
# Corso di Digital Forensics

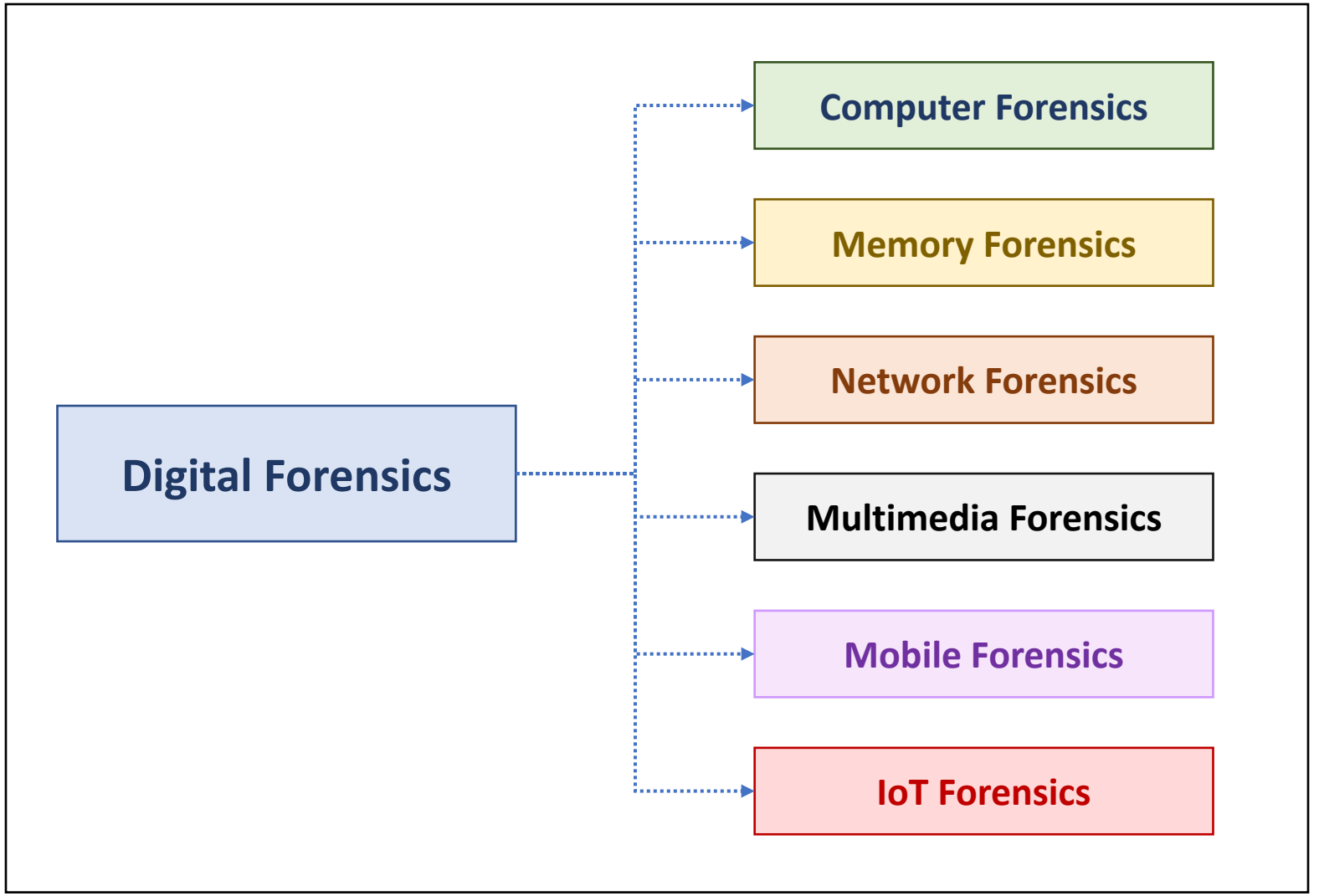
CdLM in Informatica

Università degli Studi di Salerno

Docente: Ugo Fiore

6bis – Mobile Forensics

# Principali branche della Digital Forensics



# Device mobili

- Telefoni
- Tablet
- PNA (navigatori)
- MP3 player
- Fotocamere/videocamere
- registratori digitali
- Vehicular «Black-box»
- etc...

