

IT'18
ŽABLJAK

XXIII

međunarodna naučno - stručna konferencija

**INFORMACIONE
TEHNOLOGIJE**

SADAŠNJOST I BUDUĆNOST

Urednik
Božo Krstajić

IT'18

**INFORMACIONE
TEHNOLOGIJE**

- SADAŠNJOST I BUDUĆNOST -

**Urednik
*Božo Krstajić***

*Zbornik radova sa XXIII međunarodne naučno - stručne konferencije
INFORMACIONE TEHNOLOGIJE - sadašnjost i budućnost
održanog na Žabljaku od 19. do 24. februara 2018. godine*

Zbornik radova
INFORMACIONE TEHNOLOGIJE - sadašnjost i budućnost 2018

Glavni urednik
Prof. dr Božo Krstajić
Elektrotehnički fakultet Univerziteta Crne Gore

Izdavač
Univerzitet Crne Gore
Elektrotehnički fakultet
Džordža Vašingtona bb., Podgorica
www.etf.ucg.ac.me

Tehnička obrada
Aleksandra Radulović
Centar informacionog sistema Univerziteta Crne Gore

Doc. dr Žarko Zečević
Elektrotehnički fakultet Univerziteta Crne Gore

Ivan Jokić
Elektrotehnički fakultet Univerziteta Crne Gore

Tiraž
150

Podgorica 2018.

Sva prava zadržava izdavač i autori

Organizator

Elektrotehnički fakultet, Univerzitet Crne Gore

Skup podržao

The Institute of Electrical and Electronics Engineers - IEEE

Programski odbor

Dr Novak Jauković, Elektrotehnički fakultet, UCG, Podgorica, MNE
Dr Ljubiša Stanković, Elektrotehnički fakultet, UCG, Podgorica, MNE
Dr Zdravko Uskoković, Elektrotehnički fakultet, UCG, Podgorica, MNE
Dr Vujica Lazović, Ekonomski fakultet, UCG, Podgorica, MNE
Dr Branko Kovačević, Elektrotehnički fakultet, UB, Beograd, SRB
Dr Milorad Božić, Elektrotehnički fakultet, UBL, Banja Luka, RS BIH
Dr Miroslav Bojović, Elektrotehnički fakultet, UB, Beograd, SRB
Dr Zoran Jovanović, Elektrotehnički fakultet, UB, Beograd, SRB
Dr Milica Pejanović-Đurišić, Elektrotehnički fakultet, UCG, Podgorica, MNE
Dr Despina Anastasiadou, Research & Development Innovation Academy, Solun, GRC
Dr Dejan Popović, Elektrotehnički fakultet, UB, Beograd, SRB
Dr Gabriel Neagu, National Institute for Research & Development in Informatics, Bucharest, ROU
Dr Božo Krstajić, Elektrotehnički fakultet, UCG, Podgorica, MNE
Dr Tomo Popović, Fakultet za informacione sisteme i tehnologije, UDG, Podgorica, MNE
Dr Milovan Radulović, Elektrotehnički fakultet, UCG, Podgorica, MNE
Dr Le Xie, Texas A&M University, College Station, TX, USA
Dr Sašo Gelev, Elektrotehnički fakultet, UGD, Radoviš, MKD
Dr Budimir Lutovac, Elektrotehnički fakultet, UCG, Podgorica, MNE
Dr Zoran Veljović, Elektrotehnički fakultet, UCG, Podgorica, MNE
Dr Igor Radusinović, Elektrotehnički fakultet, UCG, Podgorica, MNE
Dr Alex Sprintson, Texas A&M University, College Station, TX, USA
Dr Nikša Tadić, Elektrotehnički fakultet, UCG, Podgorica, MNE
Dr Miloš Daković, Elektrotehnički fakultet, UCG, Podgorica, MNE
Dr Milutin Radonjić, Elektrotehnički fakultet, UCG, Podgorica, MNE
Dr Slobodan Đukanović, Elektrotehnički fakultet, UCG, Podgorica, MNE
Dr Žarko Zečević, Elektrotehnički fakultet, UCG, Podgorica, MNE
Dr Ana Jovanović, Elektrotehnički fakultet, UCG, Podgorica, MNE
Dr Vesna Rubežić, Elektrotehnički fakultet, UCG, Podgorica, MNE
Dr Vesna Popović Bugarin, Elektrotehnički fakultet, UCG, Podgorica, MNE
Dr Tatjana Stanivuk, Pomorski fakultet, SS, Split, HRV
Dr Sanja Bauk, Pomorski fakultet, UCG, Kotor, MNE
Dr Vera Marković, Elektronski fakultet, UN, Niš, SRB
Dr Biljana Stamatović, Fakultet za informacione sisteme i tehnologije, UDG, Podgorica, MNE
Dr Ramo Šendelj, Fakultet za informacione sisteme i tehnologije, UDG, Podgorica, MNE
Dr Stevan Šćepanović, Prirodno-matematički fakultet, UCG, Podgorica, MNE
Dr Goran Šuković, Prirodno-matematički fakultet, UCG, Podgorica, MNE
Dr Siniša Vlajić, Fakultet organizacionih nauka, UB, Beograd, SRB
Dr Dragan Janković, Elektronski fakultet, UN, Niš, SRB
Dr Zoran Milivojević, Visoka tehnička škola strukovnih studija, Niš, SRB
Dr Chun-Yen Chang, National Taiwan Normal University, Taipei, TWN

