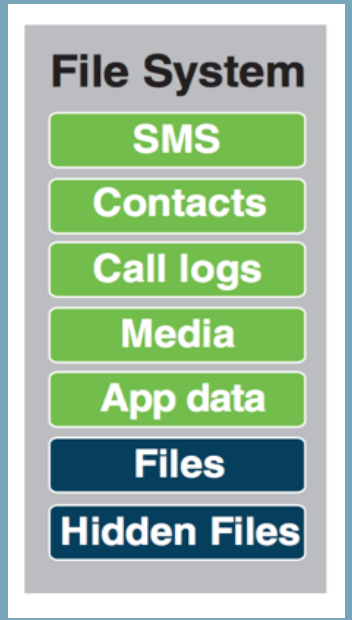
Apple IDs (3) | Wi-Fi accounts | Mail accounts (2) | Browser passwords | Credit cards | DSIDs & Tokens (2185)

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	AQAAAABVHo1W7UvlQj...
com.apple.account.FindMyFriends.find-my-friends-...	08.09.16 07:43:37	23.08.19 05:59:54	EAAdAAAABLwIAAAAAF1...
com.apple.account.DeviceLocator.token (vkatalov...	08.09.16 07:43:40	23.08.19 05:59:55	EAAdAAAABLwIAAAAAF1...
com.apple.account.DeviceLocator.find-my-iphone-...	08.09.16 07:43:40	23.08.19 05:59:55	EAAdAAAABLwIAAAAAF1...
iCloud HomeKit Identifier (564819206)	30.11.16 04:15:43	30.11.16 04:15:43	4382DA20-42F8-47E8-9...

MOBILE FORENSICS

ACQUISIZIONE

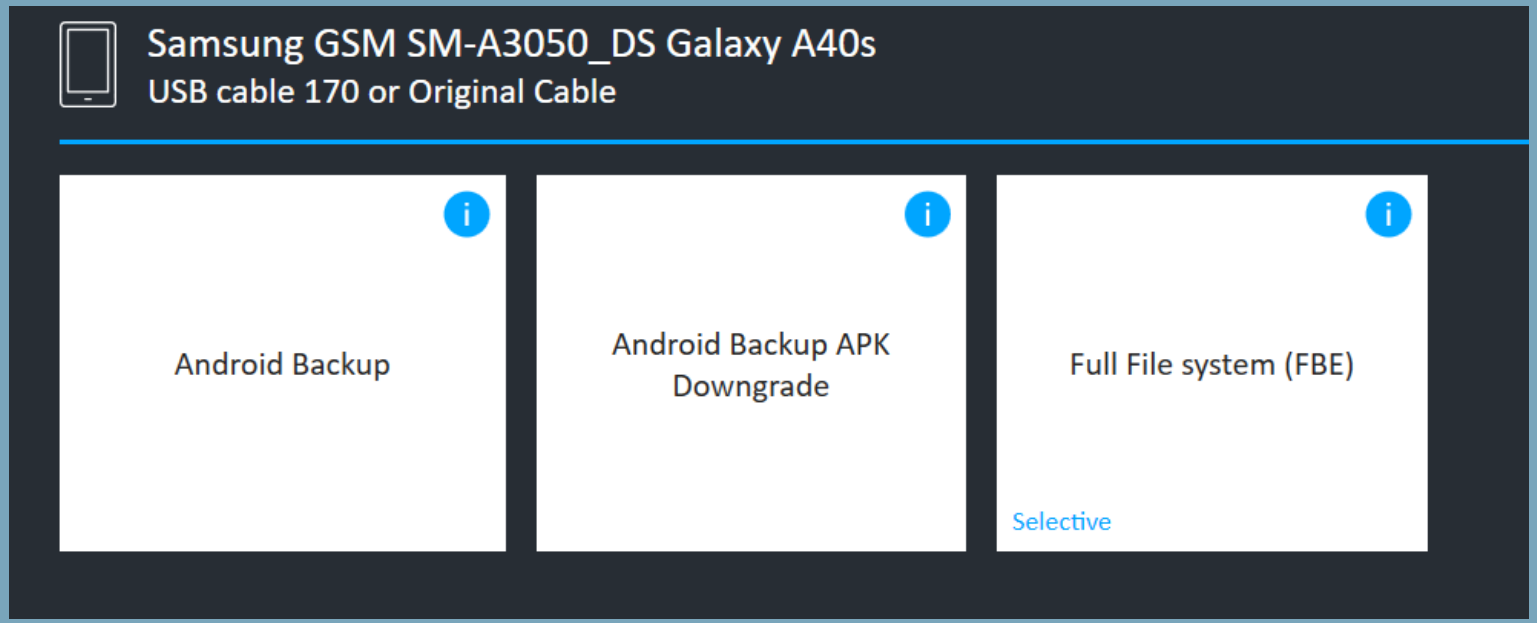
2) File system acquisition:



