

MOBILNI TELEFON KAO IZVOR INFORMACIJA: ŠTA MOŽE DA PRUŽI PRI ISTRAZI

Dragutin Vukotić, MSc
IT / Telecom Management Consultant
dragutin@wdlp.jazztel.es

Abstrakt: Mobilna telefonija je prihvaćena širom sveta. Poslednjih godina broj korisnika je porastao na dramatičan način. Moderni mobilni telefoni čuvaju sve više informacija o svom vlasniku: pored podataka o pozivima, poslatim i primljenim porukama, brojevima telefona u imeniku, sve više se koriste za druge svrhe. Poseduju foto-kameru za fotografije i video snimke, reprodukciju muzike, video igre i razne druge namene. Sa velikom i rastućom svakodnevnom upotrebom, jedan takav izvor informacija kakav je mobilni telefon, prosto je nezamislivo ne uzeti u obzir kao sastavni deo bilo koje istrage.

Ključne reči: mobilna telefonija, forenzika, digitalni dokazni materijal

Mobile Phone as an Information Source:

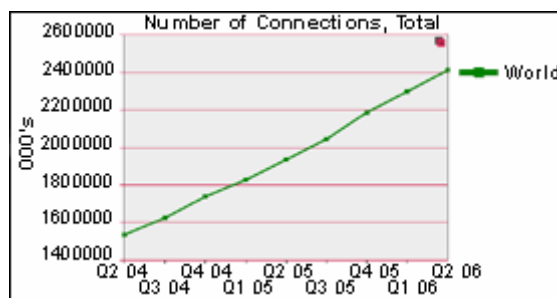
WHAT DOES IT MEAN FOR AN INVESTIGATION

Abstract: Mobile communication is widely accepted across the world. During last period the number of user has increased in a dramatic way. Mobile phones keep an increasingly high volume of information about its owner: a part from the recent call list, received and sent messages, the phone book, they are also used in a number of different ways. Often they will have a camera for photos and video clips, music players, video games etc. With frequent daily use such a source of information as it is a mobile phone, cannot be overseen in any investigation.

Keywords: mobile phone, forensic, digital evidence.

MOBILNA TELEFONIJA: OSNOVNI PRINCIPI

Polovinom 2006 godine bilo je preko 2 milijarde korisnika od kojih je GSM najrasprostranjenija tehnologija, prisutna u 210 zemalja širom sveta, sa 269 miliona korisnika u Istočnoj i 383 miliona u Zapadnoj Evropi. To znači da oko 70% stanovništva ovoga kontinenta nosi sa sobom urđaj koji mnogo toga može reći o životu i navikama svog vlasnika. Osim GSM, postoje i CDMA, naročito rasprostranjena u Severnoj i nešto manje u Južnoj Americi, zatim UMTS kao takozvana 3 generacija mobilne telefonije itd.



Rast broja mobilnih korisnika u svetu

Izvor: www.wirelessintelligence.com

Razmena informacija ovim putem je zapanjujuća: prvog trimestra 2006 poslato je 235 milijardi SMS poruka u celom svetu (CellularOnline, www.cellular.co.za).

Mobilni telefon se sastoji od dva elementarna dela.

1. Mobilni aparat (ME - mobile equipment) je terminal koji korisniku služi za komunikaciju unutar GSM mreže. Neophodna je SIM kartica da bi pristup mreži bio moguć.
2. SIM Subscriber Identity Module: "smart" ili "inteligenta" kartica. Sadrži korisnikov broj, kodirane identifikacione podatke za mrežu, PIN (personal identification number: lični broj za identifikaciju), i razne ostale podatke kao telefonski imenik itd.

SIM kartica je u suštini specijalna vrsta smart kartice koja tipično ima procesor i između 16 i 128 Kb memorije tipa EEPROM. Takođe ima radnu memoriju (RAM) koja se koristi prilikom realizacije programa, i pre-programiranu memoriju sa operativnim sistemom i algoritmima za autorizaciju korisnika i enkripciju podataka (ROM).

Podaci su organizovani u specijalni fajl sistem i zaštićeni sa nekoliko sigurnosnih nivoa, koji omogućavaju kontrolu pristupa. Postoje sledeći nivoi zaštite: slobodan pristup, pristup sa PIN, pristup sa PIN2, administrativni i zatvoreni deo.

INFORMACIJE KOJE ČUVA MOBILNI TELEFON

Mobilni telefon pruža mogućnost za čuvanje raznovrsnih informacije. Imajući na umu opisanu tehnologiju, podaci se mogu naći na SIM kartici i u samom telefonskom aparatu.

SIM kartica

1. Informacije o korisničkom broju: jedinstven identifikator SIM kartice (ICCID), međunarodni identifikator mobilnog pretplatnika (IMSI), međunarodni pretplatnički broj (MSISDN), i opcionalno naziv mobilnog operatora (SPN)
2. Telefonski imenik i podaci o pozivima: lista imena i brojeva telefona koje je uneo sam korisnik (ADN), lista poslednjih pozvanih brojeva (LND).
3. Poruke: mogu biti samo tekst (SMS) ili multimedija (MMS), primljene, poslate. Informacije o lokaciji: informacija o lokaciji aparata (LOCI), informacija o zoni lokacije (LAI).

Mobilni aparat

U zavisnosti od modela, može da sadrži informacije slične samom SIMu: telefonski imenik, fotografije, pozivni muzički tonovi, poruke, itd. Razlika je pre svega u formatu čuvanja informacija koji su zavisni od modela aparata, i u količini memorije. Savremeniji modeli imaju mogućnost čuvanja velike količine podataka na ugrađenoj ili spoljnoj memoriji (tkzv. Flash kartice).

