SUDSKA VEŠTAČENJA IZ OBLASTI MOBILNE TELEFONIJE

Saša Savić, Telekom Srbija
sasas@telekom.yu

Apstrakt: *U radu su prikazani osnovni pojmovi iz oblasti Mobilne telefonije, način rada, složenost sistema, opisi scenarija različitih poziva (CALLDataRecorda), kao i neki primeri veštačenja koja su u proteklom periodu došla od strane sudova.*
Nedostaje abstract

UVOD

Razvitak mobilne telefonije kako u svetu, tako i u Srbiji,doveo je do raznih tehnoloških i telekomunikacionih pogodnosti za komunikaciju među ljudima.Samim tim, mobilnošću, razvijanjem raznih novih servisa (SMS, MMS, GPRS, 3G, VideoCall, mail, Internet sa mobilnog telefona), usavršavanjem i razvitkom novih servisa sigurno je doprinelo, kao svaka nova tehnologija, do razvitka i boljitka svakog društva, ali u sebi je sadržala i mogućnosti za delovanje i razvitak raznih kriminogenih i nedozvoljenih radnji. Mobilni telefon je postao tako jedan od najčešće korišćenih alatki za razne vidove komunikacije i prevare te stoga, često korišćen, postao i nezaobilazni deo mnogih dokaznih postupaka, za različita kriminogena dela.

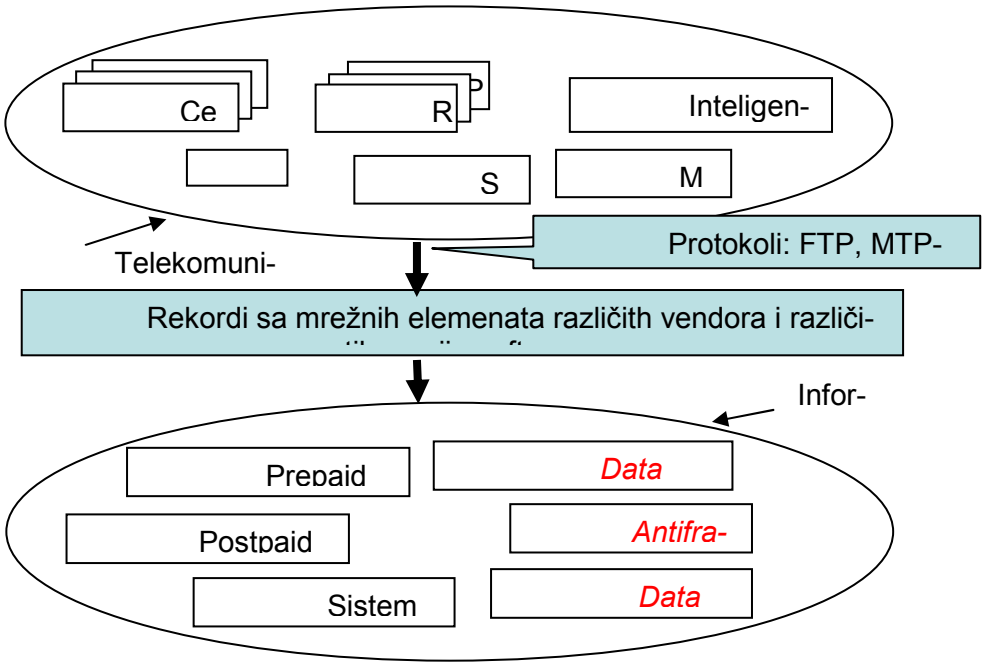
1. PRIKAZ RADA MOBILNE TELEFONIJE I SCENARIJI SAOBRAĆAJA

Mobilna telefonija Srbije, kao deo Telekoma Srbije, je nastala i počela sa radom 1998. godine. U početku sa malim brojem baznih stanica imala je i mali broj korisnika. Mobilna telefonija danas ima:

- 3.000.000 korisnika *prepaid* usluga
- 390.000 *postpaid* korisnika

Ona pokriva oko 98% teritorije Srbije i ima skoro 201 ugovor o romingu u 115 zemalja po celom svetu. Razvijen je i prepaid roaming servis tako da i mnogi naši korisnici koji imaju prepaid kartice mogu imati roaming sa određenim operaterima u svetu sa kojima imamo potpisan ugovor.

