DIGITAL FORENSICS

Acquisizione Forense di Evidenze da Mobile

INDAGINI ONLINE

AGENDA

- Acquisizione e analisi forense
  - Identificazione
  - Raccolta
  - Acquisizione
  - Analisi
- Presentazione dei risultati – Reporting
  - Esempio di Report + Esercitazione
- Conclusioni – Quesiti

Acquisizione e analisi forense

INDAGINI ONLINE

Problema

I dispositivi digitali portatili (cd. Mobile device) - come il telefono cellulare, il palmare, lo smartphone, lo smartwatch, il tablet, il laptop, il lettore digitale, il riproduttore digitale, il navigatore portatile gps, ecc. - rappresentano, spesso inconsapevolmente, **il diario multimediale di ognuno di noi.**

Nati per consentire la comunicazione in mobilità, oggigiorno, grazie all'evoluzione tecnologica e all'avvento di un'infinità di applicazioni rivolte prevalentemente alla socializzazione e all'intrattenimento, sono diventati i contenitori di un'infinità di informazioni personali e professionali **in grado di raccontare la nostra vita**.

Per questo motivo **gli apparati mobili sono diventati oggetto di interesse** non solo dei provider di informazioni e di comunicazione, ma anche **degli esperti di sicurezza informatica**, che, rispondendo alle esigenze degli utenti, tentano di rendere protette e riservate le informazioni trasmesse e memorizzate, e parallelamente, su fronti opposti, **dei criminali e degli investigatori**, quest'ultimi a caccia di evidenze digitali per fini di giustizia.

Mobile Challenges

- Frammentazione del mercato
- Generazione di nuovi dispositivi
- Aggiornamenti continui dei sistemi operativi
- Passcode e cifratura
- Personalizzazioni utente
- Milioni di applicazioni
- Giga di dati
- Cloud
- …

Mobile Technology

Device

- Telefono cellulare
- Fotocamere digitali
- Smartphone o Tablet
- Smart watch o smart band
- Dispositivi Wearable
- Lettori Mp3
- Navigatori GPS
- Sistema Infotainment
- Droni
- Smart TV
- Assistenti Vocali
- IoT…

Communication

- TACS - ETACS
- GSM – GPRS - EDGE
- UMTS – HSPA+
- LTE / LTE-A
- 5G NR
- Wi-Fi
- WiMAX
- BLUETOOTH
- NFC
- IrDA

Mobile Technology

INDAGINI ONLINE

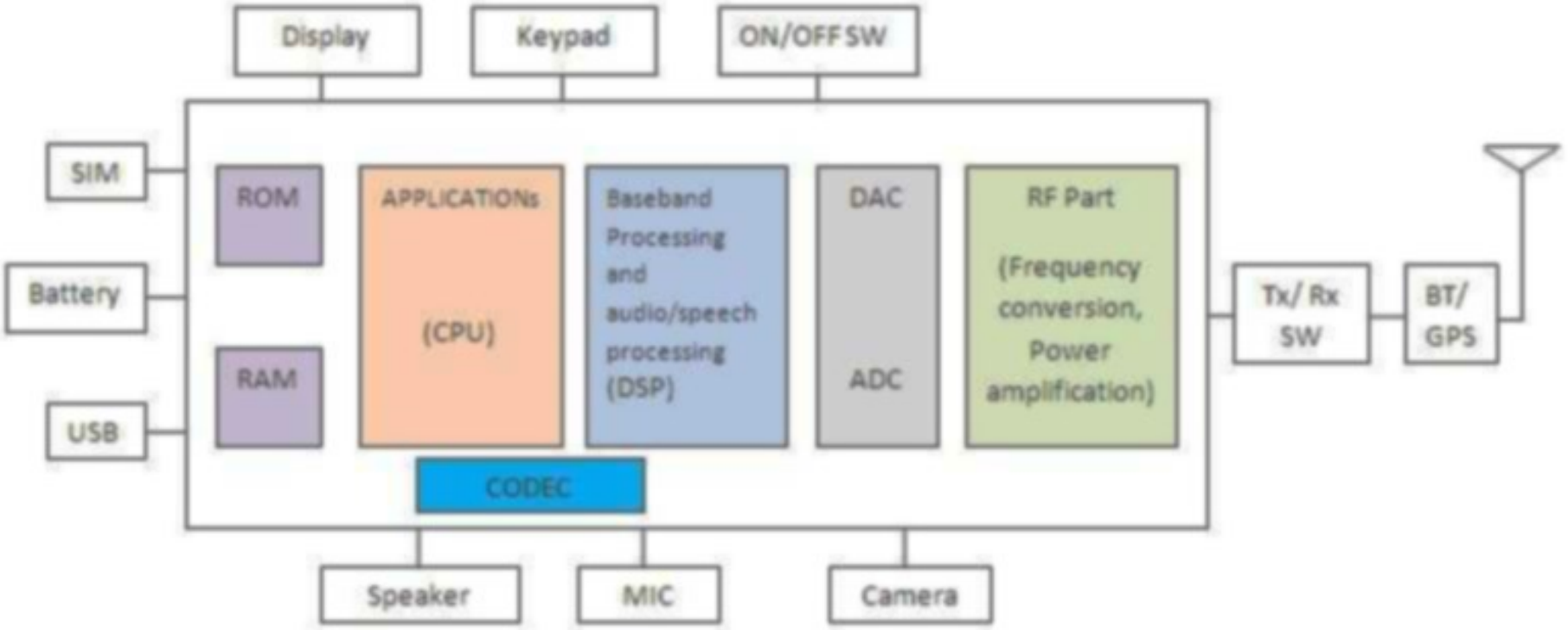
Mobile Technology - Hardware

	Basic Phone	Feauture Phone	Smartphone/Tablet
Processor	Limited Speed	Improved speed	Superior speed
Memory	Limited Capacity	Improved capacity (~5MB)	Superior capacity
Display	Grayscale	Small size color, 4k – 260k	Large size color, 16,7 million
Card Slots	None	None, MicroSD	MicroSDXC
Camera	None	Still, Video	Still, Panoramic and Video
Text Input	Numeric Keypad	Numeric Keypad QUERTY-style keyboard	Touch Screen, Handwriting Recognition, QUERTY-style keyboard
Voice Input	None	None	Voice Recognition (Dialing and Control)
Cell Interface	Voice and Limited Data	Voice and Limited Data	Voice and High Speed Data (4g e 5G)
Positioning	None	None, GPS receiver	GPS recevier
Wireless	IrDA	IrDA, Bluetooth	Bluetooth, WIFI and NFC
Battery	Fixed/Removable Rechargeable Li-Ion Polymer	Fixed/Removable Rechargeable Li-Ion Polymer	Fixed/Removable Rechargeable Li-Ion Polymer

Mobile Technology - Software

	Basic Phone	Feauture Phone	Smartphone/Tablet
OS	Proprietary	Proprietary	Android, BlackBerry OS, iOS, Symbian, WebOS and Windows Phone
PIM	Simple Phonebook	Phonebook and Calendar	Enhanced Phonebook, Calendar and Reminder List
Applications	None	MP3 Player, Notepad, Games	Applications (games, office, social media)
Call	Voice	Voice	Voice, Video
Messaging	Text Messaging	Text with Simple Embedded Images and Sounds MMS	Text Enhanced Text, Full Multimedia Messaging
Chat	None	SMS Chat	Enhanced Instant Messaging
Email	None	Via Network Operator's Service Gateway	Via POP e IMAP Server
Web	None	Via WAP Gateway	Direct HTTP