# Componenti di un mobile device

- Device (marca, modello, serial number)
- SIM Card
- Flash Card (Memoria interna)
- Mass Storage (Mem. esterna)
- Cloud (Dropbox, iCloud, GDrive, etc...)

In particolare ci concentriamo sui telefoni

# Identificazione del dispositivo

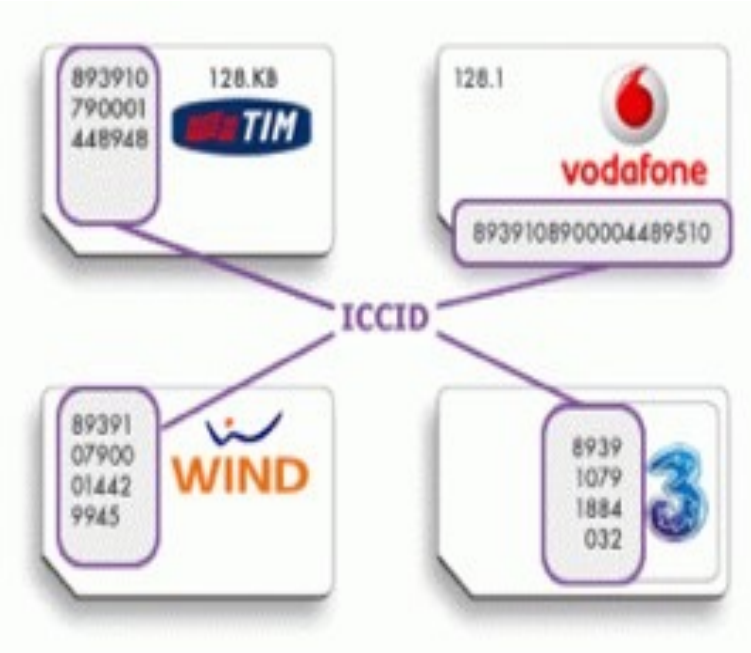
- International Mobile Equipment Identifier (IMEI)
- scritto all’interno del dispositivo, dietro  la batteria
- Se il telefono è acceso, si può ricavare dall’IMEI (codice *#06#”)
- Valore univoco attribuito al cellulare sulla rete
- www.numberingplans.com, www.trackimei.com

# SIM Card

- Subscriber Identity Module (SIM)
- Permette il collegamento del dispositivo con la rete GSM/3G/4G/5G
- Due codici: ICCID (Integrated Circuit Card IDentification) e IMSI (International Mobile Subscriber Identity)
- Sempre meno utilizzata nei dispositivi mobili per memorizzare dati rilevanti (es. quasi tutti non memorizzano più la rubrica sulla SIM)

# ICCID (Integrated Circuit Card IDentification)

- XX (prime due cifre): codice standard per l'identificazione di un sistema con scopi di telecomunicazione (89 per l'Italia)
- XX (terza e quarta cifra): 39 solo per l'Italia, corrisponde al prefisso internazionale assegnato al paese in cui opera dato gestore e varia a seconda delle nazioni
- XX(X) (due o tre cifre): codice identificativo del gestore, così suddiviso: 01 TIM, 10 Vodafone, 88 Wind, 99 H3G, 007 Noverca e 008 Fastweb
- XXXXXXX (tutte le cifre restanti fino alla fine del codice ICCID): identificativo del singolo chip



# International Mobile Subscriber Identity (IMSI)

- Codice che identifica una coppia SIM-operatore telefonico, ossia la SIM in una rete GSM
- lungo 15 cifre e così strutturato:
  - XXX - MCC (Mobile Country Code), 222 per l'Italia.
  - XX - MNC (Mobile Network Code), l'identificativo della compagnia telefonica in rete. Coincidono con quelli presenti sull'ICCID (01 TIM, 10 Vodafone, 88 Wind, 99 H3G, 007 Noverca e 008 Fastweb);
  - XXXXXXXXXX - MSIN (Mobile Subscriber Identification Number), un numero univoco che identifica ciascuna utenza.