Složeni sistemi svakog mobilnog operatera može se grubo podeliti na dva dela: radio- telekomunikacioni i informatički deo, Slika 1.



Slika 1. Gruba podela sistema mobilnih operatera

Telekomunikacioni deo pruža krajnjim korisnicima (pretplatnicima) telekomunikacioni servis. Sastoji se od mrežnih elemenata (NE – *Network Elements*). Mrežni elementi su:

- centrala mobilne telefonije (MSC – *Mobile Switching Center*)
- centar za kratke poruke (SMSC – *Short Message Service Center*)
- centar za multimedijalne poruke (MMSC – *Multimedia Message Service Center*)
- SGSN – *Serving GPRS Suport Node*
- GGSN – *Gateway GPRS Support Node*, inteligentna mreža.

Ovi mrežni elementi, pored toga što omogućavaju telekomunikacione servise, generišu *fajlove* sa *zapisima podataka* (o pozivu ili nekom događaju), koji su namenjeni informatičkom delu mobilnog operatora, zarad naplate, statistike i drugih obrada.

Sistem za naplatu ili informatički deo čine:

1) posrednički sistem (u Ericsson-ovoj terminologiji EMM – *Ericsson Multi Mediation*), koji vrši predobradu zapisa podataka (pristiglih sa mrežnih elemenata): dekodiranje, filtriranje, formatiranje, grupisanje, kodiranje i
2) postobradni sistemi (PPS – *Post Processing System*), od kojih su neki: *prepaid* sistem za naplatu, *postpaid* sistem za naplatu, sistem za statistiku i *Data Warehouse* sistem mobilne telefonije u kome se smeštaju svi *call datarecordi*.

Fajlovi koji stižu sa centrala mobilne telefonije su sačinjeni od zapisa podataka koji u svojoj strukturi imaju *polja*, koja mogu biti brojevi, nizovi karaktera, ili složene strukture sačinjene od *podpolja*. Govorni servis, koji je, inače, kod mobilnog operatora najzastupljeniji, zahteva sopstveni tip zapisa podataka, *zapis podataka o pozivu* (*CDR*)[1]. CDR sadrži sve relevantne podatke o određenom (svakom) pozivu, kao što su, npr. broj pozivajućeg korisnika, broj pozvanog korisnika, trajanje poziva, itd. U zavisnosti od scenarija saobraćaja generišu se različiti tipovi CDR-ova.[2] U daljem izlaganju biće opisani bitni CDR-ovi za funkcionisanje mobilnog operatora. Nadalje, daćemo neke primere različitih scenarija poziva (da bi se korektnije stvorila slika) radi islustracije složenosti sistema koja se koristi kasnije kao (složena) šema za konkretna veštačenja.

Scenarija poziva *Call Data Record*-a

MOC (*Mobile Originating Call*) predstavlja *odlazni poziv*. MSC (*Mobile Switching Centre*), na kojoj je mobilni pretplatnik registrovan (na strani pretplatnika koji poziva), generiše odgovarajući CDR.

MTC (*Mobile Terminating Call*) predstavlja *dolazni poziv*. MSC, na kojoj je pozvani mobilni pretplatnika registrovan, generiše odgovarajući MTC CDR. Namenjen je za eventualno tarifiranje pozvanog korisnika, koje se sprovodi u izuzetnim slučajevima. Po strukturi se ne razlikuje od MOC CDR-a, s tim što se vrednosti pojedinih polja sada odnose na pozvanog korisnika.

TRN (*Transit Call*). CDR predstavlja tranzitni zapis podataka o pozivu, a tiče se *tranzitnog poziva*. Generiše se u slučaju komunikacije između centrala mobilne telefonije. Na primer, kada pozivajući pretplatnik ne pripada domaćoj mreži (HPLMN (*Home Public Land Mobile Network*)). Tada se generiše više tranzitnih zapisa, a najvažniji (jer služi za tarifiranje na relaciji mobilni operator-mobilni operator (*interconnect charging*)) je onaj generisan na domaćoj centrali preko koje je domaća mreža povezana sa spoljašnjom. Ta centrala nosi naziv GMSC (*Gateway* MSC). Tranzitni zapisi nastali u drugim slučajevima se uglavnom ne razmenjuju zbog rasterećenja veza po kojima bi putovali.

