FORENZIKA MOBILNIH UREĐAJA

Milorad S. Markagić, Univerzitet odbrane u Beogradu,
Vojna akademija, Katedra telekomunikacija i informatike,
Beograd

DOI: 10.5937/vojtehg61-1340
OBLAST: telekomunikacije, informacione tehnologije
VRSTA ČLANKA: stručni članak

Sažetak:

U članku je dat pregled mogućnosti digitalizovanih mobilnih (prenosnih) uređaja, kao i metode istraživanja podataka sa istih. Težište je dato na forenzičkoj istrazi mobilnih telefonskih aparata, ali su obuhvaćena i istraživanja ostalih medija za digitalnu obradu, prenos i čuvanje informacija.

Poseban osvrt je izvršen na programske alate pri vršenju akvizicije digitalnih podataka, sa ciljem upućivanja čitaoca u načine i metode zaštite podataka, ali i saznanja gde se isti sve mogu naći i kako se mogu zloupotrebiti u kriminalne svrhe.

Ključne reči: forenzika, digitalna forenzika, mobilne komunikacije, mobilni uređaji.

Uvod

Razvojem naučne misli i izuzetnom brzinom tehničkih i tehnoloških inovacija u oblasti komunikacija među pojedincima i institucijama, računari, su neizbežno postali baze gde se čuvaju podaci skoro svih ljudskih aktivnosti i interesovanja.

Ubrzanim razvojem personalnih računara, uvođenjem i sve masovnijim korišćenjem Interneta, kao i konvergencijom računarstva i telekomunikacija u jedinstvenu celinu, svet umreženih digitalnih uređaja pruža neslućene mogućnosti, ali i izazove i za kriminalce i istražioce, vlade i institucije, za poslovanje, komunikaciju kao i za sve korisnike svesne važnosti očuvanja privatnosti (Hany, Jessica, 2009), (Caloyannides).

Današnji je svet digitalni svet gde ogromna količina informacija nastaje, obrađuje, šalje i prima presreće i čuva u digitalnom obliku. Digitalne informacije utiču i koriste se u svakom aspektu ljudskog i društvenog života. Iako korišćenje podataka u digitalnom obliku donosi mnoge tehnološke i ekonomske prednosti, ono dovodi i do mnogih problema i izazova prilikom izvođenja forenzičke analize digitalnih dokaza.

mlmarkag@yahoo.com

Najčešći problemi na koje nailaze forenzičari – istražioci a koji se mogu svrstati u objektivne i realne bili bi:

1. Da digitalni podatak predstavlja samo apstraktnu reprezentaciju informacije - skup bitova i nema direktno vidljive karakteristike koje bi ukazivale na autentičnost, poreklo i verodostojnost informacije.
2. Veliki broj raznovrsnih uređaja, koji se koriste za stvaranje i čuvanje digitalnih informacija kao što su: kamere, snimači govora, lični digitalni pomoćnici, muzički plejeri, mobilni telefoni i računari.
3. Niske cene i laka dostupnost medija za čuvanje podataka, doprinosi da se količina stvorenih i sačuvanih informacija povećava geometrijskom progresijom.
4. Pregled tako velikih količina podataka oduzima previše vremena.
5. Prenos digitalnih podataka raznim komunikacionim kanalima i sa više tipova uređaja, u različitim formatima, što njihovu analizu i slaganje u smislenu celinu čini veoma teškom.
6. Digitalni podaci se lako brišu, prepravljaju, modifikuju, kriptuju, uz upotrebu velikog broja javno dostupnih i besplatnih antiforenzičkih alata,
7. Mediji za čuvanje podataka se sve više smanjuju, tako da je njihovo fizičko otkrivanje veoma otežano, i
8. Digitalni podaci su veoma ranjivi, pa često zahtevaju brzo prikupljanje, selekciju i obradu.

Kada se uzmu u obzir navedene činjenice, dolazi se do logičnog zaključka da se moraju razvijati i naučne metode za rekonstrukciju dokaza iz digitalnih podataka a nakon toga i za njihovu analizu. Metode, koje se sprovode u ovakvim postupcima čine jednu posebnu naučnu disciplinu – digitalnu forenziku.