Organizacioni odbor

Dr Božo Krstajić, Elektrotehnički fakultet, UCG, Podgorica, MNE - Predsjedavajući konferencije

Dr Milovan Radulović, Elektrotehnički fakultet, UCG, Podgorica, MNE - Finansijski rukovodilac konferencije

Dr Zoran Veljović, Elektrotehnički fakultet, UCG, Podgorica, MNE

Dr Igor Radusinović, Elektrotehnički fakultet, UCG, Podgorica, MNE

Dr Ana Jovanović, Elektrotehnički fakultet, UCG, Podgorica, MNE

Dr Tomo Popović, Fakultet za informacione sisteme i tehnologije, UDG, Podgorica, MNE

Dr Žarko Zečević, Elektrotehnički fakultet, UCG, Podgorica, MNE - Tehnički rukovodilac konferencije

Vladan Tabaš, dipl.ing., Čikom, Podgorica, MNE

Aleksandra Radulović, CIS UCG, Podgorica, MNE - Rukovodilac izdavačke djelatnosti

Ivan Jokić, Elektrotehnički fakultet, UCG, Podgorica, MNE - Kontakt za informacije

P R E D G O V O R

Poštovani učesnici i čitaoci,

Još jedno uspješno druženje je bilo, još jedna sadašnjost je postala prošlost i još jednu budućnost smo pokušali da dokučimo na protekloj 23. konferenciji “INFORMACIONE TEHNOLOGIJE – sadašnjost i budućnost” (IT’18) održanoj od 19. do 24. februara 2018. godine na Žabljaku. Pred vama je zbornik radova pisanih na našem jeziku i sažetaka radova koji su pisani na engleskom jeziku. Kompletni radovi na engleskom jeziku su dostupni u IEEE Xplore bazi i to je novina ovogodišnje konferencije. Programski odbor smatra da je to novi kvalitet konferencije, uz korišćenje programa za provjeru plagijata u procesu nezavisne anonimne međunarodne recenzije radova i pažljivom izboru plenarnih tema i predavača. No, posebnu zahvalnost dugujemo autorima koji, nesporno, iz godine u godinu podižu kvalitet ove konferencije birajući sve bolje i atraktivnije rezultate svojih istraživanja da prezentuju upravo na našoj konferenciji. Zahvaljujući vama, dragi autori, smo uspjeli da postignemo visok standard prihvaćenih radova, i prvi put da ih objavimo i u svjetski renomiranoj bazi naučnih radova kao što je IEEE Xplore.

Pred vama su 20 kompletnih autorskih radova i 32 sažetaka radova koje možete naći u IEEE Xplore bazi, prezentovani u 8 oralnih i jednoj poster sekciji, kao i sažeci 5 predavanja po pozivu koja su realizovana u plenarnom dijelu programa. Procenat radova koji su prihvaćeni za prezentovanje na ovogodišnjoj konferenciji je 74%.

Ovo je, do sada, IT sa najviše učesnika van Crne Gore jer su autori radova i predavači bili iz preko 20 država svijeta (Južna Koreja, Tajvan, Kina, Nigerija, Irak, Egipat, Turska, Albanija, Rumunija, Bugarska, Italija, Francuska, Mađarska, Rusija, Njemačka, Makedonija, Srbija, Hrvatska, ...). Preko 150 učesnika, 120 studenata sa sva 3 crnogorska univerziteta i veliki broj online posjetilaca su pratili rad konferencije 5 radnih dana. Konferencija je bila medijski ispraćena i podržana na državnom i lokalnom nivou i od velikog broja ICT kompanija.

Durmitor nas je podario ogromnim količinama snijega (preko 100 cm) koji je padao svaki dan ali su putevi bili prohodni, nije bilo mećava ili ekstremnih hladnoća i svi smo uživali u divnom zimskom ambijentu. Bilo je puno poznatih, ali i novih, ozarenih i zadovoljnih lica koja su uljepšala druženje i, nadamo se, ponijela lijepe otiske sa sniježne planine. Želimo im nova nadahnuća, ideje i snagu za život i rad, a mi ćemo ih čekati i sledeće godine na istom mjestu.

Sve detalje o ovom, prošlim i narednom skupu možete naći na web adresi konferencije www.it.ac.me.

Prof. dr Božo Krstajić

SADRŽAJ

PREDAVANJA PO POZIVU	1
Enrico Natalizio High-end IoT systems in 5G.....	2
Željko Đurović Emerging trends in system monitoring and control.....	3
Chun-Yen Chang CloudClassRoom X Mobile learning = Improved Outcomes	4
Mališa Vučinić The Devil is in the Detail: How a Real-World IoT Technology is Made – IETF 6TiSCH.....	5
Dejan Dokmanović Standards and guidelines in the design of physical infrastructure of modern data centers	6
AUTORSKI RADOVI	7
Kosta Pavlovic, Aleksandar Popovic Jezik MetaR	8
Anita Ilić, Dušan Savić, Vojislav Stanojević Veb aplikacija “Pitaj-odgovori” u Java EE okruženju	12
Strahinja Jakic, Nikola Matijevic Pametna kuća upravljiva glasom	16
Miloš Milić, Siniša Vlajić, Ilija Antović Primena SilabMetrics alata za statičku analizu softvera u procesu evaluacije kvaliteta softvera	20
Ana Ivanović, Miloš Daković Primjer integracije aplikativnih modula iz različitih aplikativnih podsistema u Centralnoj banci CrneGore.....	24
Dijana Kostić, Zoran Milivojević, Darko Brodić Uticaj audio šuma tipa reverzni govor na razumljivost	28
Milica Ilić, Dušan Savić, Saša Lazarević Primena Java biblioteke za konkurentno programiranje	32
Dragan N. Filipović, Vladan R. Durković Poduzna kapacitivnost tankog linijskog provodnika u centru uzemljenog kvadratnog oklopa.....	36
Martin P. Čalasan, Vladan Vujičić Using PSO algorithm for induction machine parameters estimation with considering of iron loss.....	40