RCF (*Roaming Call Forwarding*) predstavlja slučaj rominga. RCF CDR se generiše kada GMSC uspostavi vezu sa pozvanim domaćim (HPLMN) pretplatnikom, što se

može ostvariti ili posredno, preko neke MSC, ili direktno, za slučaj da je pozvani pretplatnik registrovan neposredno na GMSC. RCF CDR ne služi za tarifiranje kada se pozvani domaći pretplatnik nalazi u samoj domaćoj mreži, te se u tom slučaju, najčešće, ni ne generiše. Od interesa je slučaj kada je pozvani domaći korisnik u romingu, tj. kada je registrovan na nekoj centrali u nekoj spoljašnjoj, stranoj mreži (VPLMN (*Visited Public Land Mobile Network*)).

CF (*Call Forwarding*) označava slučaj *preusmeravanja poziva*. CF CDR se generiše kada pozvani pretplatnik preusmeri poziv.

MO-SMS (*Mobile Originating* SMS). CDR se generiše se pri *slanju SMS poruke*. Može nastati na dva mesta: u MSC-u (odnosno MSC/VLR-u) – koristi se za tarifiranje, jer nosi više informacija – i u SMS-IWMSC-u (*Interworking* MSC).

MT-SMS (*Mobile Terminating* SMS). CDR se generiše se pri *primanju SMS poruke*. Može nastati na dva mesta: u MSC-u (odnosno MSC/VLR-u) – koristi se za tarifiranje, jer nosi više informacija – i u SMS-GMSC-u.

Kompozitni CDR. Kompozitni tip CDR-a po svojoj strukturi predstavlja sklop više CDR-ova. Koristi se u centralama mobilne telefonije, u slučaju da pretplatnik koristi servise inteligentne mreže (*Intelligent Network* (IN) servise), kao što je npr. servis skraćenog biranja ili popularno nazvani VPN postpaid korisnici.

GPRS (SGSN i GGSN). Recimo, najpre, nekoliko reči o GPRS (*General Packet Radio Service*) sistemu mobilne telefonije. Označava se kao generacija 2.5 (2.5 G). Predstavlja nadogradnju 2. generacije (GSM (*Global System for Mobile*)), na njenom putu ka 3. generaciji. 2.5 G je kompatibilna sa 2 G (zadržani su svi 2 G servisi), i nastala je izmenama samo upravljačko-komutacionih čvorova u 2 G mreži, a korišćenjem iste postojeće ćelijske i radio strukture. Omogućava paketski prenos podataka na radio-interfejsu, sa maksimalnom brzinom prenosa do 115 kb/s, a tipičnom oko 50 kb/s (za pretplatnika). Koristi se princip udruživanja vremenskih slotova u okviru jednog radio-nosioca. Veza se uspostavlja brzo (ne *dial-up* konekcijom).

TAP file (*Transfer Account Procedure*). je fajl koji služi za dostavu CDR-ova (i naplatu poziva) koji nastaju kada je korisnik u romingu. Razmenjuje se između centrala dva mobilna operatora u dve različite države. Relativno se retko razmenjuje, otprilike jednom dnevno. TAP fajl sadrži jedan CDR koji obuhvata veliki broj MOC, MTC, i drugih CDR-ova.

IMEI, broj je najčešće sastavljen od 15 cifara od kojih svaka ima svoje značenje. Ovaj broj možemo podeliti i u četiri grupe koje čine logičku celinu kod svakog **IMEI** broja: **490147-51-197345-0**

Prvih šest cifara (**490147**) predstavljaju TAC (*Type Approval Code*) kod koga prve dve cifre (**49**) određuju zemlju u kojoj je telefon proizveden. Kod ovog telefona broj 49 bi trebao da označava Nemačku. Sedma i osma cifra (u ovom slučaju **51**) predstavljaju FAC (*Final Assembly Code*) koji predstavlja oznaku proizvođača telefona. u ovom slučaju (*Ericsson*) telefon.