Digitalnu forenziku možemo definisati kao skup naučnih metoda za prikupljanje, čuvanje, identifikaciju, analizu, interpretaciju, dokumentaciju i prezentaciju digitalnih dokaza nastalih u digitalnim izvorima, sa ciljem negiranja ili potvrđivanja učinjene kriminalne radnje ili pomoći državnim organima pri rekonstrukciji događaja (Caloyannides). Najčešće se digitalni podaci zloupotrebljavaju u kriminalne svrhe: krađe, prevare, pretnje, ucene, uznemiravanje i slično.

Digitalna forenzika je novija naučna disciplina koja se neprestano menja i nadograđuje, održavajući korak sa napretkom hardverske tehnologije i razvojem novih softvera. Kao što se fizička forenzika oslanja na naučne principe koji su se pokazali kao korisni i efikasni u realnom svetu, tako se digitalna forenzika suočava sa posebnim izazovima koji važe samo u digitalnom okruženju.

Brz razvoj prenosnih sredstava za komunikaciju i generisanje digitalnih podataka, njihova sve niža cena i uvođenje u masovnu upotrebu, doprinose sa jedne strane komfornijem korišćenju, a sa druge strane sve većoj mogućnosti manipulacije i zloupotreba. One se manifestuju kroz krađe identiteta, prisluškivanje ometanje i niz drugih nezakonitih radnji.

Pojam i osnovni pojmovi forenzike mobilnih uređaja

U ogromnom broju korisnici i ne shvataju sve mogućnosti pametnih telefona (Smart phones), iPoda, MP3 plejera, Black Berry-a, PDA-a (Personal digital assistant). Mobilni telefon ili PDA u današnje vreme poseduju moć kompjutera.

Današnji mobilni telefoni rade sa gigahercnim procesorima, radnim memorijama 1 GB i većim, hard diskom veličine više GB. Svi su mobilni telefoni u potpunosti bežično funkcionalni, sadrže Bluetooth, infracrvenu i 802.11 tehnologiju.

Ne postoji u potpunosti precizna definicija mobilnog uređaja zato što mnogi uređaji kao što su iPod-ovi i video kamere postaju sve manji i mobilniji. Većina mobilne forenzike danas se sprovodi na mobilnim telefonima i PDA. U mobilnom svetu tehnologije se menjaju veoma brzo, tako da snalažljivi korisnici često otkriju metode prikrivanja podataka i upotrebe novih uređaja za nenamenjene svrhe pre nego što forenzički istražioci u potpunosti uspeju da analiziraju uređaje i pronađu njihove slabosti i mogućnosti.

U većini računarskih područja ovaj je problem prisutan, alije posebno izražen na području mobilnih tehnologija, jer je brzina promene tako velika.

Bez obzira što korisnici često povećavaju količinu tvrdih diskova i radne memorije na svom računaru, oni u suštini koriste istu tehnologiju u toku celog veka upotrebe.

Pri vršenju istrage mobilnih uređaja treba imati na umu da se oni razlikuju od računara u tri važne činjenice:

1. Veoma česte, brze i lake promene operativnih sistema, standarda i tehnologije čuvanja podataka,
2. Veliki broj različitih platformi mobilnih uređaja, dok su kod računara više manje standardizovane platforme, i
3. Bežična tehnologija komuniciranja.

Postoje tri osnovna načina na kojima mobilni uređaji komuniciraju i koji koriste sve kompanije koje proizvode mobilne uređaje:

1. 802.11: ovaj standard koriste sve bežične mreže koje danas postoje. Domet mobilnog uređaja koji koristi 802.11 znatno varira i zavisi od snage uređaja, ali minimalnog je u prečnika 100 metara.
2. Bluetooth: standard koji se koriti na malim razdaljinama, do 50 metara
3. IC (Infracrvena komunikacija): koristeći stariju metodu komuniciranja mobilni uređaji mogu razmenjivati informacije koristeći infracrveni deo svetlosnog spektra. Ova je metoda usmerene prirode – za komunikaciju među uređajima njihovi infracrveni portovi moraju biti okrenuti jedan prema drugome.

