
**VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ**
**BRNO UNIVERSITY OF TECHNOLOGY**

**FAKULTA INFORMAČNÍCH TECHNOLOGIÍ**
**FACULTY OF INFORMATION TECHNOLOGY**


# FORENZNÍ ANALÝZA MOBILNÍCH ZAŘÍZENÍ

**FORENSIC ANALYSIS OF MOBILE DEVICES**

**BEZPEČNOST A POČÍTAČOVÉ SÍTĚ**
**SECURITY AND COMPUTER NETWORKS**


**AUTOR** **DÁVID BOLVANSKÝ**
**AUTHOR**



**BRNO 2017**

# Kapitola 1

# Forenzná analýza

> *"Aplikovanie metodickej sady techník a procedúr potrebných na získanie dôkazov z dodaného počítačového vybavenia, rôznych pamäťových zariadení a digitálnych médií, ktoré môžu byť následne prezentované v koherentnom a zmysluplnom formáte."*
>
> - Dr. H.B. Wolfe

Incidenty v informačnej bezpečnosti sa odohrávajú vo virtuálnom priestore počítačov a počítačových sieti. V ideálnom prípade by sme mali byť schopní zabrániť prípadným útokom, no nie vždy je to možné. Ak už k bezpečnostnému incidentu dôjde, je potrebné zaistiť dôkazy, správne ich vyhodnotiť a na ich základe vyvodiť závery.

Forenzná analýza je jednou z používaných analýz pri vyšetrovaní trestných činov. Cieľom počítačovej forenznej analýzy je príprava získaných materiálov na ďalšie vyšetrovanie. Rieši problematiku kto, ako a kedy uskutočnil nejakú aktivitu súvisiacu s vykonaným trestným činom. Zahŕňa využitie širokého spektra vyšetrovacích technológií a postupov a metód. Slúži ako prostriedok na získanie dôkazov k trestným činom, zneužitie právomocí, porušenie zákona, interných pravidiel alebo smerníc, preukázanie identity osôb, pravosti listín, dát alebo informácií a to ako účastníkom trestného konania tak aj komerčnej sfére. Musí byť vykonávaná podľa prísnych pravidiel aby boli dôkazy prijateľné pre organy činne v trestnom konaní. Počas forenznej analýzy je kľúčové zbieranie digitálneho dôkazového materiálu. Predmetom skúmania nie sú často len samostatné počítače, ale celé počítačové systémy. Výsledkom forenznej analýzy je znalecký alebo technický posudok alebo vyjadrenie, ktorý má v súdnom konaní dôkazovú hodnotu.

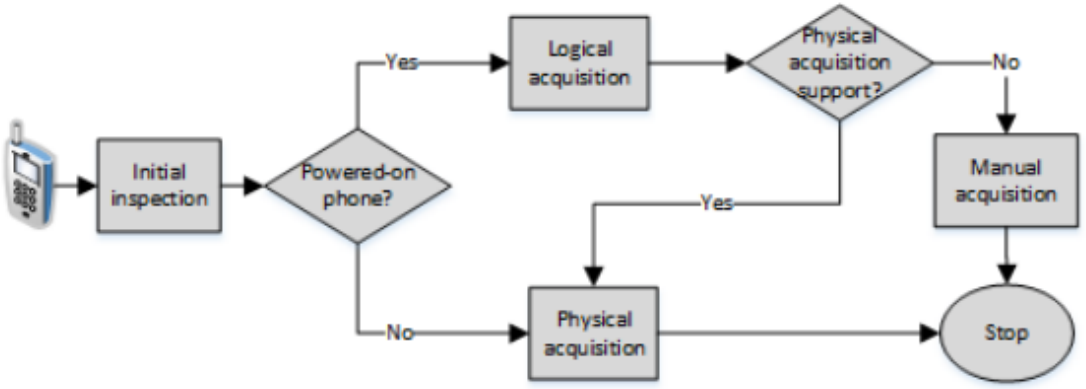
## 1.1 Mobilná forenzná analýza

> *"Mobilná forenzná analýza je veda zaoberajúca sa obnovou digitálnych dát z mobilných zariadení podľa striktných foreznych pravidiel za pomoci schválených metód."*
>
> - National Institute of Standards and Technology (NIST)

Získavanie digitálnych dokázov v mobilných forenzných aktivitách zahŕňa fyzické, logické, a ručné metódy. Fyzické spôsoby získavania dôkazov sa týkajú obnovy binárne reprezentácie internej pamäte mobilných zariadení a ich ukladania do súborov. Logické spôsoby pracujú s operačným systémom skúmaného mobilného zariadenia za účelom obnovy logických

objektov v súborovom systéme. Ručné spôsoby zahŕňajú zobrazovanie dátového obsahu uloženého v mobilnom zariadení, ktoré vyžaduje manuálnu aktivitu s tlačidlami, klávesnicou či dotykovou obrazovkou a môžu byť nahrávané na externú digitálnu kameru.