Marina Matijević, Ramo Šendelj Bezbjednosni aspekti primjene Jedinstvenog informacionog sistema za elektronsku razmjenu podataka kod elektronskog upisa djece u obrazovne ustanove	44
Rade M. Pavlovic, Vladimir S. Petrovic Sjedinjavanje multisenzorskih slika u cilju detekcije multikoptera	48
Jelena Jauković Nove FinTech-efikasne finansijske usluge bazirane na ICT	52
Bojan Prlinčević, Slobodan Bjelić Analiza rada trofaznih mostnih invertora i verifikacija rezultata simulacijom rada u izabranom programu.....	56
Mladen Antonijević, Luka Lazović Poboljšanje performansi modifikovane Sierpinski fraktalne antene pomoću metapovršina.....	60
Zoran N. Milivojević, Zoran Veličković, Darko T. Brodić Optimizacija parametara BL jezgra kod procene fundamentalne frekvencije audio signala	64
Tamara D. Šević, Milenko S. Andrić, Boban P. Bondžulić, Dimitrije M. Bujaković, Dejan S. Ivković Uticaj kriterijumske funkcije na segmentaciju spektrograma	68
Saso A. Gelev, Aleksandar Tudzarov, Vasilija J. Sarac, Vlatko T. Cingoski, Slobodan Bundalevski Metodi i alati za forenziku mobilnih telefona.....	72
Jelena Končar, Sonja Vučenović, Zita Petrović Katai Digitalizacija maloprodaje na globalnom tržištu	76
Aleksandar Tomić, Radiša Stefanović, Nada Ratković Kovačević, Aleksa Srdanov Sistem za daljinsko uključivanje i isključivanje električnih uređaja, slanjem SMS poruka	79
Marko Asanović Optimization of the characteristics of the photovoltaic system in the appearance of partial shading.....	83
ABSTRAKTI AUTORSKIH RADOVA OBJAVLJENIH U IEEE XPLOR-u	87
Vladan M. Radulović, Vladan R. Durković Surge protection of resistive loads in low voltage power installations	88
Sanja Bauk, Tatijana Dlabač, Maja Škurić Internet of Things, High Resolution Management and New Business Models.....	89
Saso Gelev, Ana Sokolovska, Dusica Curcic, Aleksandar Sokolovski Usage of Genetic Algorithms in cryptography for mobile devices	90
Filip Drincic, Saša Mujovic Energy storage systems: an overview of existing technologies and analysis of their applications within the power system of Montenegro	91

Ivana Z. Giceva, Vasilija J. Sarac, Saso A. Gelev, and Vlatko T. Cingoski Single Phasing of Three Phase Induction Motor under Various Load Conditions.....	92
Marija V. Cingoska, Vasilija J. Sarac, Saso A. Gelev, Vlatko T. Cingoski Efficiency Optimization of Electrical Devices	93
Špiro Ivošević, Sanja Bauk The use of information technology in the assessment of the corrosion damage on ship hull	94
Slavica Tomovic, Igor Radusinovic A New Traffic Engineering Approach for QoS Provisioning and Failure Recovery in SDN-based ISP Networks	95
Norbert Varga, László Bokor, Ivana Ognjanovic, Ramo Sendelj On the Mobility Management Performance of NEMO-based Nested Wireless Body Area Networks.....	96
Stevan Šandi, Sanja Radonjić, Jovana Drobnjak, Marko Simeunović , Biljana Stamatović, Tomo Popović Smart Tags for Brand Protection and Anti - Counterfeiting in Wine Industry	97
Ana Grbovic, Ivana Ognjanovic, Ivan Vuckovic Security of AMR system in HPP Perucica	98
Wei-Kai Liou, Chun-Yen Chang Virtual Reality Classroom Applied to Science Education.....	99
Hasan Yetis, Mehmet Karakose Image Processing Based Anomaly Detection Approach for Synchronous Movements in Cyber- Physical Systems	100
Luka Lazović, Ana Jovanović, Vesna Rubežić Optimization of fractal antennas in CST with Chaotic optimization algorithm.....	101
Tatjana Stanivuk, Ištvan Bodolo, Nena Tomović, Biljana Kordić Application of Digital Forensics in Traffic Conditions	102
Slobodan Bundalevski, Vlatko Cingoski, Saso Gelev Determination of the total impulse of the solid rocket motor by using two mathematical methods.....	103
Biljana Stamatovic Implementation of CA algorithm for 3D components.....	104
Aleksandar Tudzarov, Saso Gelev 5G and Software Network paradigm	105
Draško Radovanović, Božo Krstajić Review Spam Detection using Machine Learning	106
Luka B. Bulatović, Goran R. Šuković On applying evolutionary algorithms for hybrid neural networks architecture synthesis.....	107