Forenzika personalnih računara je u svom pristupu prilično standardizovana, dok mobilna forenzika koristi različite pristupe istraživanja i prilagođava se razvoju uređaja (Volonino, Anzaldua, 2008). Ovo područje računarske forenzike je relativno novo i ne važe ista pravila kao i kod

standardne forenzike. Tako se klasična pravila kao što je zabrana pisanja na istraživanom mediju često ne mogu biti realizovana prilikom obavljanja istražnih radnji u mobilnoj forenzici.

Mobilni uređaji sa aspekta forenzičke istrage

Prilikom analize mobilnog uređaja, a u zavisnosti od vrste moguće je koristiti više vrsta dokaza koji se nalaze na istima:

1. Pretplatnički identifikator na mobilnim telefonima: Ovu informaciju koriste mreže mobilnih telefona za autentifikaciju korisnika kao i verifikaciju tipa usluge vezanu za tog korisnika. Drugim rečima, moguće je povezati identitet mobilnog uređaja sa zapisima koje čuva davalac mobilne usluge.
2. SIM moduli (Subscriber Identity Modules): Sadrže informacije ugrađene u sebi, a ukoliko uređaj ne podržava SIM kartice. informacije su kodirane na sam uređaj.
3. Dnevnici: Mobilni uređaju u sebi sadrže dnevnike poziva (primljenih, propuštenih, odgovorenih) i biranih brojeva, kojima je moguće utvrditi određene vremenske tokove. Takođe, dnevnici sadrže i informacije vezane za GPS, spajanja na mrežne ćelije i vreme prekida veza s mrežnim ćelijama. Ovi dnevnici mogu i ne moraju postojati, a u zavisnosti od vrste uređaja, ali ukoliko postoje veoma je jednostavno preko njih izvršiti lociranje korisnika.
3. Telefonski imenik – lista kontakata: Sadrži listu potencijalnih svedoka, žrtava, i saučesnika koja može sadržati sliku, adresu elektronske pošte, fizičke adrese, alternativne brojeve telefona, kao i mnoge druge informacije.
4. Tekstualne poruke: Sadrže delove dokaza kao i vremenske oznake, koje su veoma važne u istrazi. Kao i kod medija za čuvanje podataka, i ovde je moguće rekonstruisati i pronaći oštećene ili obrisane poruke.
5. Kalendar – rokovnik: Sadrži informacije o obavezama osumnjičenog, njegovim kretanju i ljudima s kojima je kontaktirao.
6. Elektronska pošta: Kao i kod klasičnih računara sadrži poruke koje osumnjičeni šalje ili prima logovanjem na svoj korisnički nalog.
7. Instant poruke: Poruke koje se razmenjuju u realnom vremenu, mogu sadržati čitave razgovore kao i vremenske oznake.
8. Fotografije (slike): Urađene na samom mobilnom uređaju, primljene ili preuzete sa nekog sajta.
9. Audio zapisi: Mogu sadržati podatke koje korisnik uređaja sam kreira, zatim snimljene razgovore u toku komunikacije ili samo zapis preko diktafona mobilnog uređaja.
10. Multimedijalne poruke: Poboljšana verzija instant poruka, koje u sebi osim teksta sadrži i sliku, video zapis i govor,
11. Aplikativni dokumenti: Svi moderniji mobilni uređaji imaju mogućnost kreiranja i pregleda dokumenata, prezentacija, tablica za proračune i mnogih drugih formata dokumenata i

12. Mediji za proširenje kapaciteta: Na njima je često sačuvana istorija prethodno korišćenih aplikacija, brojeva, multimedijalnih sadržaja i sl. (Volonino, Anzaldua, 2008).

Većina mobilnih uređaja ima mogućnost korišćenja spoljašnjih medija za čuvanje kao što su SD kartice. One često služe i za prenos podataka sa računara na mobilni uređaj i obrnuto, pa zato predstavljaju važan izvor potencijalnih dokaza.