Mobilni operator

- Istorijat poziva, poruka itd.
- PUK kod, koji desblokira PIN i samu SIM karticu i aparat.

Procedura istrage

Prikupljanje digitalnih podataka je vrlo osetljivo pitanje. Sa jedne strane neke vrlo jednostavne radnje mogu promeniti ili „uprljati“ postojeće podatke. Sa druge strane, metod prikupljanja podataka mora biti perfektno jasan da može poslužiti kao neoboriv sudski dokaz.

Naprimera jednostavno vadenje baterije iz mobilnog aparata može sa jedne strane, sačuvati jedan deo podataka, ali istovremeno nepovratno izbrisati druge podatke, kao naprimera lokalna podešavanja, datum, vreme, poruke, i sve u zavisnosti od modela i proizvođača.

Prenošenje mobilnog aparata sa jedne lokacije na drugu, na primer, promeniće informaciju o lokaciji telefona. U isto vreme, dok je telefon uključen i pristupan GSM mreži, može primati pozive, poruke itd. U nekim slučajevima to se može zloupotrebiti od strane vlasnika ili saradnika – koristeći ovu mogućnost da bi se „preplavila“ memorija SIM kartice ili aparata. Naime, neki modeli čuvaju samo poslednjih N poziva ili poruka, po principu „buffer“-a FIFO (first in first out): ako pozovemo ili pošaljemo dovoljan broj puta sa napr. javnog telefona, podaci o ranijim pozivima i porukama se mogu izbrisati.

Imajući sve to u vidu, mobilni telefon koji se želi iskoristiti za analizu ili dokaz, preporučljivo je uvek na licu mesta staviti u „faraday“ vrećicu (radi se od tri metala, bakar, nikel i srebro i deluje kao izolator za radio talase koji se koriste i u mobilnoj telefoniji).

Na mestu istrage, osim uobičajenih postupaka za svaku istragu, uobičajeno je:

- Ne uključivati / isključivati aparat.
- Fotografisati ekran aparata ako je isti uključen.
- Staviti aparat u „faraday“ vrećicu.
- Pretražiti mesto istrage za bilo koje predmete koji mogu biti u vezi sa aparatom: SIM kartica, memorijska kartica, baterija, kablovi, upustvo za upotrebu itd.

Istraga u laboratoriji:

- Identifikovati proizvođača i tačan model aparata.
- Probati dobiti PIN / PUK identifikator, u slučaju da je aparat blokiran.

- Probati iskopirati sve podatke na PC računar, gde se mogu slobodno analizirati.
- Vreme je kritično: ako se baterija potroši i aparat isključi, mnogo podaci mogu biti izbrisani.

Istraga može biti ni malo lak proces: dok su računari dosta standardni, mobilni telefoni su toliko različiti od modela do modela, da jednom uspešno primenjen proces sa jednim aparatom, može lako biti potpuno beskoristan u drugom slučaju.

Alati za istraživanje i analizu

Imajući u vidu tehnološke aspekte, kritičnost vremena i potrebu da se sačuva integritet podataka, preporučljivo je koristiti specijalizovane hardver i softver alate za prikupljanje i analizu podataka.

Kritičan deo istrage je čuvanje integriteta podataka. Time se sa osigurava tačnost i kredibilnost zaključaka, ali se i ostavlja mogućnost za ponavljanje celog postupka analize, kada je to potrebno, naprimer u svetlu novih informacija.

Neki od postojećih softver alata su: GSM .XRY, SIMCon, TULP 2G, ForensicSIM, Forensic Card Reader, Cell Seiyure, etc

ZAKLJUČAK

Mobilni aparatu su nezaobilazan izvor informacija o svom korisniku. Dobro usmerena i vođena analiza može pružiti ključne podatke o istrazi, koji vode njenom daljem napretku ili čak i uspešnom zaključivanju. U isto vreme, glavni izazovi forenzike mobilnih aparata su:

- Prikupljanje podataka iz, zbog ne postojanje standarda operativnih sistema, i naročito iz nestandardnih modela i proizvođača;
- Očuvanje integriteta podataka do mere da mogu da služe kao neprikosnoveni dokaz i da služe za ponovljene analize;
- Vreme je kritično: deo podataka se može nepovratno izgubiti ako se ne sačuvaju u kratkom vremenskom periodu.

REFERENCE

1. **Tyler Moore**, The Economics of Digital Forensics
2. **Rick Ayers, Wayne Jansen, Nicolas Cilleros, Ronan Daniellou**. Cell Phone Forensic Tools: An Overview and Analysis (NISTIR 7250). National Institute of Standards and Technology
3. **Eoghan Casey**, Chapter 13: Forensic Examination of Handheld Devices, Digital Evidence and Computer Crime, 2nd edition, Academic Press, March 2004.
4. **Rick Ayers, Wayne Jansen, NIST Interagency Report (IR) 7100, August 2004**, PDA Software Tools: Overview and Analysis, <http://csrc.nist.gov/publications/nistir/nistir-7100-PDAForensics.pdf>
5. **GSM World, Mobile Terms & Acronyms, 2006**, <http://www.gsmworld.com/technology/glossary.shtml>
6. **GSM World, GSM Global Networks on Air** http://www.gsmworld.com/news/statistics/networks_complete.shtml