**MOBILE FORENSICS**

La mobile forensics è al giorno d’oggi una disciplina a se stante.

La vita delle persone è contenuta nello smartphone, molto più di altri dispositivi.

Tratteremo alla fine del corso della possibilità di installare, su validazione delle forze di polizia, dei troyan.

Come altri computer, possiedono una RAM, memorie flash-di massa, memorie aggiuntive, schede SIM che al giorno d’oggi contengono poco, bisogna fare particolare attenzione alla sincronizzazione con cloud.

Sempre solita integrità dei dati, cosa non semplice sui telefoni, il problema è sempre acquisire i dati senza alterarli.

Copia bit a bit della memoria flash, difficile perché è un po’ inutile farlo su tutta la memoria, inoltre dobbiamo avere i privilegi di root sul dispositivo.

Un'altra possibilità è la acquisizione fisica(chip-off)

Oppure acquisizione logica del filesystem, di alcuni file, o cose del genere, la maggior parte dei dispositivi tiene le informazioni in database SQLite. Molte volte l’acquisizione logica non è completa.

Acquisizione manuale come ultimo baluardo, dispositivo acceso e acquisisco le informazioni in modo manuale.

Acquisizione della RAM rara, bisogna solitamente disporre un accesso root al dispositivo e un riavvio.

Vabeh dati da cercare nelle slide, cose normali.

Software vari per ricerca di dati e metadati vabeh.

Dispositivi IOS abbastanza diversi.

Meccanismi di jail per controllare gli accessi alle funzionalità, jailbreaking per disabilitare.

Operazioni particolarmente dcelicate

Tecniche brute-force particolarmente complicate.