Mobile Technology



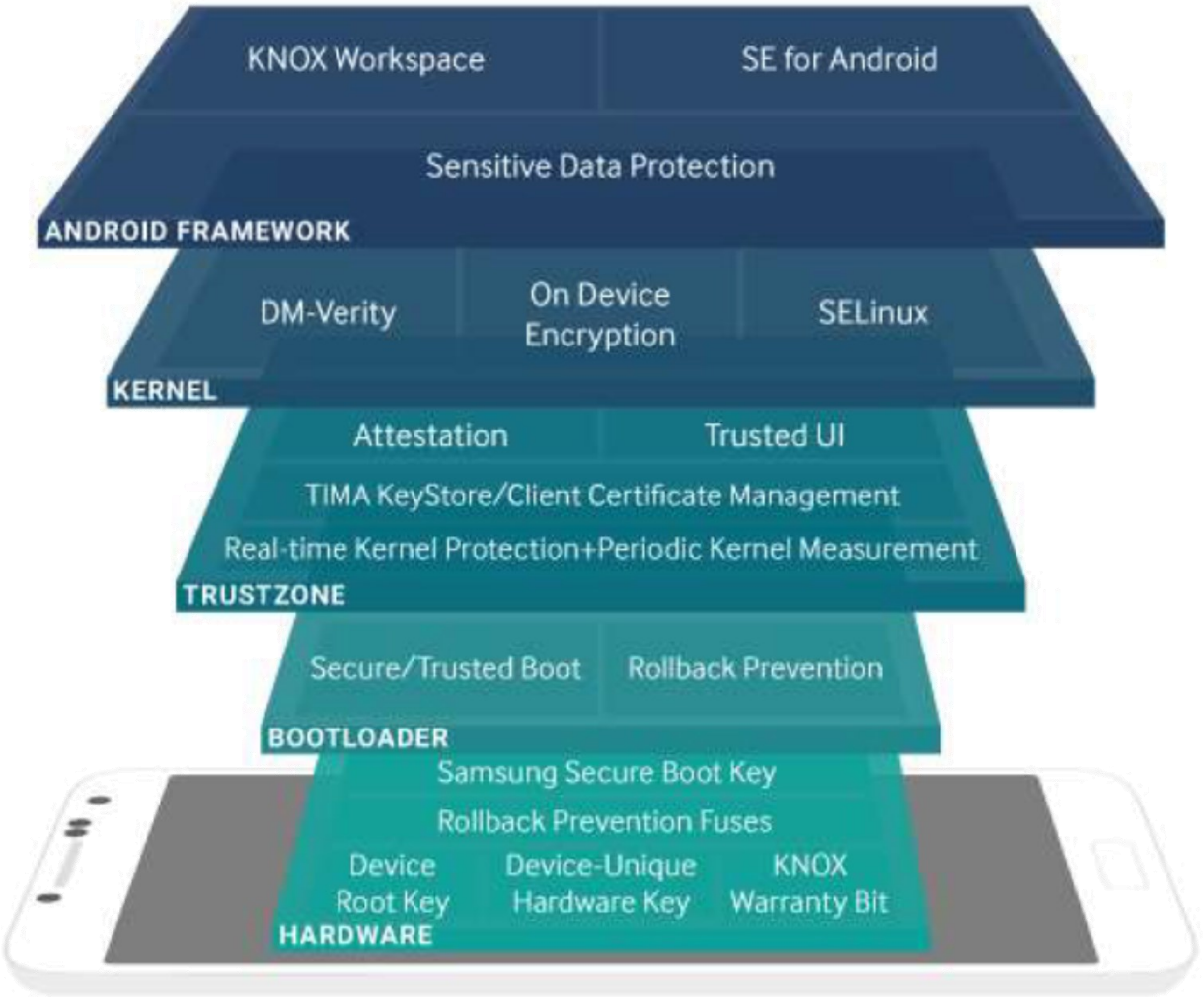
Mobile Phone block diagram

Mobile Technology

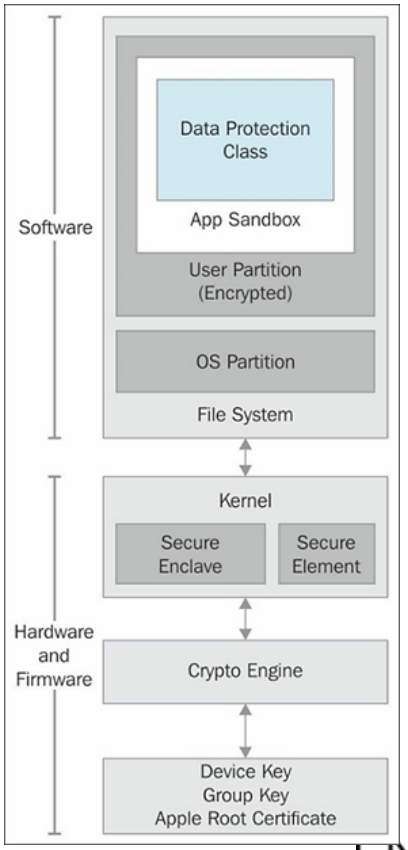
Elementi caratteristici del device mobile:

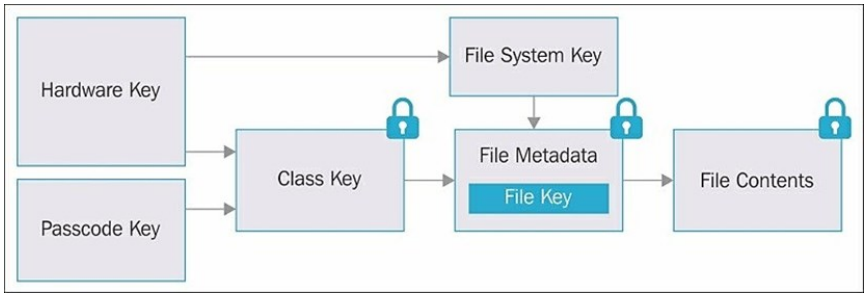
- **Firmware**
- **Sistema operativo**
- **Memoria interna per le app e i dati utente**
- **Microfono - Altoparlante**
- **Fotocamera**
- **Antenne** (GSM, UMTS, LTE, 5G, WIFI, Bluetooth, NFC, IrDA, ecc.)
- **Sensori** (GPS/Glonass, Accelerometro, Giroscopio, Magnetometro, Sensore di prossimità, Sensore di luminosità, Barometro, Lettore impronte digitali, Frequenza Cardiaca, SpO2 e VO2 Max, ecc.)
- **Touch screen**
- **SIM - Subscriber Identity Module**
- **Memoria esterna o aggiuntiva**
- **Dati sul cloud**

Samsung Knox Security Solution



Security architecture diagram of iOS





Mobile Technology

Dati che possono essere memorizzati:

- Chiamate entrata, uscita, perse
- Contatti
- Calendario
- Messaggi di testo
- Email
- Messaggi istantanei o chat
- Web pages
- Audio / Foto / Video
- Transazioni / Logs di varie Apps

Identificazione

L'identificazione delle specifiche del dispositivo è fondamentale perché ci consente di capire:

- Il modello di dispositivo
- Il sistema operativo installato di default
- Il processore
- Il tipo di memoria interna…

E, di conseguenza, **scegliere la metodologia di acquisizione** migliore, ovvero quella che consente di preservare il dato originale ed estrarre più informazioni possibili.

Alcune di queste informazioni permettono di selezionare la tecnica di acquisizione che sfrutta la vulnerabilità nota per una specifica configurazione (hardware e software).