Cilj upotrebe forenzičkog softvera

Cilj koji treba postići prilikom upotrebe forenzičkog softvera je dvostruki:

1. Zaštita postojećih podatka na originalnom uređaju – ovaj postupak osigurava integritet prikupljenih podataka, i

2. Postavljanje mehanizma koji će, izračunavajući hash vrednosti potvrditi integritet.

Funkcije proistekle iz računa hash vrednosti kao i write protect softver u samom uređaju omogućavaju ciljeve koje koriste svi forenzički alati. Ali prilikom istraživanja mobilnih uređaja često se javlja potreba pisanja po njihovoj memoriji kako bi se došlo do informacije. U ovakvim slučajevima treba težiti da se zapiše što manja količina informacija.

Najbolji primer akvizicije podataka korišćenjem neforenzičkih alata je korišćenje sinhronizacijskog softvera kako bi se pristupilo podacima na mobilnom uređaju. Tada se podaci kopiraju sa originalnog uređaja, ali se tom prilikom menjaju datumske i vremenske oznake podataka. U tom slučaju je teško dokazati da nije komprimovan integritet podataka.

Problem se javlja i ukoliko se istraga sprovodi na nekom novom mobilnom uređaju za koji još ne postoje modifikovani forenzički alati, što je čest slučaj uzimajući u obzir brzinu menjanja tržišta mobilnih uređaja (Volonino, Anzaldua, 2008).

Tada se preporučuje izrada dodatnih kopija podataka i precizno zapisivanje upotrebljenih procedura i metoda.

Forenzika mobilnih telefona i SIM kartica

Forenzička akvizicija i izvlačenje podataka sa mobilnih telefona jedan je od najzahtevnijih postupaka istrage, zbog brze promene u hardverskoj i softverskoj strukturi i velikog broja prisutnih nestandardnih uređaja na tržištu.

Ali uprkos svim pojedinačnim razlikama, mobilni telefoni sastoje se od tri osnovne komponente:

1. ROM memorije (Read Only Memory): Na ovom elementu mobilnog telefona smešten je OS, a često i softver za rešavanje problema koji se koristi za dijagnostiku i upravljanje uređajem.

2. RAM memorije (Random Access Memory): Ovo područje se koristi za privremeno čuvanje podataka – ukoliko se mobilni telefon isključi, podaci se gube.

3. Sklop ili jedinica za čuvanje podataka: Iako većina mobilnih telefona ima internu memoriju koja je najčešće zasnovana na tehnologiji flash memorije, većina naprednijih modela telefona dolaze s ugrađenim prostorom za memorijske kartice koje služe za proširenje kapaciteta za čuvanje podataka u uređaju.

Takođe se koriste i spoljašnji mediji za čuvanje podataka u obliku Mini SD kartica, SD kartica, ili MMC mobilnih kartica. Za čitanje ovih kartica na računaru potrebni su posebni čitači kartica, ali je i taj problem prevaziđen u novijim generacijama računara.

Forenzika Mobilne mreže

Osnovna stvar koju forenzičar treba da zna je na koji je tip mobilne mreže spojen telefon. Danas su najrasprostranjenije sledeće mreže:

– CDMA (Code Division Multiple Access): Ne poseduje SIM (Subscriber Identity Module) modul – praktično znači da su svi podaci sačuvani na mobilnom telefonu. Koristi se pretežno u SAD.

– GSM (Global System fo Mobile Communication): Ove mreže koriste SIM module kao odvojene komponente dizajnirane da budu prenosive sa jednog telefona na drugi – koristi se pretežno u Evropi.

– IDEN (Integrated Digital Enhanced Network): Koristi sistem naprednih SIM kartica (advanced SIM cards) – USIMs.

Od tipa mreže zavisi koji se forenzički alat koristi prilikom obrade mobilnog telefona.

Forenzika mobilnih uređaja

Nakon utvrđivanja mreže u kojoj mobilni telefon radi, sledeći korak je utvrđivanje specifičnog tipa mobilnog uređaja da bi se utvrdile njegove karakteristike i mogućnosti.