# Memoria aggiuntiva (SD Card)

- Può contenere diversi dati essenziali: fotografie,  filmati, SMS, backup, Whatsapp, etc...
- Si può analizzare con gli strumenti convenzionali


# Fasi preliminari (1/2)

- Mettere in sicurezza il telefono
- Non permettere a nessuno di operare sul dispositivo
- Annotare eventuali problemi fisici evidenti riscontrati (per esempio display rotto)
- Fotografare tutti gli aspetti esterni del telefono
- Documentare tutte le azioni intraprese
- Verificare lo stato del telefono (acceso o spento)
- Se è spento lasciarlo spento

# Fasi preliminari (2/2)

- Se è acceso
- Documentare le informazioni presenti sullo schermo del dispositivo
- Se possibile registrare data e ora del dispositivo verificandone l'eventuale scarto rispetto all'ora reale
- Non navigare nel menu o aprire alcun messaggio in questa fase
- Mantenerlo acceso, isolandone l'accesso alle diverse reti

# Isolamento dalle reti

- Esistono almeno 3 tecniche per isolare un dispositivo in fase di repertamento:
  - Jammer (disturbo radio sulle frequenze di funzionamento)
  - Gabbia di Faraday (appositi contenitori/buste)
  - Airplane mode

# Isolamento o spegnimento?

- Lo spegnimento del dispositivo potrebbe attivare il codice di autenticazione del telefono (es. il PIN della scheda SIM oppure il codice di sblocco del telefono). In alcuni casi questi codici potrebbero essere molto complessi o impossibili da recuperare, rendendo quindi di fatto impossibile un'analisi forense
- L'isolamento del telefono mediante jammer o gabbia di Faraday comporta un maggior consumo di batteria da parte del dispositivo che cercherà di connettersi (senza successo) alla rete. Queste tecniche devono quindi essere accompagnate dalla connessione del dispositivo con una fonte di carica (corrente elettrica o batterie esterne)
- La modalità Airplane garantisce l'isolamento senza spreco ulteriore di batteria, tuttavia richiede l'interazione da parte dell'operatore con la tastiera del telefono. Potrebbe comportare dei rischi se non si ha familiarità con lo specifico dispositivo (p.es. errori di attivazione).

# Analisi memoria interna

- Come detto l'analisi della memoria interna può essere di tipo **logico** (file visibili) o **fisico** (copia integrale della memoria)
- In entrambi i casi l'analisi dei dati sarà effettuata:
  - Utilizzando un personal computer su cui sia installato un software di estrazione dei dati (software di backup del telefono oppure software dedicato per la mobile forensics) oppure
  - Utilizzando un dispositivo hardware dedicato
- In entrambi i casi, è necessario garantire una connessione tra il telefono cellulare e lo strumento di acquisizione

# Acquisizione fisica

- Cellbrite UFED
- Micro Systemation XRY
- CellDEK


# HW dedicato: Celebrite UFED

- Uno degli strumenti di acquisizione forense più utilizzati
- Sviluppato da Cellebrite (dal 1999), società con centinaia di dipendenti di  cui 1/2 R&D
- Opera su mercato privato e governativo/militare
- UFED P.A. vincitore dei Forensic 4cast Awards 2012 e non solo
- Rappresenta lo standard  dei tool di analisi forense per cellulari
- es. ad oggi esegue Physical Extraction di iPhone fino al 4, iPad fino all'1  come tutti gli altri software
- device supportati: https://cellebrite.com/en/cas-supported-devices/

# Principali funzionalità di UFED

- Estrarre le chiavi del dispositivo che possono essere utilizzate per decrittografare le immagini del disco
- Svelare le password del dispositivo (non disponibile per tutti i devices)
- Analisi e decodifica dei dati applicativi
- Generazione di report in vari formati (PDF, HTML)
- Scaricare il filesystem in raw mode per analizzarlo in altre applicazioni