Existujúci výskum v oblasti mobilnej forenznej analýzy je možné klasifikovať do nasledovných častí: 1. preskúmanie možností metód získavania dôkazov, 2. vykonávanie podrobných forenzných postupov, 3. vykonávanie hĺbkovej forenznej analýzy mobilných aplikácií alebo mobilných operačných systémov.




Obr. 1.1: Procedúra získavania dát

Počiatočná kontrola predstavuje činnosť preskúmania stavu zariadenia zhromažďovaním informácií ako napríklad výrobcu zariadenia, názvu modelu a čísla IMEI. Stav zariadenia rozhoduje o použití techník na získavanie dôkazov. Logické získavanie dôkazov sa vykoná v prípade, že zariadenie je zapnuté. Začína identifikáciou zmeškaných hovorov, neprečítaných správ, času a dátumu pomocou skúmania obrazovky zariadenia.

Fyzické získavanie dôkazov je vykonávané ak je zariadenie vypnuté. Vykonávanie ručného získavania dôkazov je voliteľné, ak výsledky z logického skúmania sú obmedzené a/alebo fyzické skúmanie nie je podporované.

# Kapitola 2

# Terorizmus a mobilné aplikácie

Mobilné technológie sú často zneužívané na aktivity súvisiace s terorizmom. Forenzná analýza je dôležitý prostriedok pri vyšetrovaní takýchto aktivít. Terorizmus možno definovať ako použitie násilia skupinami alebo jednotlivcami, ktorí sa snažia presadiť svoje politické ciele. Svoje ciele si vyberajú náhodne, často ide o spôsobenie čo najväčších civilných strát.

V nedávnej dobe došlo k incidentu, kedy spoločnosť Apple Inc. odmietla pomôcť Federálnemu vyšetrovaciemu úradu v USA so žiadosťou o odblokovanie šifrovaného iPhone 5C údajne patriacemu jednému z kľúčových podozrivých, pretože podozrivý deaktivoval iCloud zálohy niekoľko týždňov pred incidentom[1].

Tento incident si získal znateľný záujem medií, ako aj rozvíril debaty medzi v výskumníkmi a politikmi. Taktiež demonštroval potenciálnu úlohu mobilnej forenznej analýzy pri obnove dôkazových materiálov z mobilných zariadení, ktoré boli použité pri plánovaní, vykonávaní terorizmu a iných kriminálnych aktivít.

Cloudové aplikácie môžu byť používané na ukladanie dát, ktoré môže byť neskôr použité pri vyšetrovaní ako dôkazový materiál [3]. Komunikačné aplikácie slúžia na výmenu hlasových a video správ. Môžu teda obsahovať potenciálne informácie o plánovaní a organizácie kriminálnych aktivít. Pomocou forenzných techník je možné obnoviť záznamy z konverzácií, multimediálne súbory, zoznamy kontaktov, geografické dáta, ktoré sú neskôr použité na určenie sledu udalosti a identifikácie rôznych súvislostí týkajúcich sa trestného činu.

[1] https://assets.documentcloud.org/documents/2716811/Statement-from-the-FBI-Feb-20-2016.pdf

# Kapitola 3

# Reverzné inžinierstvo v mobilnej forenznej analýze

Získavanie dát z mobilných zariadení je zložité kvôli rôznych dôvodom [8]. Pre obnovu dát je potrebné aby vyšetrovatelia najskôr získali uložené dáta za zariadenia. Samotné získavanie je ťažkopádne, ale často ho možno dosiahnuť použitím špeciálnych nástrojov. Je užitočné, ale nie je dostatočné na získanie dát zo zariadenia iba pomocou rozhrania alebo softvéru mobilné zariadenia. Odstránené dáta nemôžu byť získané a vymazané informácie nemôžu byť obnovené. Navyše proces zobrazenia dát môže pozmeniť určité informácie (napr. zmena času posledného prístupu).

Po získaní dát je potrebné ich interpretovať a vytiahnuť z nich potrebné informácie. Na druhej strane, softvér mobilného zariadenia je vo veľkej miere chránený a výrobcovia odmietajú pomáhať s cieľom chrániť si obchodné tajomstvá. V praxi je teda potrebné použiť reverzné inžinierstvo na preskúmanie formátu dát.