Identifikacija tipa mobilnog telefona sprovodi se pretragom proizvođača, serijskog broja uređaja koji se obično nalaze ispod baterije, sinhronizacionog softvera, kodovima proizvođača. Kroz kod proizvođača moguće je doći do informacije kao što su: proizvođač telefona, model, kod zemlje u kojoj je proizveden, a nalazi se uglavnom oko istog područja gde i serijski broj (Volonino, Anzaldua, 2008).

U operativnom sistemu mobilnog telefona moguće je pronaći sledeće informacije: ESN (Electronic Serial Number), ICCID (Integrated Circuit Card Identification), IMEI (International Mobile Equipment Identifier).

Nakon utvrđivanja tipa mobilnog telefona traži se lista karakteristika koje daje proizvođač, pa se na temelju te liste izdvoje najverovatnija mesta gde je moguće pronaći dokazne materijale. Mada često specifikacije proizvođača mogu biti umnogome različite od stvarnog stanja u mobilnom telefonu zbog korisnikovih dopuna i izmena.

Pregledom specifikacija dobija se uvid u:

1. Metode bežičnog spajanja: da li telefon koristi bluetooth, WiFi ili infracrvenu tehnologiju uz mobilnu tehnologiju komuniciranja,
2. Pristup internetu,
3. Kamera,
4. Upravljači ličnim informacijama PIM (Personal information manage): variraju u zavisnosti od tipa uređaja, ali svi sadrže kalendar, imenik, kao i softver za produkciju i pregled raznih tipova dokumenata,
5. Poruke: mogu li se telefonom slati samo SMS poruke, multimedijalne poruke, elektronska pošta ili svaka od njih,
6. Aplikacije: sa kojim tipom aplikacije je telefon isporučen od proizvođača, a koja je trenutno u upotrebi i
7. Spajanja: koji tipovi kablova su potrebni za spajanje telefona sa računarom.

Forenzika SIM kartica

SIM (Subscriber Identity Module), upotrebljava se u GSM i IDEN mrežama. Omogućava korisniku prebacivanje podataka kao što su imenik, poruke i korisničke autentifikacije između mobilnih telefona. Korisnik može menjati mobilne telefone, ali se on i dalje može pronaći korišćenjem odnosno praćenjem SIM kartice. Da bi se izbeglo kontaminiranje dokaza ne preporučuje se pristupanje telefonu korišćenjem druge SIM kartice.

Kloniranje SIM kartica: korišćenjem forenzičkih alata najsigurniji je način pristupanja mobilnom telefonu. SIM kartica zaštićena je PIN brojem (Personal identification number), čiji je zadatak ne samo zaštita podataka na kartici već i na samom uređaju. PIN broj dugačak je od četiri do osam cifara i vrši sigurnosnu opciju blokiranja uređaja ukoliko se unese pogrešan PIN određen broj puta – najčešće tri. Mobilni telefon se nakon blokiranja može otključati PUK brojem (PIN Unblocking Key), a ako se kojim slučajem nekoliko puta nese i pogrešan PUK broj, uređaj se više ne može odblokirati.

Do nedavno su se PDA koristili kao samostalni uređaji, ali se danas mogućnosti PDA i mobilnog telefona nalaze objedinjeni u pametnim telefonima (Smart phones). Danas su retko u upotrebi ovi uređaji, a koriste se većinom Palm OS, koja je najpopularnija PDA platforma i koja se trenutno još uvek negde koristi. Analiza, obrada i prikupljanje podataka na PDA obavlja se na isti način kao i ne mobilnim telefonima. U suštini, jedina razlika između PDA i mobilnog telefona je ta što se PDA-om ne mogu obavljati pozivi.

Forenzika Digitalnih kamera i fotoaparata

Digitalni fotoaparati i kamere su u današnje vreme isti uređaj. Prilikom njihovog pregleda najbitnije je naravno područje za čuvanje fotografija i snimaka. Iako je broj proizvođača digitalnih fotoaparata i kamera ogroman, način komunikacije i korišćena oprema je standardizovana.