Zoran S. Veličković, Zoran N. Milivojević, Marko Z. Veličković A Secured Digital Video Watermarking in Chrominance Channel.....	108
Nikola Popović, Sanja Vujnović, Predrag Vasilić, Aleksandra Marjanović, Željko Đurović One approach to acoustic signals contamination detection	109
Kruna Ratković Notion of Strong Monad in Computing.....	110
Predrag Vasilić, Sanja Vujnović, Nikola Popović, Aleksandra Marjanović, Željko Đurović Adaboost algorithm in the frame of predictive maintenance tasks.....	111
Natalia S. Podzharaya, Anastasiia S. Sochenkova The virtual museum development with the use of intelligent and 3d technologies on the basis of the Maritime museum in Kotor	112
Trifun Savić, Milutin Radonjić WSN Architecture for Smart Irrigation System	113
Žarko Zečević, Božo Krstajić Low-Complexity Dynamic Synchrophasor Estimation Algorithm	114
Bozidar Skrbic, Draško Radovanovic, Slavica Tomovic, Luka Lazović, Zarko Zecevic, and Igor Radusinovic, A decentralized platform for heterogeneous IoT networks management.....	115
Ivan Jokić, Žarko Zečević and Božo Krstajić State-of-Charge Estimation of Lithium-ion Batteries using Extended Kalman filter and Unscented Kalman filter.....	116
Amar Kapić, Žarko Zečević and Božo Krstajić An Efficient MPPT Algorithm for PV Modules Under Partial Shading and Sudden Change in Irradiance	117
Sario Al Mustafa and Nikola Žarić MasterRoute: Android Application for Finding the Optimal Traffic Route.....	118
Miloš Brajović, Ljubiša Stanković, Miloš Daković Micro-Doppler Removal in Radar Imaging in the Case of Non-Compensated Rigid Body Acceleration.....	119

Metodi i alati za forenziku mobilnih telefona

Saso A. Gelev, Aleksandar Tudzarov, Vasilija J. Sarac, Vlatko T. Cingoski and Slobodan Bundalevski

Sadržaj — Mobilni telefon predstavlja multifunkcionalni telekomunikacijski uređaj, koji postaje neraskidljiv deo ljudske svakodnevnice. Mobilne telefone danas koriste sve generacije. Korisnici svoje mobilne telefone uvek nose sa sobom. Posedovanje više uređaja ili korisničkih brojeva više nije isključak već potreba. Mobilni telefoni su bogat izvor različitih podataka i informacija, počevši od ličnih podataka pa sve do podataka važnih za uspešno poslovanje preduzeća, državnih institucija i same države[1]. Ovo znači da je pitanje bezbednosti najviši prioritet, zato što su oni putem Interneta dostupni svakom korisniku bez odzira na nameru. U ovom radu dat je pregled načina, alata i procedura za akviziciju podataka koji se nalaze na mobilnim telefonima kao i specifične povezane sa forenzikom mobilnih telefona u krivičnim postupcima, od aspekta digitalnog dokaza kao suštinskog rezultata digitalne forenzičke analize.

Gljučne reči — mobilni telefon, digitalna forenzika, softverski forenzički alati

I. UVOD

MASOVNA upotreba mobilnih telefona, zbog njihove funkcionalnosti, jednostavne upotrebe i pristapnosti, pristupačne cene, mogućnosti da ga uvek nosite sa sobom, i široke lepeze različite moguće upotrebe uslovlje su da se javi veliki interes za njihovu upotrebu[1],[2]. Mobilni telefoni u krivičnom postupku mogu se nalaziti u nekoliko situacija: kao sredstvo za izvršenje krivičnih dela, kao objekat nad kojim je izvršeno krivično delo ili da bude nositelj dokaza koji se odnosi na određeni zločin (dokazi su različiti, brojni u digitalnom obliku).

Najčešće se u toku svake faze upotrebljavaju različiti uređaji.

Daleke 2003 godine Kris Samers u svom napisu „Mobile phones - the new fingerprints“ za BBC News kaže da je veliki broj ubojica u Velikoj Britaniji osuđeno zahvaljujući dokazima koji su bili povezani s njihovim

Saso A. Gelev, Assoc.Prof. Faculty of Electrical Engineering, University Goce Delcev - Stip, Macedonia, Address: „Krstes Misirkov“ No.10-A, P.O 201, Stip - 2000, R.Macedonia, (phone: 389-78-203759; e-mail: saso.gelev@ugd.edu.mk).

Aleksandar Tudzarov, Assoc.Prof. Faculty of Electrical Engineering, University Goce Delcev - Stip, Macedonia, Address: „Krstes Misirkov“ No.10-A, P.O 201, Stip - 2000, R.Macedonia, (phone: 389-78-203759; e-mail: aleksandar.tudzarov@ugd.edu.mk).

Vasilija J. Sarac, Assoc.Prof. Faculty of Electrical Engineering, University Goce Delcev - Stip, Macedonia, Address: „Krstes Misirkov“ No.10-A, P.O 201, Stip - 2000, R.Macedonia, (phone: 389-76-487069; e-mail: vasilija.sarac@ugd.edu.mk).