Sledećih 6 cifara (**197345**) označavaju serijski broj uređaja, dok je poslednja cifra (**2** u našem primeru, najčešće **0**) samo dodatni broj koji nema nikakvo posebno značenje.

Znači, IMEI ili serijski broj telefona je tako koncipiran da za svaki aparat bude jedinstven u svetu, da se serijski brojevi ni kod jednog proizvođača ne poklapaju, zbog toga ako se telefon ukrade, da ga se lakše nađe i tako zaštiti vlasnik telefona, naravno, ako ga je legalno kupio.

Primer MOC CDR-a ASCII dekodovanog

```
CME20R10MSCber.CallDataRecord.uMTSGSMPLMNCallDataRecord
{
   mSOriginating
   {
      callIdentificationNumber : '228450'H
      typeOfCallingSubscriber : '01'H
      callingPartyNumber : '4146433827F8'H
      callingSubscriberIMSI : '220032012449652F'H
      callingSubscriberIMEI : '353104007543000F'H
      calledPartyNumber : '216064612171'H
      disconnectingParty : 'callingpartyrelease (0)'
      dateForStartOfCharge : '060A10'H
      timeForStartOfCharge : '091018'H
      chargeableDuration : '00002D'H
      chargedParty : 'chargingofcallingsubscriber (0)'
      tariffClass : '003D'H
      tariffSwitchInd : 'notariffswitch (0)'
      mSCIdentification : '11836105000400'H
      outgoingRoute : "SSFĐO"
      incomingRoute : "BKG05DI"
      firstCallingLocationInformation : '22F030D3125289'H
      lastCallingLocationInformation : '22F030D3125289'H
      teleServiceCode : '11'H
      iNMarkingOfMS : 'originatingcamelservice (5)'
      radioChannelProperty : 'dualratefullratepreferred (3)'
      networkCallReference : '9FC2E90002'H
      bCSMTDPData1
      {
         serviceKey : '0000038F'H
         gsmSCFAddress : '11836115070000'H
      }
      gSMCallReferenceNumber : '9FC2E90002'H
      mSCAddress : '11836105000400'H
```

Iz primera ASCII dekodovanog MOC CDR moze se primetiti da se on u sebi sadrži mnoga polja bitna za opis poziva, ali i za sam sistem funkcionisanja mobilne telefonije, počevši od ''CallIdentificationNumber'': '228450'H kontrolnih polja, pa do početka poziva, trajanja, IMSI-a, IMEI-a odlaznih, dolaznih ruta, teleservisa, i tako dalje, za svaki scenario tipa poziva ima odgovarajuće polje... no pošto to nije tema ovog rada pomenuću samo kao pojam, da je sve to poznavanje ipak bitno ukoliko dolazi do veštačenja vezana za CDR-ove.

2. VEŠTAČENJA

U ovom delu rada daćemo samo mali deo iz prakse da bi se ipak lakše, na konkretnim slučajevima, objasnila složenost (valjda postupaka veštačenja) vezana za CallDataRecord-e i ostale usluge mobilne telefonije onima kojima je ova tema strana

2.1.Primer, iz opštinskog suda.

Sudija NN je trazio da se nakon 4 godine sudskog procesa, gomile neutvrđenih ili utvrđenih činjenica, utvrdi ko je korisnik neke e-*mail* adrese preko koje je slata gomila pretećih *mail*-ova. U ovom slučaju radilo se o uceni naše poznate kompanije sa vrlo delikatnom i ostvarivom pretnjom. U cilju tajnosti, neću otkrivati detalje, ali recimo da se

radilo o novčanoj uceni sa mogućnošću štetnih posledica za krajnje korisnike ucenjenog preduzeća.

Kod uhvaćenog NN izvršioca dela, prilikom hvatanja, inspektori MUP-a, koji su na obeleženo mesto ostavili novac za otkup, zatekli su dotičnu osobu uhvatili je i priveli kod sudije za prekršaje.