Digitalne kamere koriste standardni ili mini USB priključak za spajanje sa računarom, standardne memorijske kartice kao što su Mini SD ili Compact Flash, za proširenje kapaciteta čuvanja. Većina trenutno dostupnih sistema prilikom istrage tretira se kao samo još jedna jedinca za čuvanje podataka olakšavajući time posao forenzičarima, jer je moguće korišćenje standardnih metoda i alata za digitalnu forenziku. Kako se analize i pretrage sprovode preko USB porta, potrebno je omogućiti opciju zabrane pisanja po mediju, kako se prilikom analize podaci ne bi slučajno modifikovali. Isto pravilo važi i za čitanje ili prenos podataka sa memorijskih kartica (Swaminathan i dr., 2009).

Kao i kod digitalnih kamera, većina digitalnih audio uređaja kao što su MP playeri, ili iPod-ovi, tretiraju se kao mediji za čuvanje podataka pa se shodno tome i obrađuju forenzičkim alatima.

Izbor alata za forenzičku obradu

Područje mobilne forenzike još uvek je relativno novo pa zato ne postoji samo jedan alat ili skup alata koji bi pokrio sve moguće situacije.

Digitalna forenzika deli se na dva načina akvizicije podataka: fizičku i logičku akviziciju.

Tehnike mobilne forenzike prate isti format, ali zbog velikog broja postojećih platformi, logička forenzička akvizicija je tip koji se najčešće sprovodi. Očigledno se ovaj tip akvizicije koriti zato što forenzički softver koristi operativni sistem mobilnog uređaja za izvlačenje podataka. Fizička akvizicija podataka ima prednost nad logičkom, jer je sa njom moguće izvući podatke koje operativni sistem ne vidi ili im nema pristup.

Primarno područje delovanja mobilne forenzike je da se bavi akvizicijom podataka sa mobilnih telefona. Ali alati korišćeni za akviziciju mobilnih telefona, mogu se koristiti i na PDA uređajima. Alati za mobilnu forenziku dele se na dve grupe: GSM i CDMA tipovima za akviziciju. Drugim rečima, neki forenzički alati rade samo analizu uređaja, dok neki i uređaja i SIM kartice. Postoje alati koji su toliko specijalizovani da rade samo na određenom tipu mobilnog uređaja.

Najpoznatiji i najčešće korišćeni, mada ne i jedni alati kojima se obrađuju mobilni uređaji i SIM kartice su:

1. Paraben,
2. Logicube,
3. CellDEK kit,

4. Crownhill,
5. Inside Out Forensics i
4. Xygen software.

Parabenov skup alata za mobilne uređaje pokriva područja od Palm uređaja sve do Garmin GPS (Nolan, 2005).

Uređaji koji se koriste u mobilnoj forenzici

Izbor tipa forenzičkog uređaja koji će se koristiti za mobilnu forenziku prilično se razlikuje od standardne opreme za računarsku forenziku. Osnovni razlog zašto je to tako je tome što se ovde radi sa većim brojem različitih tipova mobilnih aparata za bežično komuniciranje.

Jedan vid sastava osnovnog kompleta bio bi:

1. Faradejev kavez – sprečava komunikaciju mobilnih uređaja sa spoljašnjim bežičnim uređajima, tako što vrši presretanje radio talasa, pa se ponaša kao velika spoljašnja antena, koja preusmerava radio signal od mobilnog uređaja. Znači, sprečava primanje i slanje podataka i vrši izolaciju uređaja. U okruženju mobilne forenzike, izolacija uređaja prvi je korak pre početka istraživanja,
2. Čitači SIM kartica,
3. Čitači SD kartica i
4. Spojni kablovi za povezivanje sa računarom i energetski kablovi za punjenje baterija.

Izolovanje mobilnih uređaja

Kada se vrši istraga mobilnog uređaja on mora biti izolovan ne samo od drugih mobilnih telefona, već i od bilo kakve komunikacije korištenjem bluetootha, WiFi-a ili infracrvene komunikacije. Takođe se mora izbeći kontaminacija podataka na mobilnom uređaju nakon što je zaplenjen. Ovo iz sledećih razloga:

1. Praktični: forenzičar ne želi da mu podatke i moguće dokaze prebrišu ili prekriju novi podaci,
2. Bezbednosni: postoji više tipova uređaja i mehanizama pomoću kojih je moguće zaključati ili uništiti uređaj iz daljine i
3. Legalni: sud će odbaciti sakupljene dokaze ukoliko postoji sumnja u njihov integritet.