MOBILE FORENSICS

ACQUISIZIONE

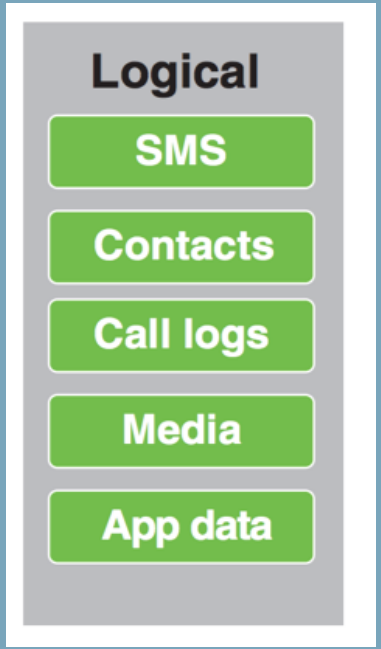
2) File system acquisition:



MOBILE FORENSICS

ACQUISIZIONE

3) Logical Acquisition :



MOBILE FORENSICS

ACQUISIZIONE

Dispositivi mobili non convenzionali

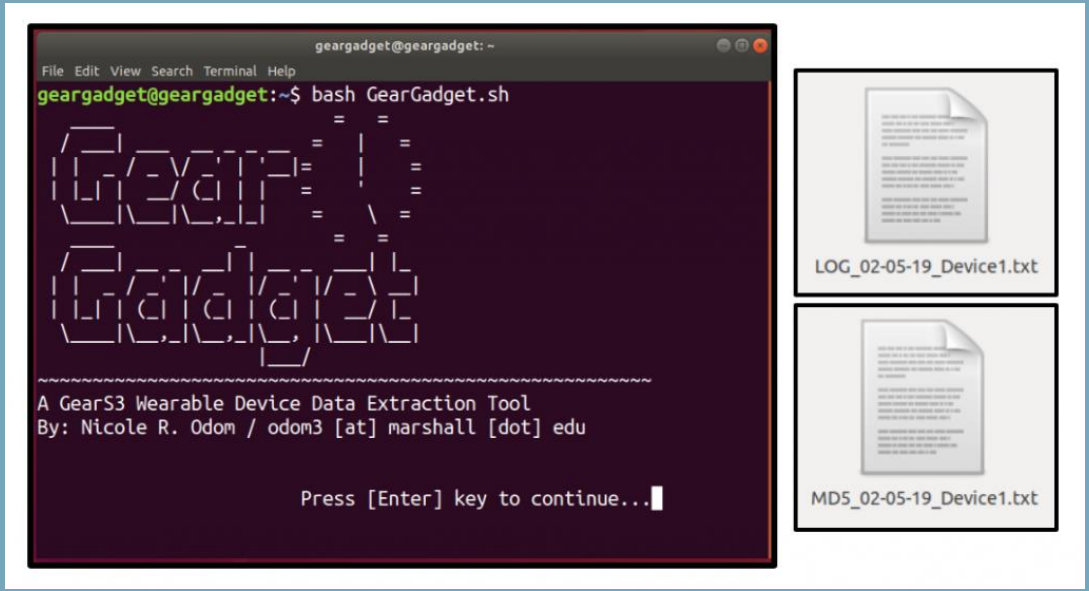
Esempio Samsung Gear 3 smartwatch

MOBILE FORENSICS

ACQUISIZIONE

Dispositivi mobili non convenzionali

Samsung Gear 3 smartwatch

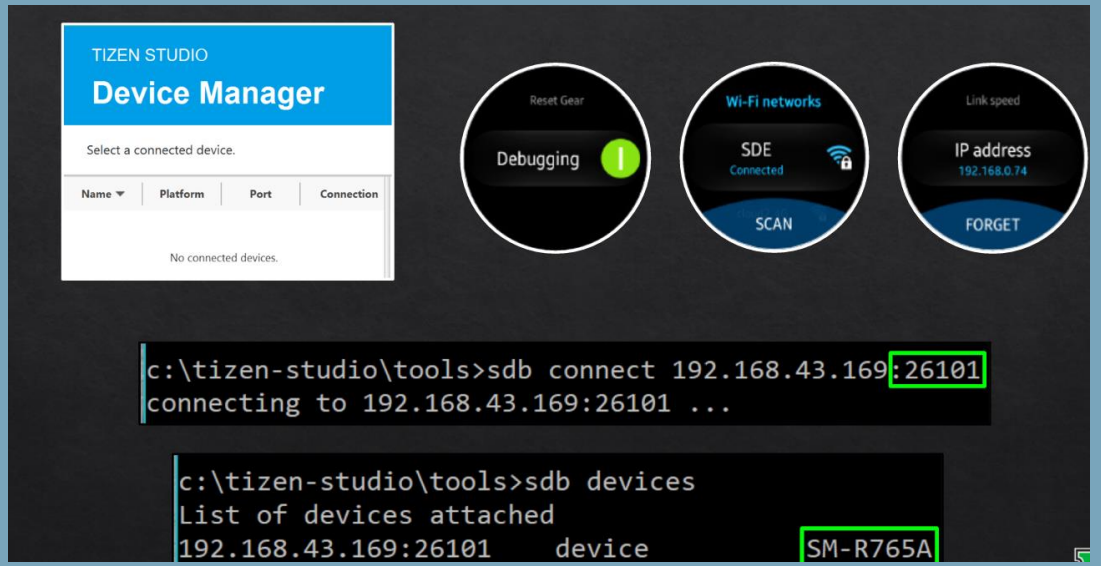


MOBILE FORENSICS

ACQUISIZIONE

Dispositivi mobili non convenzionali

Samsung Gear 3 smartwatch