Cieľom reverzného inžinierstva je interpretovať dáta, ktoré boli vytvorené podľa neznámej formátovej špecifikácie S skúmaním reprezentatívnych vzoriek dát. Predpokladajme, že máme sadu vzoriek $R = \{r_1, r_2, ..., r_n\}$. Každá vzorka dát je vytvorená podľa $S$ a skladá z jedného alebo viacerých neprekrývajúcich sa polí. Platí, že $r_i = \{f_1, f_2, ..., f_n\}$. Pole predstavuje zmysluplný súbor údajov, napríklad celé číslo alebo reťazec. Predpokladáme, že hranice medzi políčkami nie sú známe a že v zázname nie sú žiadne explicitné oddeľovače polí. Inými slovami, bez znalosti formátu, každý záznam je to postupnosťou binárnych dát. Pre každý záznam $r_i$ je cieľom poskytnúť predpokladaný výklad $r_i^{'}$. Táto interpretácia zahŕňa východiskovú pozíciu $s$, dĺžku $l$, typ $t$ každého poľa v zázname tak, že $r_i^{'} = \{f_1^{'}, f_2^{'}, ..., f_n^{'}\}$, kde $f_j^{'}$ je trojica $(s_j, l_j, t_j)$.

Niekoľko spoločností predávajú nástroje na analýzu dát v mobilných zariadeniach za pomoci znalostí získaných z manuálne ručného reverzného inžinierstva. Tento proces je náročný a musí sa často opakovať z dôvodu vývoja a predaja nových zariadení. V dôsledku toho tieto nástroje môžu byť veľmi drahé - niektoré dosahujú cenu 20 000 dolárov.

Avšak i celá sada týchto mnohých forenzných nástrojov nepokrýva veľkú množinu dostupných mobilných zariadení. Tieto dôvody iniciovali mnoho pokusov na uľahčenia procesu reverzného inžinierstva.

## 3.1 Prístup založený na vzorkách

Existuje viacero nástrojov, ktoré používajú techniku vzorkovania vstupných dát na vzorky za účelom odvodenia formátu dát.

Discoverer [5] sa snaží automaticky odvodiť formát správ zasielaných sieťovým protokolom na úrovni aplikačnej vrstvy. Po získaní vzorku, Discoverer rozdelí každú správu do tokenov, zhlukuje každý token a pokúša sa odvodiť formát tokenu porovnaním s iným správami v rovnakom zhluku.

LearnPADS [7] je ďalší nástroj využívajúci vzorkovaní na odvodzovanie formátu ad hoc dát. Vytvára špecifikáciu tohto formátu v jazyku PADS na opis dát. LearnPADS začína rozdelím vstupných dát na série zhlukov, typicky riadok po riadku alebo súbor za súborom. Zhluky sa ďalej rozdeľujú do tokenov pomocou lexikálneho analyzátora. LearnPADS používa histogram frekvencií tokenov na odvodenie štruktúry dát.

## 3.2 Prístup založený na inštrumentácii

Mnoho prístupov, zahŕňajúc Polyglot [2], Tupni [6] a Dispatcher [1], vyžaduje komplexný proces inštrumentácie binárneho spustiteľného súboru.

Polyglot bol vytvorený na prekonanie nedostatkov prístupov založených na vzorkách sledovaním toho, ako program spracováva prijaté správy. Tupni používa tzv. taint analýzu na spätné vytváranie vstupných formátov s vysokou presnosťou. Dispatcher sa taktiež snaží odvodiť formát správ odoslaných programom, ako aj sémantiku polí v odosielaných a prijatých správach.

# Kapitola 4

# Forenzná analýza prevádzky mobilných zariadení

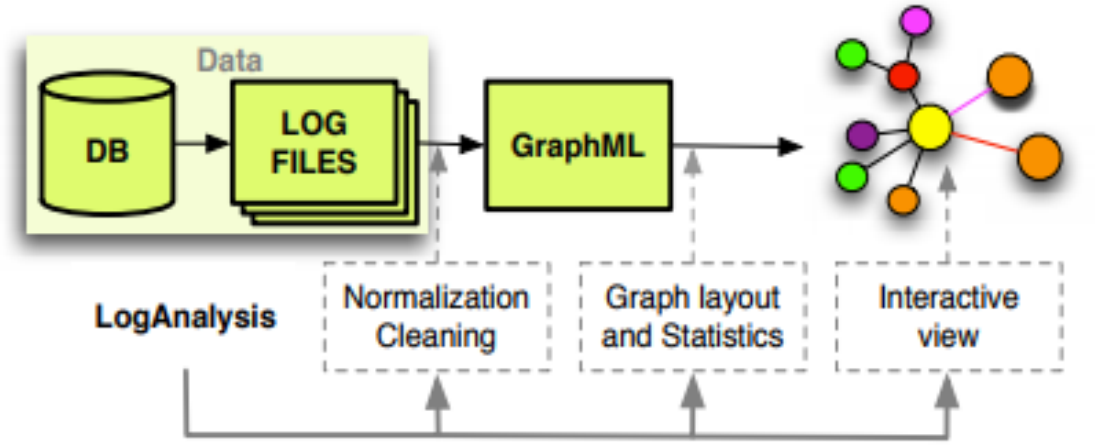
Telefónne spoločnosti musia podľa súčasné predpisy mať záznamy týkajúce sa prevádzky telefónov za dané časové obdobie [4]. Tieto súbory obsahujú obrovské množstvo dát, ako sú telefonické hovory, SMS, MMS, GPRS a internetové služby. Zaujímavé informácie sú tiež získané z prevádzky, ktorú produkuje bunka Global Identities (CGI) vo vnútri týchto oblastiach. Analýza správ od telefónnych spoločností umožňuje rekonštrukciu vzťahov medzi jednotlivcami v sieti