Vlatko T. Cingoski, Prof. Faculty of Electrical Engineering, University Goce Delcev - Stip, Macedonia, Address: „Krstes Misirkov“ No.10-A, P.O 201, Stip - 2000, R.Macedonia, (phone: 389-70-250210; e-mail vlatko.cingoski@ugd.edu.mk).

Slobodan Bundalevski, Asst.Prof. Faculty of Electrical Engineering University Goce Delcev - Stip, Macedonia, Address: „Krstes Misirkov“ No.10-A, P.O 201, Stip - 2000, R.Macedonia, (phone: 389-70-306980; e-mail: bobobundalevski@yahoo.com).

mobilnim telefonima ili mobilnim telefonima njihovih žrtava [3].

U SAD-u, na osnovu opsežne analize 2006-te godine konstatovano je da su oko 80% sudskih slučajeva na jedan ili na drugi način bili povezani sa digitalnim dokazima, izvedena iz zločina povezanih sa njima.[4].

II. DIGITALNI DOKAZI IZ MOBILNIH TELEFONA

Današnji mobilni telefoni su komunikacijski uređaji koji poseduju široku lepezu funkcija. Konstantni razvoj uvodi nove mogućnosti i veliki broj tehničkih unapređenja. Progresivni razvoj mobilnih telefona, naročito pametnih (smartphones), je u oblasti aplikativnog softvera (npr. repozitorij operativnog sistema Android poseduje najmanje 500.000 aplikacija [5], a App Store najmanje 700.000 aplikacija [6]).

Skladiranje, distribucija i obrada velikog broja podataka najrazličitijeg formata, čini mobilne telefone interesantne od aspekta forenzičkih i krivičnih postupaka kao izvora akvizicije digitalnih dokaza. Kao dokazi koriste se:

- SMS, MMS poruke i e-mail poruke sa podacima o onome koji šalje i prima poruke i vremenske podatke.
 - Podaci o podešenim vremenskim zonama na telefonu (ako nije sinhronizovana sa forenzičkim računarom), može dati pogrešne informacije o vremenu.
 - Fotografije, audio, video zapisi (naročito su interesantni za forenzičare ako su snimljeni na telefonu koji se analizira).
 - Aplikacije instalirane na telefonu.
 - Telefonski imenik, kalendar i druge PIM aplikacije.
 - Podaci povezani za upotrebom Internet aplikacije i podaci dobijeni upotrebom telefona za tu namenu, kao što je istorija aktivnosti (History), omiljene stranice, tj. njihovi fragmenti kada su u pitanju dinamičke stranice.
- Da bi sakrio svoje radnje, kriminalac često koristi više mobilnih aparata. Pri tome, podaci koji su značajni prestupniku čuva na SIM (Subscriber Identity Module) kartici. SIM kartica sadrži i sledeće podatke značajne za forenzičku analizu:
- Serijski broj kartice i podaci mobilnog operatora odakle se mogu dobiti podaci relevantni za istragu
 - Oblast gde se nalazio korisnik u trenutku kada je uređaj zadnju put upotrebljen pomoću LAI (Location Area Identifier).
 - Upotrebljene poruke, može ih biti 40 do 50 [7], čak i ako su izbrisane ili prekrivene drugim podacima, rekonstrukcijom određenim forenzičkim alatima.
 - Lista kontakata korisnika (današnji telefoni sadrže najmanje 250 kontakata).
 - Lista biranih brojeva.

Za vreme forenzičke istrage nikako ne smemo zaboraviti i mobilne celularne mreže. One sadrže podatke koji se mogu upotrebiti kao dokaz, a misli se na datoteku pozivanih brojeva (CDR – Call Data Record) koja je u vlasništvu operatora, a koja sadrži sve pozive u mreži[8]. Operator osim podatke koji su značajni za naplatu, kratko vreme, čuva i podatke koji njemu nisu bitni (primer ako je isključen telefon, baterija je prazna ili se isključi telefon iz bilo kog razloga, podaci kojima se otkriva gde se nalazio telefon kada je isključen. Ovo je naročito značajno kada se vodi istraga nestale osobe)[8].

III. FORENZIKA MOBILNIH TELEFONA

Forenzika mobilnih telefona je pod-disciplina digitalne forenzike i definiše se kao nauka koja se bavi sakupljanjem digitalnih dokaza iz memorije i SIM kartice u forenzičkim uslovima, upotrebom validnih prihvaćenih metoda [9].

Forenzičke metode za akviziciju podataka

Akvizicijom se sakupljaju podaci iz inkriminiranih uređaja, ali sve radnje koje se izvode moraju sačuvati integritet podataka. Moraju se strogo poštovati određeni principi [10]:

- Sve preduzete akcije ni u kom slučaju ne smeju narušiti integritet podataka (ne smeju se menjati), neovisno dali su oni na mobilnom telefonu ili na memoriskoj kartici.
- Ljudi koji pristupaju podacima moraju biti kompetentni i sposobni da objasne svaku aktivnost koju preduzimaju.
- Neophodno je precizno dokumentovati svaki korak preduzetih aktivnosti.
- Osoba koja vodi istragu ima odgovornost da obezbedi poštovanje ovih principa i sprovedi aktivnosti u skladu sa važećim propisima.