Identificazione

IDENTIFICAZIONE DEL DISPOSITIVO:

- **Marca**
- **Modello number** *(in genere scritto sul retro del dispositivo*
- **Serial number** *o dietro la batteria)*
- **IMEI** *(si può ricavare digitando *#06#)*
- **Caratteristiche fisiche** (forma, dimensione, etc.)
- **Specifiche tecniche** (S.O., memoria, sistema sicurezza)
- **Stato del dispositivo**:
  - **acceso / spento**
  - **bloccato / sbloccato**
  - **integro / danneggiato**
  - **completo / incompleto**

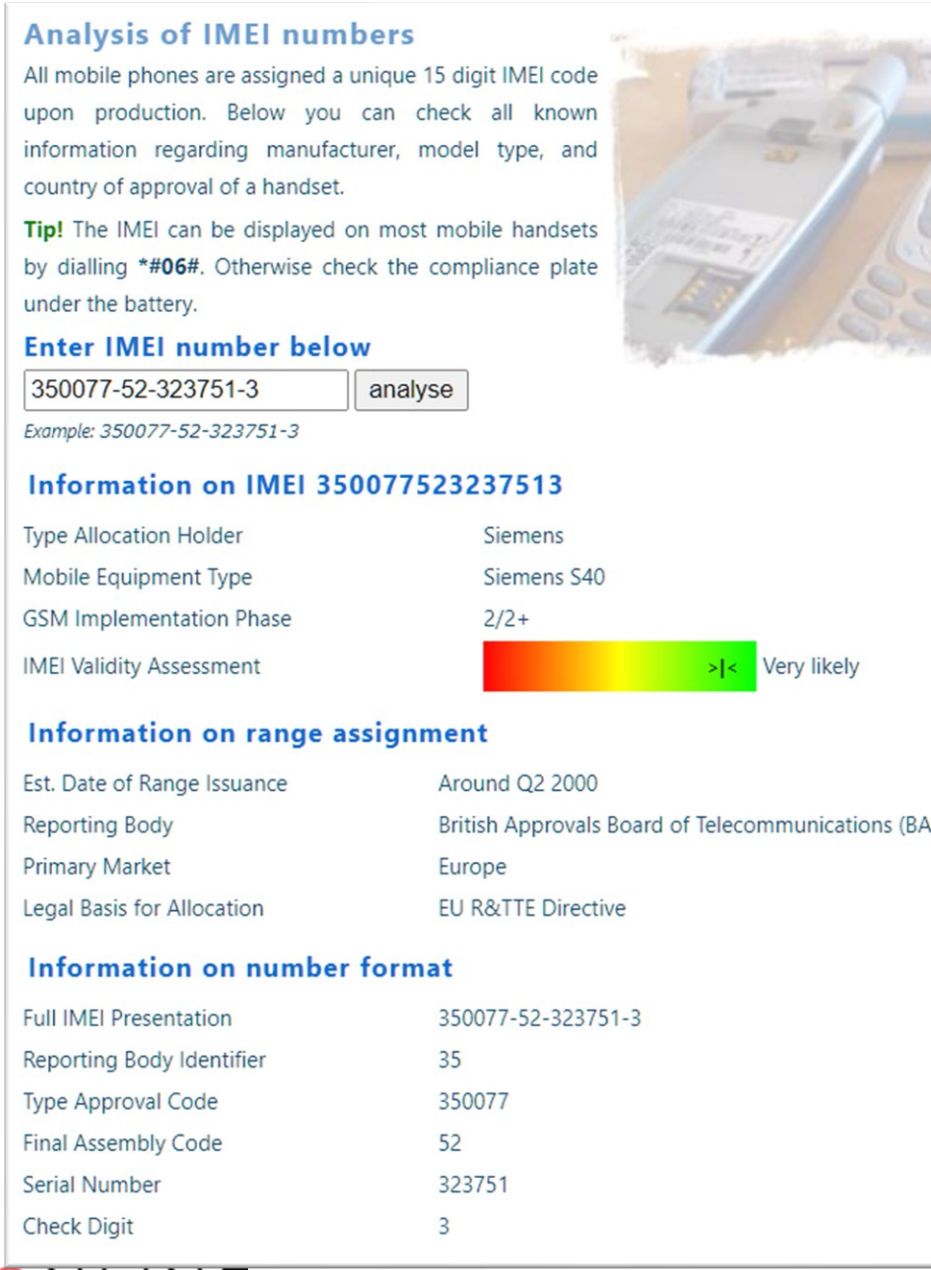
INDAGINI ONLINE

Identificazione

IMEI - International Mobile Equipment Identifier

I terminali radiomobili GSM sono caratterizzati da un codice di quindici cifre detto IMEI utilizzato per identificare il dispositivo all'interno della rete cellulare. Tale codice rappresenta in maniera univoca la casa costruttrice, il modello e la nazione in cui il terminale è stato prodotto.

http://www.numberingplans.com
http://www.trackimei.com



INDAGIN ONLINE

Identificazione

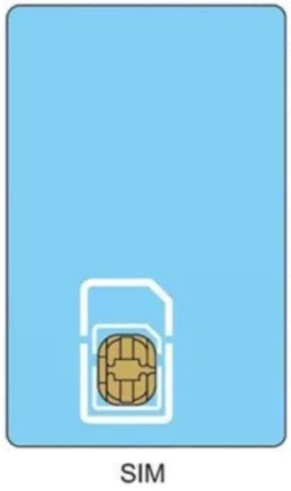
DEVICE IDENTIFICATION/INFORMATION

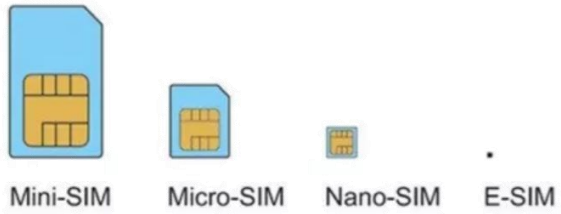
Website	URL
Firmware.mobi	https://desktop.firmware.mobi/
GSM Arena	https://www.gsmarena.com/
Hard Reset.info	https://www.hardreset.info/
IMEI.INFO	https://www.imei.info/
IMEIPRO	https://www.impeipro.info/
Numbering Plans	https://www.numberingplans.com/
PhoneDB	http://phonedb.net/
PhoneScoop	https://www.phonescoop.com/
Sammobile	https://www.sammobile.com/
The iPhone Wiki	https://www.theiphonewiki.com/

Identificazione

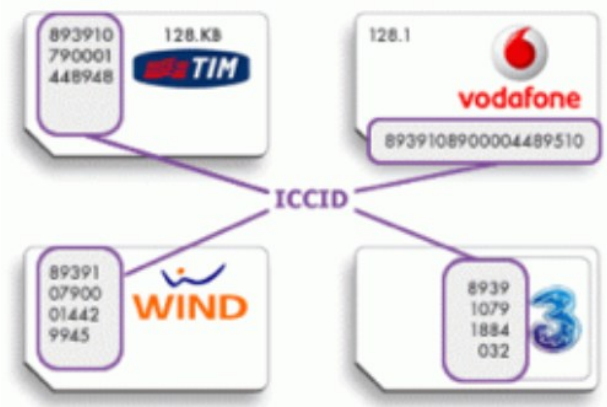
L'UICC (Universal Integrated Circuit Card), generalmente indicato come modulo d'identità (detto Subscriber Identity Module [SIM], Universal Subscriber Identity Module [USIM], CDMA Subscriber Identity Module [CSIM]), è un componente rimovibile contenete le informazioni relative al sottoscrittore del servizio mobile (utente). È composto di due codici:

- **ICCID (Integrated Circuit Card IDentification):** Codice lungo 20 cifre stampato sul dorso della scheda e la identifica univocamente
- **IMSI (International Mobile Subscriber Identity):** Codice lungo 15 cifre che identifica la coppia SIM-operatore telefonico





INDAGINI ONLINE



Identificazione

IDENTIFICAZIONE DELL'OPERATORE DA ICCID o IMSI:

Nel caso in cui fosse necessario identificare l'operatore di una SIM (scheda bloccata o per richiedere il codice PUK) si può utilizzare il portale **www.numberingplans.com**

Analysis of SIM card numbers

All mobile phone SIM cards have each been assigned a unique SIM card number. Below you can enter a SIM card number to check its validity as well as find out more about the mobile network that issued the chip.

