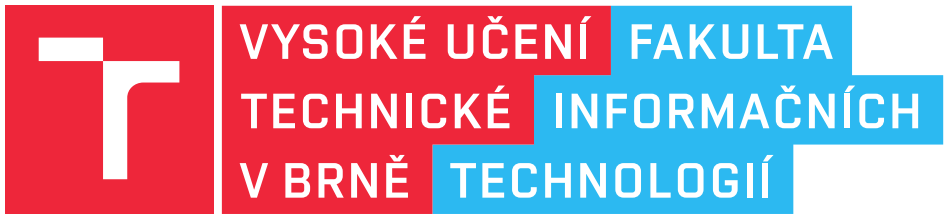
Forenzná analýza mobilných zariadení

Dávid Bolvanský

xbolva00@stud.fit.vutbr.cz



Mobilná forenzná analýza

- veda zaoberajúca sa obnovou digitálnych dát z mobilných zariadení
- musí dodržiavať striktné forénzne pravidlá
- vykonávaná pomocou schválených metód

Klasifikácia:

- preskúmanie možností metód získavania dôkazov
- vykonávanie podrobných forenzných postupov
- vykonávanie hĺbkovej forenznej analýzy mobilných aplikácií alebo mobilných operačných systémov

Terorizmus a mobilné aplikácie

- cloudové aplikácie môžu byť používané na ukladanie dát, ktoré môže byť neskôr použité pri vyšetrovaní ako dôkazový materiál
- komunikačné aplikácie slúžia na výmenu hlasových a video správ
- môžu obsahovať potenciálne informácie o plánovaní a organizácie kriminálnych aktivít
- incident, kedy spoločnosť Apple Inc. odmietla pomôcť Federálnemu vyšetrovaciemu úradu v USA so žiadosťou o odblokovanie šifrovaného iPhone

→ preskúmanie formátu neznámych dát

- Prístup založený na vzorkách
  - technika vzorkovania vstupných dát na vzorky za účelom odvodenia formátu dát
  - Discoverer, LearnPADS
- Prístup založený na inštrumentácii
  - vyžaduje komplexný proces inštrumentácie binárneho spustiteľného súboru
  - Discoverer, LearnPADS

- tri hlavné typy analýzy denníka prevádzky telefónu
  - prvá skúma vzťahy medzi individuálnymi užívateľmi
  - druhá sa zaoberá geografickou polohou telefónu
  - tretia skúma udalosti v prevádzke v časovej ose
- LogAnalysis sa zaoberá na prvý typom analýzy
  - import dát vytvorenými informatívnymi systémami mobilných telefónov
  - konverzie do formátu GraphML, ktorý je štruktúrovaný formát XML vhodnejší pre grafické znázornenie a výmeny medzi aplikáciami na kreslenie grafov
  - cieľom je získať zaujímavé informácie pre vyšetrovanie z celkovej štruktúry siete