Tokom forenzičke istrage, prvi princip najteže je poštovati. Naime, napadnuti telefon se uključuje ili isključuje. Ako je isključen, moramo ga uključiti i spojiti na sudski računar. Postoji velika verovatnoća da će to biti zamka koja bi oštetila ili izbrisala podatke. Ako je promena podataka neizbežna, neophodno je učiniti što manje promena. [11].

Kada govorimo o akviziciji podataka mobilnog telefona, govorimo o akviziciji unutrašnje memorije. .

Razlikujemo dva tipa pristupa za akviziciju mobilnih telefona [12] :

- Akvizicija koja se izvodi na logičkom nivou. To je u stvari prikupljanje podataka iz memorije mobilnog telefona uz pomoć operativnog sistema telefona.
- Akvizicija koja se izvodi na fizičkom nivou. To je u stvari kopija ukupne memorije. Kopira se bit po bit i na taj način se prikupljaju podaci i iz prostora koji operativni sistem ne nalazi, odnosno rekonstrukcija izbrisanih podataka.

Ručni pregled mobilnih telefona

To je teška metoda akvizicije koja zahteva duži vremenski period. To je logički nivo pristupa koristeći aplikacije koje su dostupne na telefonu. Naime, ručnim pristupom svakom sadržaju pretraživanja različitih menija

i podmenija, podaci se preuzimaju bez automatskog procesa. Forenzička osoba mora detaljno da upozna telefon kako bi smanjila greške. Konkretno sa forenzičkog aspekta SMS poruke su važne. Zbog toga, proces njihovog skidanja mora biti siguran, jer u izveštaju mora biti prenet njihov nepromenjen originalni sadržaj [12].

Greške ne smeju biti dozvoljene. Poseban izazov su najnoviji jeftini telefoni koje prodaju-doniraju operateri. Najčešće nemaju korisan interfejs za povezivanje sa forenzičkim uređajem, ali zato poseduju veliki kapacitet gde se čuvaju SMS poruke. Tokom forenzičke analize, telefon mora biti uključen. U tom periodu postoji opasnost od primanja novih poruka, poziva itd. što će narušiti analizu. Zbog toga telefon se postavlja u tkz Faradejev kafaz koji blokira uticaj bilo kog eksternog električnog polja ili se klonira SIM kartica (na praznoj kartici se snimaju ICCID I IMSI brojevi, sa kojom telefon radi ali nema pristup mobilnoj mreži).

Akvizicija pomoću konekcionih servisa

Akvizicija pomoću konekcionih servisa trenutno je najčešći metod koji se zasniva na funkcionisanju forenzičkih alata koji koriste protokole za slanje komandi i prijem podataka za komunikaciju sa servisima. To je akvizicija na logičkom nivou, koristeći otvorene protokole [13] kao što su AT Command Set, SyncML ili OBEX koji su zastareli ili fabrički protokoli kao što je Nokia FBUS [14]. Postoje i razvojni alati [15] koji omogućavaju programerima da kreiraju aplikacije koristeći usluge mobilnih telefona bez primene osnovnih protokola.

Postoje dve vrste alata za akviziciju: neforenzički i forenzički alati.

Neforenzički alati uglavnom su namenjeni za sinhronizaciju komuniukacije mobilni telefon - računar ili za pravljenje rezervnih kopija. Moramo biti izuzetno oprezni kada koristimo ove alate jer oni mogu ozbiljno oštetiti vjerodostojnost preuzetih podataka ili ih predstaviti u formatu koji je neupotrebljiv za forenzički izveštaj. (npr. Nokia PC Suite SMS poruke prikazuje samo tabelarno i nedozvoljava kopiranje podataka, i ne daje nikakav njihov eksport).

U drugoj vrsti alata za akviziciju (forenzički alati) spadaju:

- Forensic Tool Kit (FKT),
- EnCase,
- Expert Witness,
- Norton Utilities,
- Hashkeeper,
- HexEditor,
- SMARTLinux,
- ForensiX
- Logicube CellDEK;
- MicroSystemation XRY
- MicroSystemation XRY i dr.

Oni koriste iste protokole kao i neforenzički alati, ali ne implementiraju komande koje eksplicitno menjaju sadržaj mobilnih telefona. Ipak, nije garancija da njihovom

upotrebom nećemo modifikovati sadržaj mobilnog telefona [16], jer komande za akviziciju mogu dovesti do toga da operativni sistem menja podatke.

Konekcioni agenti

Predstavljaju mali programi koji se instaliraju na uređaju da bi obezbedili konekciju između telefona i forenzičkog alata. Ovaj pristup koristi klijent-server arhitekturu, gde agent igra ulogu servera. Bez agenta alat ne može dobiti podatke sa telefona.

Ovaj se metod najčešće koristi kod pametnih telefona. Mora se naglasiti da bez obzira što ovaj softver zauzima mali prostor, mora se snimiti (instalirati) u memoriju pametnog telefona, čime se deo njegovog sadržaja briše.

Pristup memoriji direktno [2]

Ovaj pristup memoriji mobilnog telefona se najbolje slaže sa forenzičkim principima, ali ujedno zahteva i najkompleksniji hardverski i softverski sistem (finansiski najskuplji) [7]. Ovim pristupom se prikupljaju podaci celokupne memorije telefona, neovisno od zauzetog kapaciteta i to na fizičkom nivou. Direktni pristup dozvoljava oporavak izbrisanih ili delimično istisnutih podataka, kao i zaobilaznje sigurnosnih mera koje onemogućavaju pristup podacima na logičkom nivou. Druge metode ne mogu izbeći ove mere bez dodatnih intervencija čiji uticaj može ugroziti integritet prikupljenih dokaza.