Enter SIM card number below

8923440000000000003 analyse

Example: 8923440000000000003

Information on SIM card number

Network name	M-Tel
Operator name	Nigerian Mobile Telecommunications Ltd
Country or global network	Nigeria
MCC-MNC	621-40

Analysis of IMSI numbers

All mobile phone subscribers are assigned a unique 15-digit IMSI number to allow foreign mobile networks to identify subscribers from abroad. Below you can check the subscriber's home network, provided you know the IMSI.

Enter IMSI number below

262013564857956 analyse

Example: 262013564857956

Information on IMSI number range 26201XXXXXXXXXX

Country or destination	Germany
Network operator	T-Mobile Deutschland GmbH
Network name	T-Mobile D
Network status*	active

Identificazione

IDENTIFICAZIONE DELLE MEMORIE AGGIUNTIVE:

- Può contenere diversi dati essenziali:
  - fotografie, filmati, SMS, backup, Whatsapp, etc...
- In fase di sequestro: cercare tutte le memorie compatibili con gli slot del dispositivo
- L'esame può essere effettuata in parallelo, con gli strumenti della mobile forensics, o separatamente, con gli strumenti tradizionali per digital forensics.
- Non escludere che altre copie di backup siano state trasferite su altri dispositivi di memoria (pen drive, dischi esterni, ecc.)

Identificazione

COPIE DI BACKUP

- Possono essere presenti copia di backup del dispositivo su:
  - Personal computer
  - Cloud
  - SD card
  - Altre Memorie rimovibili
- Le copie di backup possono contenere informazioni cancellate non più rinvenibili dal dispositivo,
- oppure rappresentare l'unica fonte di dati per un dispositivo non rinvenibile o non funzionante o bloccato

Identificazione

DATI SUL CLOUD

- Il dispositivo può non contenere tutti i dati, ma i riferimenti per potervi accedere
- Valutare la presenza di client per Cloud come Dropbox, iCloud, Google Drive, Huawei cloud, Mi Cloud, Samsung, SkyDrive, etc...
- Attenzione perché in taluni casi (es. iCloud) permette all'utilizzatore di operare da remoto sul cellulare

Repertamento

Quando ci viene consegnato un dispositivo dobbiamo assicurarci che:

- **Non siano perse informazioni volatili**
- **Non sia compromessa la fase di acquisizione**
- **Non sia possibile alterare o cancellare il contenuto anche a distanza**
- **Non si attivino i sistemi di sicurezza che impediscono la successiva fase di acquisizione**
- **Sia valutata attentamente la scena del crimine**

Repertamento: preservation

Abbiamo quattro scenari:

1. Acceso e sbloccato
2. Accesso e bloccato
3. Spento, con codice
4. Spento, senza codice

Se conosciamo i codici di protezione possiamo procedere, altrimenti dobbiamo fare qualcosa.

P.e. Sui dispositivi IOS è utile acquisire l'identificato UDID e cercare, su altri dispositivi, un certificato recente di lockdown (***device_UDID.plist***)

Repertamento: preservation

Se il dispositivo è spento:

- lasciarlo spento
- sequestrare anche eventuali schede di memoria e la batteria (per risparmiarsi problemi in seguito se disponibili prendere anche cavetti, caricabatteria, confezione SIM, software, etc...)
- documentare lo stato del telefono (foto)
- non lasciare la batteria all'interno o isolarla per evitare che si accenda inavvertitamente o suoni la sveglia o si possa accendere su timer

Repertamento: isolamento

Se il dispositivo è acceso:

- Mantenerlo acceso con una powerbank, ma isolato da tutto (jammer, gabbia di faraday, airplane mode)
- Documentare data/ora ed eventuali info su display, valutare possibile encryption o lock
- Se si dispone dei codici di sblocco spegnerlo, altrimenti ragionare!!!

Repertamento: collection

E' fondamentale riuscire a:

- Procurarsi i codici di sblocco del dispositivo e, se possibile, disabilitare i sistemi di protezione
- Disabilitare l'autenticazione biometrica
- Procurarsi i codici PIN e PUK della SIM
- Procurarsi eventuali credenziali di accesso al Cloud
- Se il dispositivo è collegato ad un computer, o si acquisisce che lo sia stato in passato, repertare anche il computer perché potrebbe contenere informazioni correlate al dispositivo
- Imballaggio, trasporto e conservazione sicuro

Acquisizione

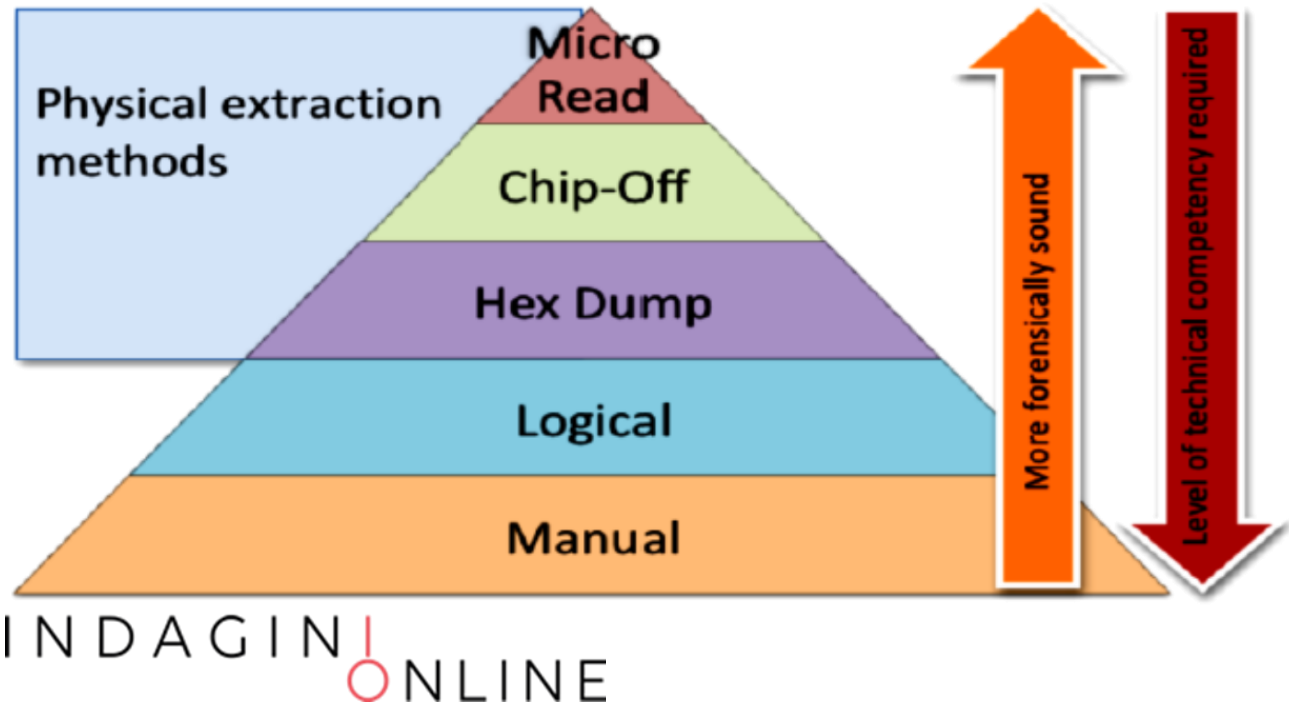
L'acquisizione è il processo che consente di ottenere l'immagine o, in alternativa, le informazioni da un dispositivo mobile e dai supporti di memoria associati.