Vzťahy vytvorené prostredníctvom telefonickej prevádzky možno preskúmať prostredníctvom rôznych techník. Niektoré forenzné analýzy sa týka telefónnej prevádzky uskutočnenej pomocou International Mobile Subscriber Identity (IMSI) a International Mobile Equipment Identity (IMEI). IMSI je jedinečné číslo spojené so všetkými GSM a UMTS užívateľmi. Je uložené na SIM karte v telefóne a je odosielané telefónom do siete. IMEI je jedinečný 15 alebo 17-miestny kód používaný na identifikáciu mobilnej stanice v sieti GSM alebo UMTS.

Detektívi vo všeobecnosti rozlišujú tri hlavné typy analýzy denníka prevádzky telefónu. Prvá skúma vzťahy medzi individuálnymi užívateľmi. Druhá sa zaoberá geografickou polohou telefónu a tretia skúma udalosti v prevádzke v časovej ose.

## 4.1 Analýza záznamov – LogAnalysis

*LogAnalysis sa zaoberá na prvý typom analýzy denníka telefónu.*




Obr. 4.1: Architektúra *LogAnalysis*

*Architektúra je tvorená rozšíriteľnými úrovňami: import dát vytvorenými informatívnymi systémami mobilných telefónov (zvyčajne bytové súbory), 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.*

# Literatúra


[1] *Caballero, J.; Poosankam, P.; Kreibich, C.; aj.: Dispatcher: Enabling Active Botnet Infiltration Using Automatic Protocol Reverse-engineering. In* Proceedings of the 16th ACM Conference on Computer and Communications Security*, CCS '09, New York, NY, USA, 2009, ISBN 978-1-60558-894-0, s. 621–634.*

[2] *Caballero, J.; Yin, H.; Liang, Z.; aj.: Polyglot: Automatic Extraction of Protocol Message Format Using Dynamic Binary Analysis. In* Proceedings of the 14th ACM Conference on Computer and Communications Security*, CCS '07, New York, NY, USA: ACM, 2007, ISBN 978-1-59593-703-2, s. 317–329.*

[3] *Cahyani, N. D. W.; Ab Rahman, N. H.; Xu, Z.; aj.: The Role of Mobile Forensics in Terrorism Investigations Involving the Use of Cloud Apps. In* Proceedings of the 9th EAI International Conference on Mobile Multimedia Communications*, MobiMedia '16, ICST, Brussels, Belgium, Belgium: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2016, ISBN 978-1-63190-104-1, s. 199–204.*

[4] *Catanese, S. A.; Fiumara, G.: A Visual Tool for Forensic Analysis of Mobile Phone Traffic. In* Proceedings of the 2Nd ACM Workshop on Multimedia in Forensics, Security and Intelligence*, MiFor '10, New York, NY, USA, 2010, ISBN 978-1-4503-0157-2, s. 71–76.*

[5] *Cui, W.; Kannan, J.; Wang, H. J.: Discoverer: Automatic Protocol Reverse Engineering from Network Traces. In* Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium*, SS'07, Berkeley, CA, USA: USENIX Association, 2007, ISBN 111-333-5555-77-9, s. 14:1–14:14.*

[6] *Cui, W.; Peinado, M.; Chen, K.; aj.: Tupni: Automatic Reverse Engineering of Input Formats. In* Proceedings of the 15th ACM Conference on Computer and Communications Security*, CCS '08, New York, NY, USA, 2008, ISBN 978-1-59593-810-7, s. 391–402.*

[7] *Fisher, K.; Walker, D.; Zhu, K. Q.; aj.: From Dirt to Shovels: Fully Automatic Tool Generation from Ad Hoc Data.* SIGPLAN Not.*, ročník 43, č. 1, Leden 2008: s. 421–434, ISSN 0362-1340.*

[8] *Wilson, R.; Chi, H.: A Case Study for Mobile Device Forensics Tools. In* Proceedings of the SouthEast Conference*, ACM SE '17, New York, NY, USA, 2017, ISBN 978-1-4503-5024-2, s. 154–157.*