Postoje nekoliko metoda direktnog pristupa [12]:

- Prva metoda podrazumeva odstranjivanje memorijskog čipa sa štampane ploče mobilnog telefona i očitavanje njegovog sadržaja (Ovo je relativno rizična metoda jer se čip uklanja zagrevanjem leмова na ploči. Razvijena temperatura može oštetiti čip, a time i potencijalne digitalne dokaze).

- Druga metoda direktnog pristupa koristi JTAG porte za test (Joint Test Action Group, standardizirana procedura koja se upotrebljava za testiranje interkonekcije štampane ploče i blokova unutar integriranog kola [17]) u cilju pravljenja kompletnih forenzičkih kopija sadržaja promenljive i nepromenljive memorije telefona. Najveći nedostatak u najnovijim modelima telefona je činjenica da je vrlo teško doći do porte jer je proizvođač sakriva [12].

- Treća metoda direktnog pristupa koristi alat za flešovanje (flasher tools) namenjen za programiranje memorije uređaja (EEPROM ili fleš memorije), ali i za dijagnostiku i otkrivanja grešaka. Postoje nedostaci u primeni ove metode: u nekim slučajevima, samo se deo memorije može čitati; različiti proizvođači koriste različite pristupe interfejsu tako da se generalna primenljivost ne može postići [12].

Potrebni su kvalitetni uslovi za rad, visok nivo znanja i tehničkog obrazovanja da bi primenili bilo koju gore pomenutih metoda. Međutim, veliki nedostatak u pogledu drugih metoda jeste činjenica da ona pruža sirove podatke koji se moraju dodatno analizirati, razdvojiti značajne i korisne informacije, odnosno dokaze koji se mogu predstaviti u razumljivoj formi.

Mobilne celularne mreže i prikupljanje podataka

Telefon radi u okviru mobilne celularne mreže [18]. Podatke koje beleži mrežni sistem mogu se koristiti za forenzičku analizu telefona. Pre svega mogu se razdvojiti detaljni podaci za komunikaciju u oba smera u dužem vremenskom periodu. Ovi podaci su mnogo vredniji od podataka izvučenih iz samog telefona. Zbog toga se ovaj metod često koristi za validaciju podataka dobijenih drugim metodama.

Ne postoji idealna metoda za prikupljanje podataka, ali u praksi se koristi kombinacija višestrukih metoda i pristupa u pravcu postizanja optimalne efektivnosti i efikasnosti. Forenzičar, na osnovu operativnih podataka, bira koje metode će koristiti sa kojim prioriteto za svaki pojedinačni slučaj, pokušavajući da prikupi što više digitalnih dokaza, čime se smanjuje rizik promene sadržaja telefona.

Da bi dokazao da svojim aktivnostima ne krši integritet telefona, forenzičar mora u najvećoj meri minimizirati interakcije sa uređaja i dokumentovati bilo koju aktivnost. Što je broj interakcija veći, komplikovanije je dokazati da ove aktivnosti nisu kompromitovali digitalne dokaze [13]. Ako je mobilni telefon zapečaćen u posebnoj kovrtu u prisustvo i sa potpisom osumnjičenog i njegovog advokata, i u njihovom prisustvu, koverat se otvara i vrši forenzička analiza, onda se primljeni podaci mogu koristiti kao validni digitalni dokazi, tj. ukloniti svaku sumnju.

IV. ALATI ZA FORENZIKU MOBOLNIH TELEFONA

Alati forenzičke analize mobilnih telefona mogu se podeliti u dve osnovne grupe: Alati čija je glavna funkcija forenzička analiza i alati koji imaju drugu namenu, ali ih je proizvođač softvera nadgradio forenzičkim funkcijama (npr. Mobile Phone Examiner Plus i Neutrino firme Guidance Software).[2]. Daćemo pregled nekoliko alata.

XRY je alat za digitalnu forenziku mobilnih uređaja švedske tvrtke Micro Systemation koja se koristi za analizu i oporavak podataka s mobilnih uređaja kao što su mobilni telefoni, pametni telefoni, GPS navigacijski alati i tablet računala. Sastoji se od hardverskog uređaja koji omogućuje povezivanje telefona s računalom i softver za izdvajanje podataka (SI.1).



Slika 1. MicroSystemation XRY

XRY trenutno može da vrši akviziciju na više od 3000 različitih modela mobilnih telefona, da napravi forenzičku kopiju memorije na više od 1000 modela, i da dekodira forenzičke kopije na više od 1000 telefona.

Iste principe rada koristi i alat Cellebrite UFED, s tom razlikom što su hardverske i softverske komponente smeštene u jednom uredu, i zbog toga nije potreban

računar za akviziciju podataka (Slika 2). Podržava logičku akviziciju podataka više od 3000 modela mobilnih telefona. Može da prikuplja i dekodira podatke na fizičkom nivou na preko 1000 različitih modela, kao i da izdvoji šifre na više od 750 modela.



Slika 2 Cellebrite UFED

Logicube CellDEK omogućava akviziciju samo na logičkom nivou na preko 2000 različitih modela mobilnih telefona (Slika 3).