Se si esegue un'acquisizione sulla scena del crimine si ottiene il vantaggio di evitare la perdita di informazioni a causa dell'esaurimento della batteria, oppure per i danni che possono sopravvenire durante il trasporto e lo stoccaggio.

Le acquisizione on-site, a differenza di quelle effettuate in laboratorio, possono essere più complicate a causa dell'assenza di un ambiente dedicato in cui lavorare con un'attrezzatura adeguata e che soddisfa ulteriore prerequisiti.

Metodi di acquisizione

- **Manual Extraction**
- **Logical Extraction / File System**
- **Hex Dump / JTAG**
- **Chip-Off**
- **Micro Read**



Metodi di acquisizione

Prima di procedere all'acquisizione dobbiamo stabilire in quale scenario siamo e identificare con precisione le caratteristiche del dispositivo:

- Dispositivo acceso o spento?
- Dispositivo sbloccato o bloccato?
- Dispositivo con sistema di cifratura?
- Dispositivo di cui conosciamo le credenziali di accesso?

L'ultima domanda è importante poiché dobbiamo ricordare che, nonostante siano disponibili tecniche di hacking che ci consentono di bypassare le misure di sicurezza impostati dall'utente, dobbiamo assolutamente preservare la genuinità del dato presente all'interno della memoria del dispositivo.

Per cui, se ci trovassimo in questa situazione dobbiamo:

1. Chiedere espressamente l'autorizzazione ad usare le tecniche di hacking
2. Informare il committente delle alternative e quali rischi stiamo accettando
3. Utilizzare procedure testate e, se possibile, provarle prima su un clone

Metodi di acquisizione

MANUALE:

- Il metodo di estrazione manuale consiste nel visualizzare i dati memorizzati sul dispositivo e memorizzarla sottoforma di screenshot o filmato
- Si usa quando non è possibile acquisire i dati in altro modo
- Non è possibile rinvenire le informazioni cancellate
- È un metodo che comporta un dispendio notevole di tempo
- Durante l'interrogazione le informazioni possono essere modificate, cancellate o sovrascritte
- La lingua impostata sul device deve essere conosciuta dall'investigatore

Metodi di acquisizione

Esempio di Acquisizione MANUALE:

- Si possono utilizzare i software per il mirroring dello schermo del dispositivo su una postazione connessa tramite cavo o wireless (wi-fi o bluetooth):
  - AirDroid e Air Mirror (android)
  - Vysor
  - Scrcpy (android)
  - MirrorGo (android e ios)
  - LetsView (mirrorcast e airplay)
- Acquisire di dati collegando il dispositivo ad una postazione forense cavo o wireless
- Acquisire i dati tramite web o app installata su PC:
  - WhatsApp
  - Instagram
  - Facebook

Metodi di acquisizione

LOGICA:

- Attraverso funzionalità del sistema operativo o tramite agent
- Estrazione dei dati visibili ed esposti dal sistema operativo
- Non recupera i files cancellati
- Non recupera i dati protetti (WA, FB, TW)
- Tipicamente è necessario avere il dispositivo sbloccato
- Si collega il dispositivo ad una postazione forense
  - Wired (USB RS-232)
  - Wireless (IrDA, Bluetooth, WiFi)

Metodi di acquisizione

FILE SYSTEM:

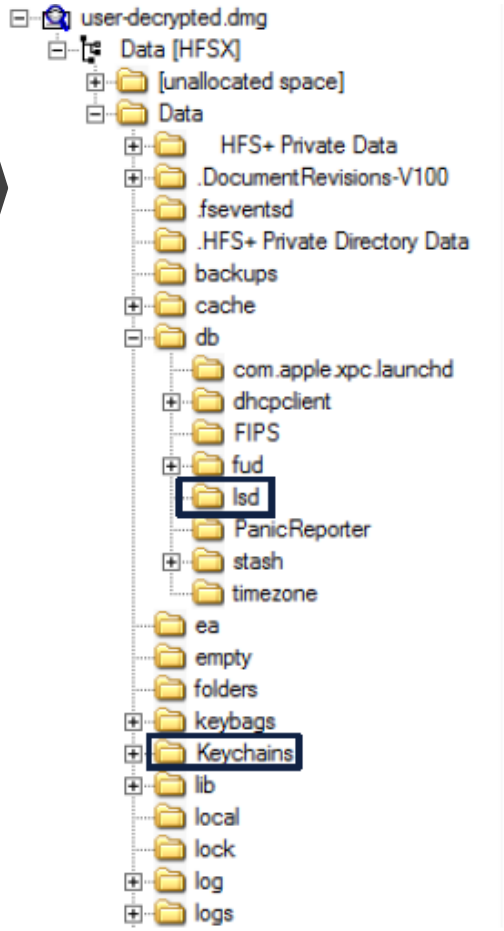
- È un tipo di acquisizione logica più completa
- Si può eseguire attraverso:
  - Funzionalità di backup del dispositivo
  - Vulnerabilità/funzionalità dello specifico sistema
  - Rooting/Jailbreaking (per ottenere i permessi di amministratore)
  - Flashing delle partizioni (dove non sono presenti dati utente)
- L'accesso ai dati dipende se si ottiene un **partial file system** oppure una **full file system**
- Permette di recuperare i contenuti cancellati presenti all'interno di altri file (es. record cancellati in database SQLite)
- Tipicamente necessario avere il dispositivo sbloccato, tranne in caso di specifiche vulnerabilità

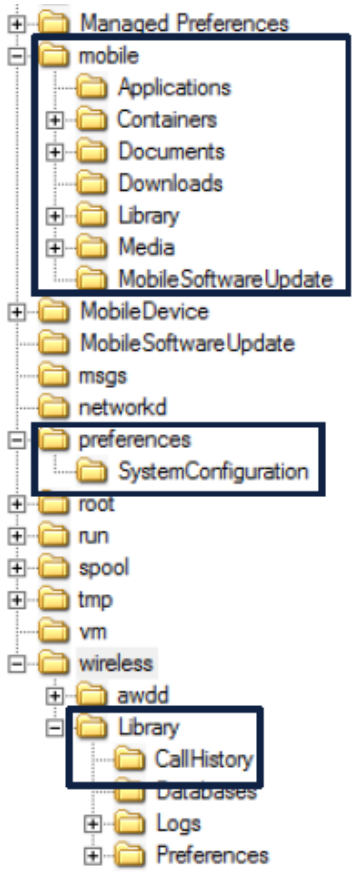
Metodi di acquisizione

Differenze di acquisizione tra:

- partial file system

- full file system





INDAGINI ONLINE

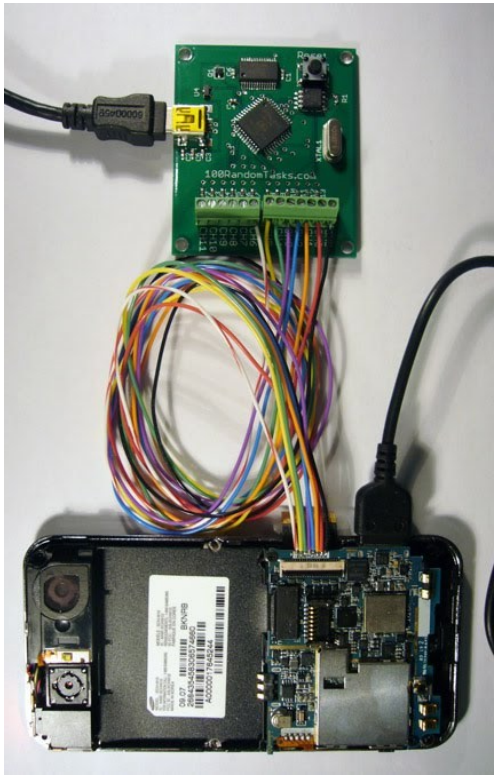
Metodi di acquisizione

HEX DUMPING / JTAG:

