UNIVERSITY OF TARTU
Institute of Computer Science
Cyber Security Curriculum

Lukáš Bortník, 1772181IVCM

Mobile phone digital evidence providers to investigate driver's distraction

Master's Thesis (30 EAP)

Supervisor(s): Pavel Laptev,

Satish Narayana Srirama

Tartu 2019

Mobile phone digital evidence providers to investigate driver's distraction

Abstract:

Police officers investigating car accidents have to consider driver's interaction with mobile device as a possible cause of the accident. Unfortunately, mobile device artefacts which could help to prove driver's distraction are volatile and can be purged either by user or the operating system itself. As currently available digital forensics frameworks do not allow uncovering driver's behaviour thoroughly, the study analyses prospective evidence providers which could assist forensic practitioners to prove or disprove driver's distraction. The focus is taken on analysis of Android operating system services' data acquired by Android dumpsys. The study inspects the possibility to identify the interaction with mobile device applications without ac-cessing user's personal content. The research outcomes demonstrate the ability to distinguish events generated by operating system vital services and events originating from intentional driver's interaction. The analyses involve specific driver's activities such as interaction with social media, calling, texting, browsing offline content and possible anti-forensics activities to avoid being persecuted. In addition, the method can be used to discover system level activities, such as login activities, charging methods, changing device settings or switching between appli-cations and in-app activities. Besides traditional telecom services, proposed method provides a solution to identify telephony activities conducted via cross-platform VoIP applications, such as Viber, Messenger, WhatsApp, Signal or Telegram. Moreover, as drivers may conduct their phone calls via external handsfree kit, the thesis provides a solution how to identify individual call routing methods - either using device's earpiece, wired kit, or Bluetooth connected car's stereo. Furthermore, study also demonstrates possibility to retrieve the information about cur-rent and historical environment settings – e.g., connected wireless networks, bluetooth connec-tions, paired devices and associated network artefacts. The thesis is finalized by case study analyses of simulated car accident. In addition to successfully identified driver's interaction with mobile device, the case study analyses demonstrate how to apply researched method in the real-life examination, includes recommendations for targeted time and cost-effective inves-tigation, and proposes the areas of future research.

Keywords:

digital evidence, mobile forensics, car accident, driver's distraction, android dumpsys

CERCS: P170

Digitaalse tõendusmaterjali allikad nutiseadmetes sõidukijuhi tähelepanu hajumise uurimiseks

Lühikokkuvõte:

Liiklusõnnetuste uurimisel tuleb arvestada võimalusega, et õnnetuse põhjuseks võis olla autojuhi tähelepanu hajumine mobiilseadme kasutamise tõttu. Tänasel päeval kohtuekspertiisis kasutatavad lahendused ei võimalda anda põhjalikku ülevaadet seadme kasutaja täpse käitumise osas. Lisaks on nutiseadmetesse salvestunud andmed tihti ebapüsivad võides hävineda nii kasutaja tegevuse kui operatsioonisüsteemi töö tagajärjel. Käesoleva magistritöö eesmärk on uurida võimalikke tõendusmaterjalide allikaid, mis aitaksid tõendada juhi tähelepanu hajumist või mittehajumist.

Töö keskendub Android operatsioonisüsteemiga seadmetele, täpsemalt dumpsys kaudu omandatavatele andmetele ning uurib võimalusi tõestamaks mobiilseadme käsitsemist kasutamata selleks kasutaja isiklikke andmeid. Töös tutvustatakse meetodit, kuidas eristada taustasündmusi tahtlikust seadme kasutamisest, muuhulgas sotsiaalmeedia kasutamine, helistamine, sõnumite saatmine, muu sisu sirvimine ning ka võimalikud hilisemat ekspertiisi takistavad tegevused. Meetod aitab tuvastada ka VoIP programmidega (Viber, Messenger, WhatsApp, Signal või Telegram) tehtud kõned. Lisaks kasutaja tegevusele eristatakse mitmeid süsteemseid tominguid, nende seas seadistuse muutmine, seadme aku laadimine, kontodest sisse

või välja logimine ja seadme ühenduvuse ajalugu (traadita võrgud ja Bluetooth). Autojuhid kasutavad helistamiseks erinevaid juhtmevabu tehnoloogiaid, välja töötatud meetod suudab eristada täpset kõne tegemise viisi – seade ise, juhtmega ühendatud kõrvakomplekt või Bluetooth kaudu ühendatud auto. Töö sisaldab juhtumiuuringuid, mis analüüsivad esitatud meetodit simuleeritud liiklusõnnetuste korral. Lisaks edukale juhi tähelepanu hajumise tuvastamisele, näitavad juhtumiuuringud viise, kuidas väljatöötatud metoodit kasutada reaalelulisetes situatsioonides, soovitusi kulu vähendamiseks menetlemisel ning pakub välja edasise uurimustöö suundi.

Võtmesõnad:

Digitaalne tõendusmaterjal, mobiilseadme kohtuekspertiis, autoõnnetus, sõidukijuhi tähelepanu hajumine, android dumpsys

CERCS: P170

Non-exclusive licence to reproduce thesis and make thesis public

I,_____*Lukáš Bortník*_____,

(*author's name*)

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to:

1.1. reproduce, for the purpose of preservation, including for adding to the DSpace digital archives until the expiry of the term of copyright, and

1.2. make available to the public via the web environment of the University of Tartu, including via the DSpace digital archives, under the Creative Commons licence CC BY NC ND 3.0, which allows, by giving appropriate credit to the author, to reproduce, distribute the work and communicate it to the public, and prohibits the creation of derivative works and any commercial use of the work from ***16/05/2019*** until the expiry of the term of copyright,

_____

Mobile phone digital evidence providers to investigate driver's distraction

(*title of thesis*)

supervised by *Pavel Laptev, Satish Narayana Srirama*

(*supervisor's name*)

2. I am aware of the fact that the author retains the rights specified in p. 1.

3. I certify that granting the non-exclusive licence does not infringe other persons' intellectual property rights or rights arising from the personal data protection legislation.

Lukáš Bortník

16/05/2019