Slika 3 LOGICUBE CellDek F-LC7000 Police Forensic Cell Phone Data Extraction Analyzer

MOBILedit je samo aplikacija koja obezbeđuje vezu između mobilnog telefona i računara pomoću Bluetooth, Infrared ili USB kabla, u zavisnosti od modela telefona. Koristi se za očitavanje SMS poruka, logova poziva, fotografija i drugih važnih podataka sa mobilnog telefona.



Slika 4 Mobiledit

Ovi alati omogućavaju akviziciju podataka i sa GPS uređaja i tableta kao što su iPad, Galaxy Tab što je i normalno jer ovi uređaji koriste operativne sisteme iOS i Android koji se takođe koriste u mobilnim telefonima.

Analiza prikupljenih podataka (sa mobilnog telefona i sa operatera) vrši se uz pomoć analitičkog softvera za izradu šematskog prikaza..

Rezultati akvizicije se mogu eksportovati u različitim oblicima (tabelarni prikaz prikupljenih podataka sa telefona sa svim detaljima, do eksportovanje datoteka) u forenzičkoj laboratoriji, gde se u laboratorijskim uslovima obrađuju u vidu digitalnih dokaza, a dokazi se čuvaju i pripremaju za prezentaciju istražnim i sudskim organima.

V. ZAKLJUČAK

Zajednica forenzičara za mobilne telephone stalno se součava sa izazovima i mora da je u toku sa najnovijim tehnologijama (sa aspekta razvoja mobilnih telefona i sa

aspekta razvoja forenzičkih metoda i tehnika) kako bi se otkrili relevantni tragovi u toku istrage [7].

Proizvođači mobilnih telefona često menjaju konekcijske servise i operativne sisteme. Na taj način oni otežavaju posao forenzičara (moraju edukaciski i resursno da budu u skladu sa promenama), a isto tako otežavaju posao i proizvođačima forenzičkih alata (menjaju i usavršavaju svoje proizvode čime se povećava cena).

Forenzičari moraju stalno da prate način izvršavanja krivičnih dela i da usavršavaju svoje postupke u otkrivanju digitalnih dokaza [19].

Pošto digitalni dokazi i njihovi izvori (mobilni telefoni) dobijaju sve veći značaj u krivičnom postuku, forenzičari su primorani da za svaki zasebni slučaj koriste različite alate, postupke i metode. Iako cela procedura pri skupljanju digitalnih dokaza sa mobilnih telefona u krivičnom zakonu Republike Makedonije nije do kraja jednoznačno definisana, poštovanjem postojećih propisa o privremeno oduzetih predmeta i poštovanje osnovnih kriminalističkih i forenzičkih principa, može se osigurati kredibilitet digitalnih dokaza, što je i cilj digitalne forenzike.

LITERATURA

- [1] Hristov R., Kaević Z., „Detektivska informatika“, EURM Skoplje 2011
- [2] Vuković Igor, „Digitalna forenzika mobilnih telefona za potrebe krivičnog postupka“ telekomunikacije.rs
- [3] Summers C., "Mobile phones - the new fingerprints", BBC News, 2003
- [4] Rogers M., "A Practical Approach to Digital Crime Scene Analysis", Department of Computer Technology, Purdue University, 2006
- [5] <http://www.appbrain.com/stats/number-of-android-apps>
- [6] [http://en.wikipedia/wiki/App_Store_\(iOS\)#Number_of_launched_applications](http://en.wikipedia/wiki/App_Store_(iOS)#Number_of_launched_applications)
- [7] Willassen S., "Forensic analysis of mobile phone internal memory", Norwegian University of Science and Technology, 2005
- [8] Willassen S., "Forensics and the GSM mobile telephone system", International Journal of Digital Evidence, 2003.
- [9] Jansen W., Ayers R., "Guidelines on Cell Phone Forensics", National Institute of Standards and Technology, U.S. Department of Commerce, 2007
- [10] Ayers, R., Jansen, W., Cilleros, N., Daniellou, R., "Cell phone forensic tools: An overview and analysis", National Institute of Standards and Technology, Gaithersburg, Maryland 2005.
- [11] Carrier, B., "Open source digital forensic tools – the legal argument", Research report, At Stake, 2002
- [12] Keonwoo Kim, Dowon Hong, Kyoil Chung, Jae-Cheol Ryou, "Data Acquisition from Cell Phone using Logical Approach", Proceedings of World Academy of Science, Engineering and Technology, 2007.
- [13] Mokhonoana P., Olivier M., "Acquisition of a Symbian smart phone's content with an on-phone forensic tool," Proceedings of the Southern African Telecommunication Networks and Applications Conference 2007 (SATNAC 2007), Sugar Beach Resort, Mauritius, September 2007.
- [14] Kot, P. and Zoltan, B. (2006). gnokii project. Website.
- [15] McDowall, I., "Programming PC Connectivity Applications for Symbian OS", Wiley, 2004.
- [16] McCarthy, P., "Forensic analysis of mobile phones", Master's thesis, University of South Australia, 2005.
- [17] http://en.wikipedia.org/wiki/Boundary_scan
- [18] Croft, N., "Secure interoperation of wireless technologies", Master's thesis, University of Pretoria, 2004.
- [19] Milosavljević M. Grubor G. Digitalna forenzika – udzbenik, Univerzitet Singidinum, Beograd 2009

ISBN 978-86-85775-22-2



9 788685 775222 >