- Si può eseguire attraverso:
  - Vulnerabilità/funzionalità dello specifico sistema
  - Rooting/Jailbreaking (per ottenere i permessi di amministratore)
  - Approccio diretto sul dispositivo (JTAG/ISP/Chip-Off)
  - Contro: file system cifrato
- Contiene l'intera struttura di partizioni e file system del dispositivo
- Permette di recuperare:
  - I contenuti cancellati presenti all'interno di altri file (es. record cancellati in database SQLite)
  - I files cancellati all'interno del dispositivo (carving)

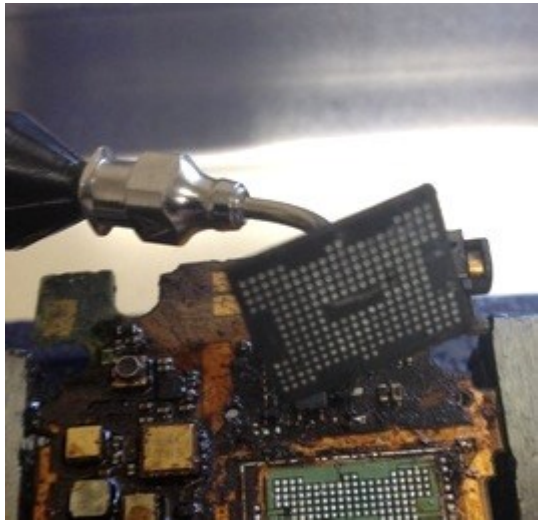
Metodi di acquisizione

JTAG
Joint Test Action Group



ISP
In-System Programming

CHIP-OFF



INDAGINI ONLINE

Metodi di acquisizione

MICRO READ

La tecnica Micro Read consiste nell'osservazione fisica delle porte NAND e NOR del chip attraverso l'uso di un microscopio elettronico.

A causa delle difficoltà estreme che comporta lo svolgimento di una lettura Micro Read, questa tecnica di acquisizione è utilizzata solo per i casi di alto profilo equiparati ad una crisi della sicurezza nazionale e dopo che sono state escluse tutte le altre tecniche di acquisizione. Per questo tipo di intervento occorre un team di esperti, l'attrezzatura adeguata, il tempo e la conoscenza approfondita delle informazioni riservate.

Attualmente non c'è in commercio un tool per applicare questa tecnica.

Metodi di acquisizione

Una volta che è stato identificato il dispositivo occorre scegliere la metodologia più adatta.

- Verificare il supporto da parte dei tools di Mobile Forensics
- Provare per prima le metodologie meno invasive o che siano già state verificate
- Identificare metodologie alternative (*)
- Individuare specifiche vulnerabilità il cui sfruttamento non è implementato nei tools (*)
- Valutare la possibilità di approcci fisici (*)

(*) Ricordarsi che la fonte di prova deve essere preservata, quindi se occorre effettuare tentativi di exploit non vanno eseguiti sul dispositivo originale, ma su un «muletto» e prima di attuarli sul dispositivo originale occorre farsi autorizzare dal proprietario o dall'Autorità competente.

Selezione degli strumenti

I seguenti criteri sono suggeriti come l'insieme di requisiti che gli strumenti devono garantire per l'applicazione forense:

- **Usabilità**: la possibilità di presentare i dati in un formato utile all'investigatore
- **Completezza**: la possibilità di presentare tutti i dati in modo che possano essere identificati, contemporaneamente, gli elementi a carico e discarico
- **Precisione**: sono stati testati i risultati dello strumento
- **Deterministico**: la possibilità di produrre lo stesso output dallo stesso insieme di istruzioni e di input
- **Verificabile**: la possibilità di garantire la precisione dell'output, avendo accesso alla traduzione intermedia ed ai risultati della presentazione
- **Testato**: la possibilità di determinare se, noti i dati presenti nella memoria interna del dispositivo mobile, questi non vengano modificati e riportati con precisione dallo strumento

Framework di acquisizione

Il National Institute of Standards and Technology (NIST) ha avviato il progetto **Computer Forensics Tool Testing (CFTT)**

Open/Free:

- Android SDK
- Xda-developers.com
- Twrp
- CF-Auto-Root
- SuperSU
- Smart Phone Flash Tools
- Andriller
- AFLogical
- Autopsy
- iTunes
- SQLite Browser
- Plist Editor
- WpInternals

Commerciali:

- Cellebrite UFED4PC / Physical Analyzer
- Oxygen Forensics
- Magnet Axiom
- Elcomsoft Phone Breaker
- Elcomsoft iOS Forenics Toolkit
- Elcomsoft Cloud Explorer
- Blackbag Blacklight Mobilyze
- Scanderson SQLite Forenisic Browser
- MSBA XRY
- Mobiledit
- SPF Pro (SmartPhone Forensic System Professional)

Metodi di acquisizione

CARATTERISTICHE DI UNA SIM

Acquisizione dei dati memorizzati nella SIM

Informazioni utili da recuperare:

- ICCID
- IMSI
- Ultima cella agganciata
- Elenco chiamate
- Rubrica
- SMS (anche cancellati)

Se protetta tramite PIN sconosciuto, chiedere il PUK al Gestore

Metodi di acquisizione

ACQUISIZIONE E CLONAZIONE DELLA SIM

I principali software disponibili per la SIM sono:

- **Paraben SIM Card Seizure (commerciale)**
- **SIMiFOR - http://www.forensicts.co.uk/ (commerciale)**
- **SIMcon - http://www.simcon.no/ (commerciale)**
- **USIM Detective - http://www.quantaq.com (commerciale)**
- **Dekart SIM Manager - http://www.dekart.com (commerciale)**
- **SIMSpy2 - http://www.nobbi.com/ (freeware)**
- **Tulp2G - http://tulp2g.sourceforge.net/ (freeware)**

Metodi di acquisizione

CARATTERISTICHE DI UNA SD-CARD

Può essere acquisita insieme al dispositivo d'origine oppure direttamente con un software di clonazione come FTK-Imager.

All'interno è possibile recuperare dati utente quali:

- Immagini, video, audio
- App installate dall'utente
- Database delle app
- Backup

L'analisi è di norma effettuata insieme alla copia del dispositivo

Metodi di acquisizione

BACKUP

La funzionalità di backup può variare per il tipo di supporto di destinazione:

- **Backup su memorie esterne**: con questa terminologia si identificano quelle copie dei dati effettuate direttamente dal dispositivo d'origine su schede o dispositivi di memoria collegati allo stesso. Questa opzione è preferita nel caso si desideri spostare velocemente i dati da un dispositivo ad un altro;
- **Backup o sincronizzazione su PC**: con questo tipo si individuano quelle copie effettuate attraverso appositi programmi di sincronizzazione (Apple iTunes, Nokia PC Suite, Samsung Kies, Microsoft ActiveSync), presenti contemporaneamente sul terminale sorgente e su quello di destinazione, e consentono di effettuare backup o ripristino dei dati in entrambi i versi. Questa operazione è preferita nel caso in cui si desidera effettuare una copia sicura dei dati, eventualmente protetta da password, o per elaborarli in formati diversi;
- **Backup su Cloud storage**: la presenza di connettività ad Internet sempre attiva e veloce ha permesso la diffusione di quest'altro tipo di backup che consiste nel copiare o trasferire i dati dal dispositivo su uno spazio di archiviazione online. Spesso lo spazio è offerto dalla stessa casa madre del s.o. installato sul dispositivo (p.e. Apple iCloud, Google Drive, Microsoft OneDrive), l'accesso è protetto da credenziali e i dati vengono cifrati. Questa funzionalità è molto apprezzata da parte degli utenti perché, rispetto alle altre, non richiede nessun accessorio aggiuntivo ed avviene in maniera del tutto automatica.