Nakon ispitivanja u pritvoru sudija je doneo oslobađajuću presudu tako da se optuženi brani sa slobode. Optuženi se branio ćutanjem sa izjavljujući da nije kriv i da se u na mestu za otkup našao sasvim slučajno, a paket, koji je uzeo, uzeo iz ''čiste radoznalosti'', jer je bio ''bačen na pod''.

Kod osumničenog, u istražnom postupku, pronađen je mobilni telefon, bez SIM kartice, i bez baterije, upisan je od strane MUP-a IMEI broj telefona i to je sve. Sve pretnje dotičnom preduzeću su upućivane sa govornica, ili preko mail-a. Registrovan je i broj mobilnog telefona, više brojeva, oba operatera MTS Srbija i tadašnjeg i MOBTEL -a, Telenor danas.

Veštačenje se odnosilo da se utvrdi ko je korisnik IMEI broja i da li je taj IMEI možda koristio neki od kartica sa kojeg je pozivan fiksni broj ucenjenog preduzeca.

Inspektori SUP-a su dostavili sudu pretragu po IMEI-u od strane MOBTEL-a ali ne i od Telekom Srbije, jer tadašnji sistem za kontrolu CDR-ova nije ni hardverski i ni softverski mogao da ispuni sve zahteve za pretragu ogromne količine podataka koji stižu i *backup*-uju se na raznim sistemima za backup mobilne telefonije.

Dnevno stiže oko 29.000.000 slogova, ili mesečno oko 700.000.000. To je oko 200 GB mesečnih podataka i to samo CallDataRecord-a koji imaju u sebi sve zapise, ali, napominjem, *fajlovi* se beleže i na sistemima za naplatu.

Data Warehouse je nastao da podrži kontrolu oba sistema za naplatu i da ne opterećuje sisteme koji isključivo služe za tu namenu.Policijski listinzi, različite statistike sistema, i druge analize se znači uzimaju iz skladišta podataka.Baza podataka je ograničena samo veličinom slobodnog prostora na diskovima i celokupni *Data Warehouse* system je nastao u Službi za analizu i razvoj, domaći je proizvod, i ima sve odlike svih svetskih standarda i programa za izradu *Data Warehouse* sistema.. Koristi Microsoft SQL Server i druge alate, ali algoritmi i programi za tako složen projekat su nastali kao delo domaćih stručnjaka.

Ponovnim pregledom fajlova mobilnih operatera, koristeći savremeni program za pretragu i *Data Warehouse* system Mobilne telefonije Srbije, pretragom po IMEI-u došao (ko!?) do određenih podataka koji su mi ukazali da je baš sa tog IMEI-a pozivan fiksni telefonski broj ucenjenog preduzeća.

Mogu odgovorno tvrditi da se pojmovi, kao **IMEI** (*International Mobile Equipment Identity*) odnosno (serijski broj mobilnog telefona), prikazuje istim u bilo kojoj mreži i kod bilo kog operatera na svetu.Zapravo, prilikom svakog poziva centrala beleži niz podataka koju su neophodni za funkcionisanje sistema, između ostalog, broj sa koga zovete, broj koji ste zvali, vreme poziva, dužina poziva, **IMEI** – serijski broj aparata, koju ste baznu stanicu kontaktirali i još niz podataka se beleži, kako kod Preduzeća za telekomunikacije "Telekom Srbija" a.d., odnosno Mobilne telefonije Srbije, kao i kod operatera Mobilne telekomunikacije "Srbija BK-PTT" d.o.o. MOBTEL, sadašnji TELENOR.

U ovom konkretnom slučaju veštačenje preko IMEI-a u oba operatera je pokazalo da se IMEI broj ne menja i da ga je koristilo optuženo NN lice te da je upravo sa oduzetog Mobilnog aparata bilo poziva i pretnji preduzeću koje trebalo da plati ucenu.

Tehnički, iako sve ostalo skoro savršeno urađeno, većina kriminalaca napravi neku grešku jer nisu toliko tehnički obrazovani da bi mogli sve faktore rizika da predvide.