MOBILE FORENSICS

ACQUISIZIONE

Dispositivi mobili non convenzionali

Samsung Gear 3 smartwatch

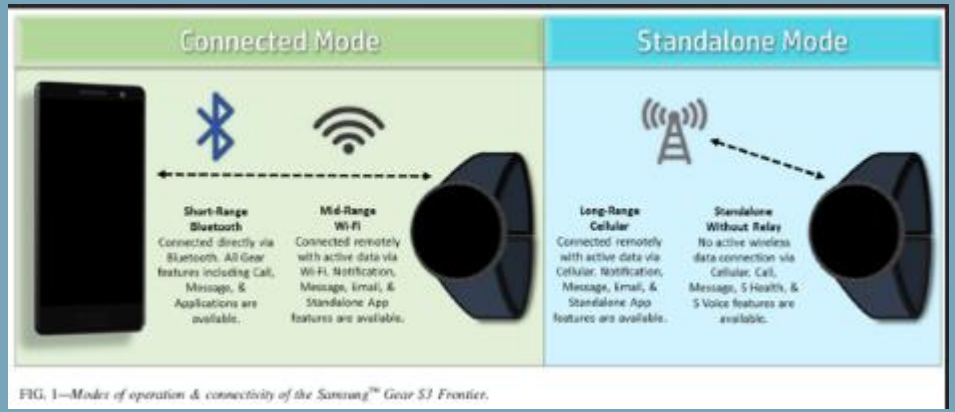
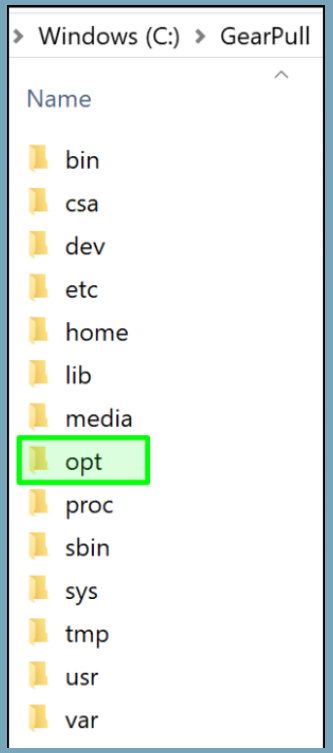


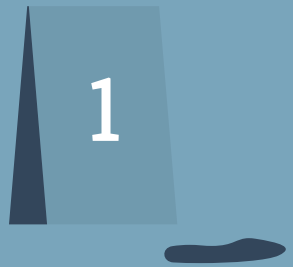
FIG. 1—*Modes of operation & connectivity of the Samsung™ Gear S3 Frontier.*



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

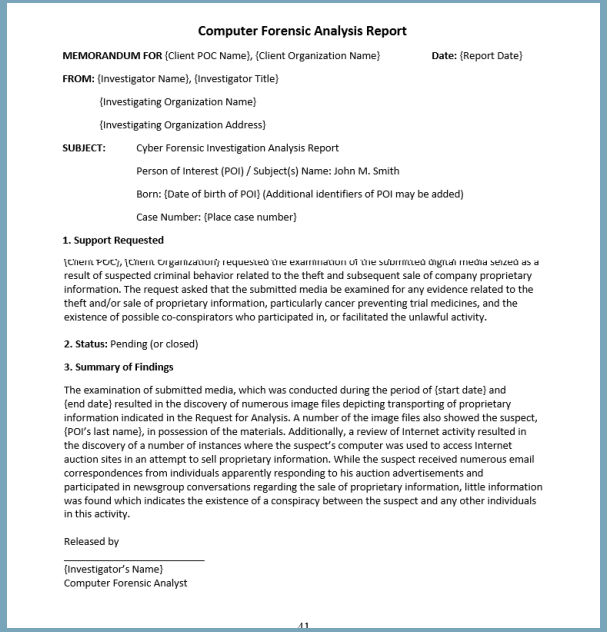
LAB INVESTIGATIONS

- 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

REFERTO 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.