Metodi di acquisizione

BACKUP

- iTunes (Apple)
- Microsoft ActiveSync
- BlackBerry Desktop Manager (BB Link)
- Nokia Suite
- Samsung Kies
- HiSuite (Huawei)
- Mi PC Suite (Xiaomi)
- MOBILedit Forensic Express

Metodi di acquisizione

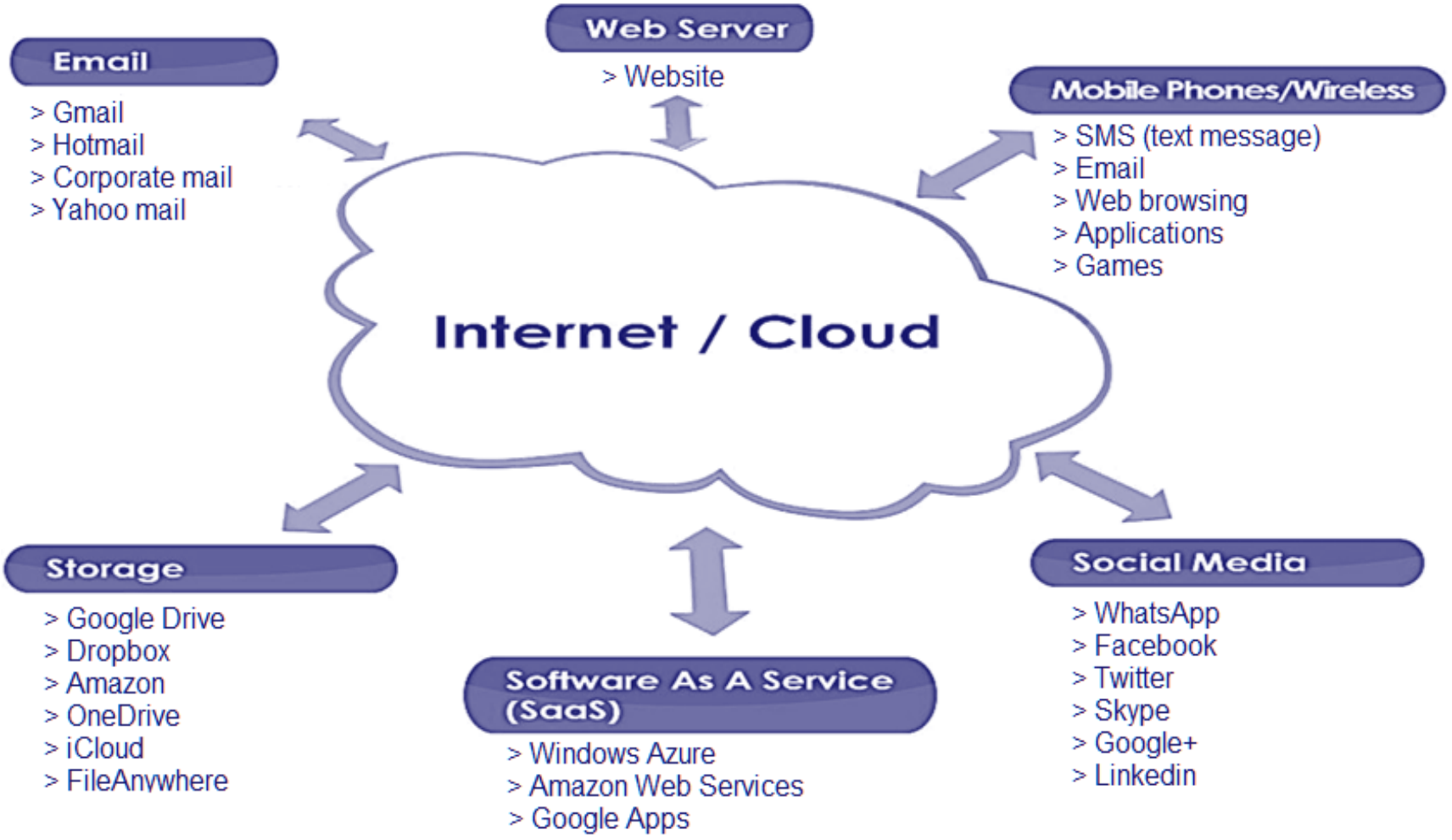
CLOUD STORAGE

I maggiori produttori di smartphone o di mobile app forniscono uno spazio di archiviazione per estendere la memoria del dispositivo o per effettuare il backup dei dati.

Accedendo a tale spazio di memoria, sia tramite il dispositivo stesso, oppure utilizzando le credenziali di autenticazione, è pertanto possibile acquisire:

- Il backup dei dati del dispositivo (produttore del dispositivo)
- Una copia di backup dei dati utente (piattaforma dell'app)

Metodi di acquisizione



Metodi di acquisizione

CLOUD STORAGE

L'acquisizione può essere effettuata:

- Direttamente dal dispositivo su cui sono registrate le credenziali di accesso
- Dall'interfaccia WEB del provider (Grazie, soprattutto, al GDPR)
- Tramite software di analisi forense che sfruttano le WEB API messe a disposizione del provider

Metodi di acquisizione

CAPTATORE INFORMATICO

Il captatore informatico è un malware che costituisce, per le forze di polizia e per la magistratura (???), uno strumento in grado di bypassare i sistemi di cifratura dei sistemi e delle app.

Esso viene inoculato negli smartphone e nei personal computer e, in base alle norme in vigore, può attivare il microfono per ascoltare le conversazioni, geolocalizzare lo smartphone, attivare la telecamera e scattare le foto, leggere il contenuto della memoria all'insaputa dell'indagato.

In realtà è in grado di fare moltissime altre attività (tecnicamente impossibili con altri strumenti meno invasivi)
che la legge non prevede e non disciplina.

Inoltre, non viene gestito in prima persona sempre e solo da ufficiali di polizia giudiziaria ma da società private (???).

Rientra tra i metodi di captazione da remoto.

Analisi

Il processo di ricerca consente di trovare le prove digitali, comprese quelle nascoste o bloccate.

I risultati ottenuti, attraverso l'applicazione di metodi scientificamente provati, dovrebbero descrivere in maniera completa il contenuto, lo stato dei dati, la fonte ed il loro potenziale significato.

Una volta che tutti i dati sono stati estratti, si può procedere alla loro riduzione effettuando la separazione dei dati pertinenti dalle informazioni irrilevanti.

Il processo di analisi differisce dalla ricerca in quanto considera i risultati della ricerca per il loro significato ed il valore probatorio che possono assumere per il caso.