2.2. Primer

Veštačenje od strane suda vezano za pretplatnika koji tvrdi da nikada nije zvao broj švajcarskog operatera, i da nikada nije koristio WAP uslugu i, da ne zna ni šta je to, kamoli da koristi takvu uslugu.

U listingu poziva videlo se da je korisnik zvao broj švajcarskog operatera. Advokat koji je branio optuženog dostavio je sudu informaciju da je to nepostojeći broj, što se iz klasičnog "voice" poziva može i utvrditi.Nedovoljno tehničko obrazovanje sudija, kao i nove tehnologije unose dosta zabune, tako da se često usluge Mobilne telefonije poistovećuju sa starim uslugama koje je nudila fiksna telefonija. Tako da, ako se kaže da se na Internet ili WEB portal može otići sa mobilnog telefona i poslati poslovnom partneru mail, ili iskoristiti takva usluga i za neke kriminogene radnje, samo unosi zabunu kod onih ljudi kojima tehnički deo sistema nije jača strana, nego se isključivo bave svojom strukom, u ovom slučaju pravom i pravnim aspektima suđena.

Upravo u ovakvim slučajevima IT veštaci će imati sve više imati posla u različitim komplikovanim slušajevima. Konkretno, u ovom slučaju, pregledom fajlova sa centrale bivšeg MOBTEL utvrdio sam da je posle filtriranja sa Mediation sistema, registrivan Data MOC CDR.što znači da je pokušana komunikacija preko WAP protokola sa Švajcarskim operaterom. To je utvrđeno pregledom po IMEI-u aparata koji je korisnik koristio.Utvrdio sam da je mobilni telefon dekodiran, da je stigao iz mreže švajcarskog operatera.Da li je poklonjen ili kupljen na crno, to nije bitno.Dekodiran da radi samo za VOICE opciju svaki takav aparat koji ima mogućnosti za GPRS odnosno WAP uslugu, svi drugi parametri u telefonu ostaju isti, tj nemoguće ih je dekodirati, te stoga, ako slučajno ili namerno pokušate da aktivirate opciju za odlazak na Internet ili WAP portal operatera kod koga ste u mreži, može vam se dogoditi da vaš telefon, tj kartica uporno pokušava da uspostavi kontakt, ali u ovom slučaju sa operaterom odakle je i setovana,npr. Wap *gateway* švajacarskog operatera.Iz data MOC se to konkretno i vidi, i takav poziv naravno ukoliko nije IP rutiran prealazi preko međunarodne centrale i traifira se kao međunarodni poziv."Nesreća" je u tome što kada WAP *gateway* švajcarskog operatera, uvrdi da pretplatnik nije u njegovoj mreži i zabrani mu pristup usluzi, poziv se prekida, ali opcija autoredial na telefonu ako je uključena uporno pokušava da se ponovo uključi.Naravno,eto otkud je toliki broj poziva i zašto toliki računi. Sa druge strane nema nikakvih pokušaja da operater ošteti pretplatnika, naprotiv, *antifraud* služba pretplatnika u ovim slučajevima na vreme isključuje da račun ne bude i veći.

3. ZAKLJUČAK

Ovim radom se želelo da se pokaže kako se radi u mobilnoj telefoniji Srbije, ukaže na kompleksnost i složenost sistema, i da sami po sebi listinzi telefonskih brojeva koje rade policija i sudovi u istražnim postupcima u pozadini jednostavnih odlaznih i dolaznih poziva imaju u sebi i sadrže daleko više složenosti.Upravo zbog toga veštačenja *CallDataRecord*-a mobilne telefonije, Gprs-a WAP-A i ostalih usluga zahtevaju znanja iz domena rada mobilnih operatera u svetu, te s toga smatram da veštačenja iz oblasti mobilne telefonije treba da rade stručnjaci koji poznaju probleme iz te, ili slične oblasti i samim tim odgovorno i stručno odgovore na sve potrebe suda i sudskih procesa u istražnim radnjama, u cilju da se isključivo na tehnički podržanim dokazima dođe do pravih rezultata i to isključivo bude istinito i samo istinito onako kako pravila i kodeks veštačenja i nalažu.