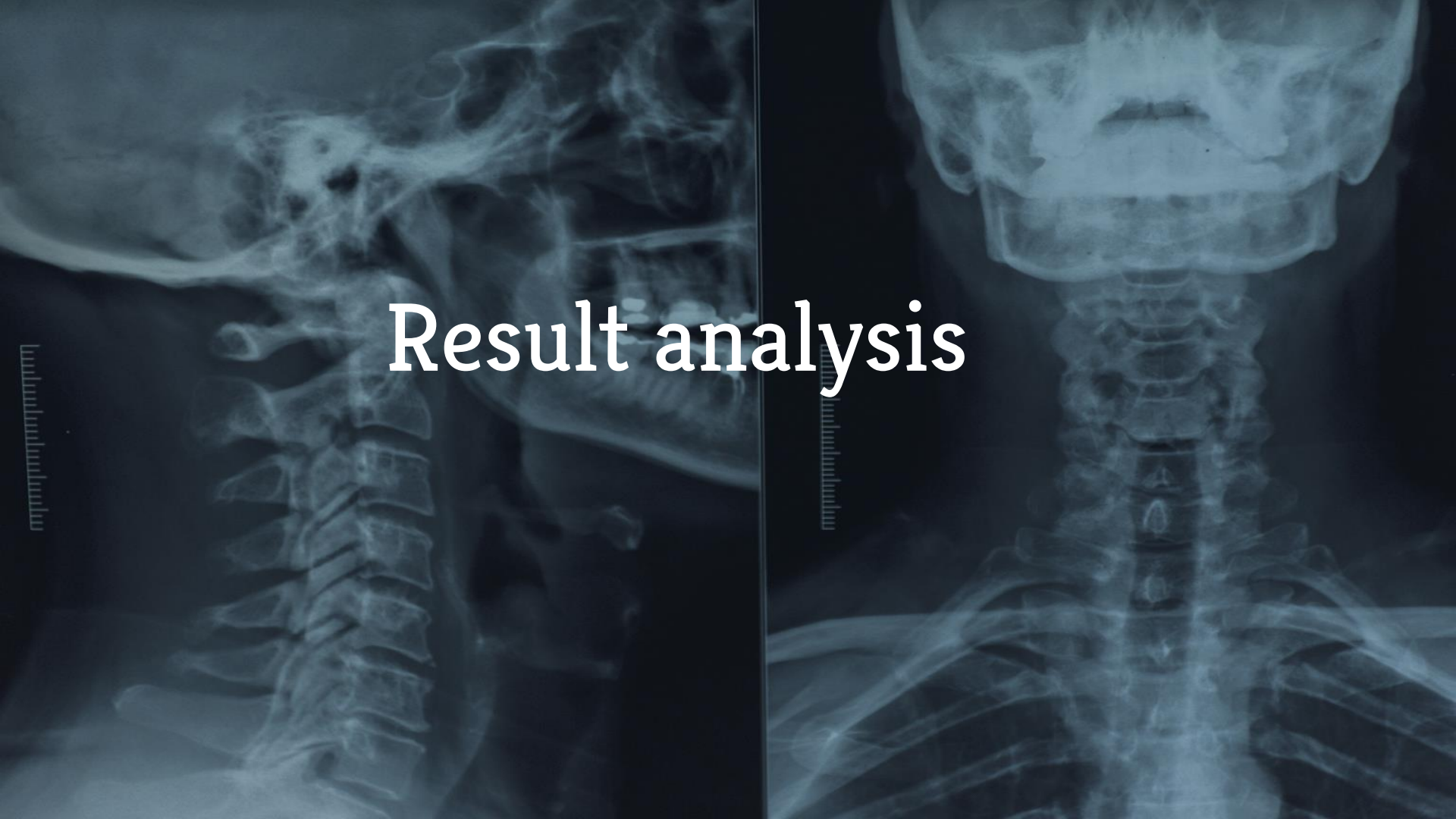
Released by

_____
{Investigator's Name}
Computer Forensic Analyst

41

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.



Result analysis

THANKS

fabio.massa@angif.it