Analisi: la regola delle 6 W

LE "6" W / I DATI	WHO	WHAT	WHERE	WHEN	WHY	HOW	
Identificativi intestatario o dispositivo	■						ALL PHONE
Registri di chiamate	■			■			
Rubrica	■						
Calendario	■	■	■	■	■	■	
Messaggi	■	■	■	■	■	■	
Messaggi chat / mail	■	■	■	■	■	■	SMARTPHONE
Localizzazione spaziale			■	■			
Weburl / Contenuti web	■	■	■	■	■	■	
Immagini/Audio/Video	■	■	■	■			
Altri dati	■	■	■	■	■	■	

INDAGINI ONLINE

Analisi

Il Dipartimento di Giustizia Americano ha realizzato la **Forensic Examination of Digital Evidence – A Guide for Law Enforcement** con cui evidenzia i seguenti suggerimenti utili all'analisi dei dati estratti:

- **Proprietario e utilizzatore**: Identifica le persone che hanno creato, modificato o acceduto un file; chiarisce il dubbio di chi, tra proprietario e utilizzatore, abbia utilizzato il dispositivo in una particolare data; localizza i file di interesse in posizioni non predefinite; recupera le password che indicano utente o proprietario; identifica il contenuto dei file specifici di un utente.
- **Analisi delle applicazioni e dei file**: Identifica le informazioni rilevanti all'indagine, attraverso l'esame del contenuto dei file; correla i files alle applicazioni installate; individua le relazioni tra files (per esempio e-mail con allegati); determina il significato dei tipi di file sconosciuti; verifica le impostazioni di configurazione del sistema; analizza i metadati del file;
- **Analisi temporale**: Attraverso l'esame dei file di log e delle date e ore presenti sul file system si può determinare quando si sono verificati determinati eventi sul sistema, in modo da poter associare l'utilizzo con un determinato individuo. A tal fine possono rivelarsi utili anche i registri delle chiamate, le date e le ore contenute nei messaggi e nelle e-mail. (Questi ultimi possono essere confermati anche con i tabulati del fornitore del servizio);
- **Analisi dei dati nascosti**: Individuare e recuperare i dati nascosti può aiutare a approfondire le conoscenza, il proprietario e il movente; accedere ai file cifrati o protetti da password; accedere alla immagini trattate con la steganografia; accedere allo spazio non allocato del file system.

Analisi

I passi che solitamente si posso intraprendere sono:

- Verificare la configurazione del dispositivo e le app installate
- Interpretare i database (SQLite, Plist) di sistema, delle app native e di quelle installate dall'utente
- Rinvenire le informazioni di interesse
- Recuperare eventuali informazioni cancellate
- Ricostruire la timeline
- Connettere i contatti di più dispositivo (voice, sms, chat)
- Vedere i log delle app di interesse
- Verificare la presenza di malware

Consultare il paper: **for585.com/course**

INDAGINI ONLINE

Tools di analsi

Open/Free:

- **APOLLO** Apple Pattern of Life Lazy Output'er
  https://github.com/mac4n6/APOLLO
- **iLEAPP** iOS Logs, Events, And Properties Parser
  https://github.com/abrignoni/iLEAPP
- **iOS-Mobile**- iOS installation and uninstallation
  https://github.com/abrignoni/iOS-Mobile-Installation-log parser
- **iOS Triage** Incident response tool for iOS devices
  https://github.com/ahoog42/ios-triage
- **fplist** Converts plist files to json,
  https://www.hack42labs.com/tools/fplist/details/
- **iOS_sysdiagnose_** Scripts for parsing various iOS
  https://github.com/cheeky4n6monkey/iOS_forensic_scripts
- **ALEAPP** Android Logs Events & Protobuf Parser
  https://github.com/abrignoni/ALEAPP
- **Android Parser** for Android Usagestats files in
  https://github.com/abrignoni/Android-Usagestats-XML-Protobuf
- **ftree** Identifies, hashes and destructures all
  https://www.hack42labs.com/tools/ftree/details/
- **FAPK** Extracts apk files from an https://www.hack42labs.com/tools/fapk/
- **DFIR-SQL-REPO** Collection of SQL query templates
  https://github.com/abrignoni/DFIR-SQL-Query-Repo
- **SQLite-Deleted**- Recovers deleted entries from
  https://github.com/mdegrazia/SQLite-Deleted-
- **SQLECmd** Automates the identification and
  https://github.com/EricZimmerman/SQLECmd
- **sqlite_miner** Mines SQLite databases for BLOBs and
  https://github.com/threeplanetssoftware/
- **4n6-scripts** Collection of forensic and third-party scripts
  https://github.com/cheeky4n6monkey/4n6-scripts

Commerciali:

- Cellebrite UFED4PC / Physical Analyzer
- Oxygen Forensics
- Magnet Axiom
- Elcomsoft Phone Breaker
- Elcomsoft iOS Forenics Toolkit
- Elcomsoft Cloud Explorer
- Blackbag Blacklight Mobilyze
- Scanderson SQLite Forenisic Browser
- MSBA XRY
- Mobiledit Forensic Express
- SPF Pro (SmartPhone Forensic System Professional)

Analisi

DATI DAL CLOUD

Se siamo stati in grado di estrarre di dati dai profili social associati al dispositivo possiamo ricavare:

- Informazioni cancellate o non presenti sul dispositivo
- Informazioni provenienti da altri dispositivi associati
- Informazioni sulla localizzazione del dispositivo

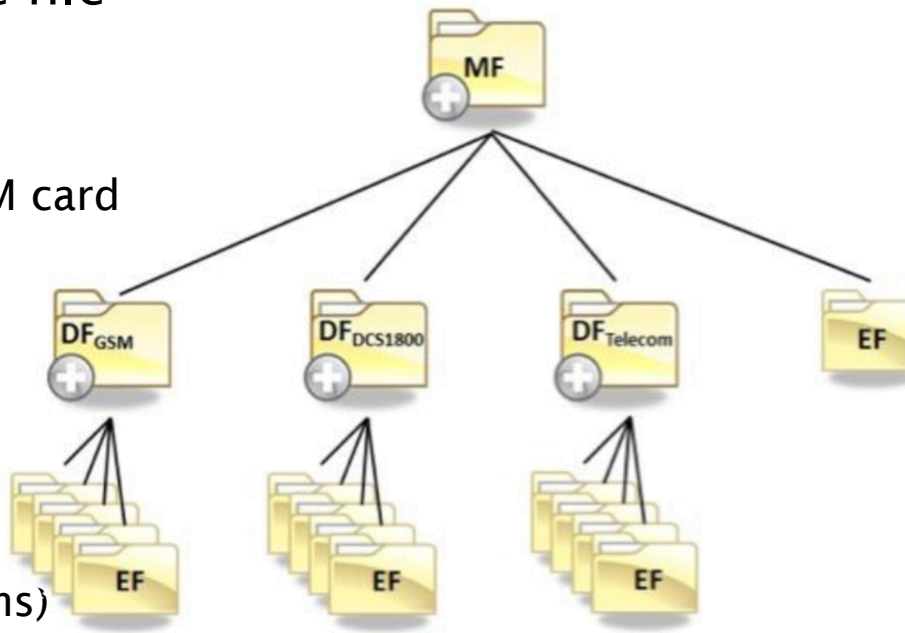
Analisi

STRUTTURA DATI DI UNA SIM

È un “File system” con una struttura ad albero n-ario

Contiene tre tipologie di strutture file

- MF – Master File
  - Composto da un header
  - E’ la radice del file system della SIM card
- DF – Dedicated
  - File Composto da un header
  - una directory
- EF – Elementary File
  - Composto da header + body
  - Rappresenta il file (es. contatto, sms)



MF - Master File (root and main container of DF and EF)
DF - Directory File
EF - Elementary File

Analisi

TABULATI

Spesso l'analisi forense avente ad oggetto un dispositivo mobile si incrocia con l'analisi forense dei tabulati telefonici del gestore

Tale incrocio è utile a corroborare le informazioni contenute:

Per esempio è possibile:

- Integrare il registro delle chiamate
- Confutare la genuinità di un messaggio chat
- Migliorare la localizzazione del dispositivo
- Arricchire la timeline di utilizzo del dispositivo

Contatti

info@vincenzocalabro.it

Linkedin vincenzocalabro

INDAGINI ONLINE