Mobilni telefon može biti izolovan na nekoliko načina:

1. Potpunom izolacijom bežične komunikacije korišćenjem Faradejevog kaveza ili nekog uređaja za ometanje. Ovaj način izolacije funkcioniše do trenutka kada se isprazni baterija uređaja. Imajući u vidu da većina

uređaja povećava snagu odašiljanja prilikom pokušaja spajanja, baterija se samim tim brže prazni,

2. Isključivanjem uređaja i

3. Postavljanjem uređaja u avionski režim rada u kome su isključeni svi bežični načini komunikacije. Mana ovog pristupa je potreba interakcije sa uređajem pa se samim tim rizikuje mogućnost promene dela podataka (Volonino, Anzaldua, 2008).

Pronalaženje mobilnih podataka

Sledeći korak nakon što je izvršena izolacija telefona je da se baterija održava, punom čime se izbegava rizik gubljenja podataka smeštenih u radnoj memoriji (ROM). Nakon toga sledi pronalaženje traženih informacija.

Bez obzira da li se radi o GSM ili CDMA uređajima, procedure izvlačenja podataka se malo razlikuju. Ako se radi preko SIM kartica, one se prvo kloniraju, ili se izradi imidž podataka korišćenjem čitača kartica. Tada se mora voditi računa da se onemogući bilo kakvo pisanje na originalni medij.

Nakon izvlačenja podataka za analizu, forenzički alati izvršavaju „pronađi i dohvati“ automatizovane softverske funkcije.

Kada se podaci izvlače iz samog uređaja, procedure se ne razlikuju se od onih koje se koriste kod SIM akvizicije (Nolan, 2005).

Zaključak

Digitalna forenzika nastala kao izazov novim metodama, algoritmima i alatima za kriminal na polju digitalnih medija, nastoji da sa jedne strane onemogući ili bar oteža kriminalne radnje, a da sa druge strane, ako do njih i dodje omogući nadležnim institucijama brzo reagovanje. Sve je veći broj antiforenzičkih alata koji su u mogućnosti da zavaraju forenzičke alate, sve je veći broj kriminalnih radnji na, još uvek, apstraktnom polju digitalnih medija.

Ali ipak izrada falsifikata, krađa identiteta i lak dolazak do digitalnih podataka postaju stvar prošlosti, prvenstveno zbog sve većeg broja edukovanog kadra i sve sigurnijih softverskih rešenja, pa kriminalne radnje zahtevaju sve više vremena, i postaju sve kompleksniji procesi. Ipak je jedno sigurno – ti se procesi nikada neće u potpunosti zaustaviti.

Savremena tehnologija omogućava manipulaciju digitalnim medijima i promene na istima, načinima koji su pre nekoliko godina bili nemogući i nezamislivi. Sasvim je sigurno da će se upotreba i laka dostupnost do digitalnih medija sve više koristiti u kriminalne svrhe.

Kako se nastavlja razvoj tehnologije biće sve važnije da nauka digitalne forenzike drži korak s tim razvojem. Kako se razvijaju tehnike i metode za otkrivanje digitalnih prevara, razvijaće se i nove sofisticiranije metode izrade falsifikata koje će biti teške za otkrivanje.

Literatura

Caloyannides, M. A., *Forensics Is So Yesterday*, IEEE Security&Privacy.

Hany, F., Jessica, F, 2009, Image forgery detection, IEEE Signal Processing Magazine.

Nolan, R., 2005., *First responders guide to Computer Forensics,* CERT.

Swaminathan i dr., 2009, *Component Forensics*, IEEE Signal Processing Magazine, Vol. 26, No. 2.

Volonino, L., Anzaldua, R., 2008, *Computer Forensics*, Wiley publishing inc.

FORENSICS OF MOBILE DEVICES

FIELD: Telecommunications, IT
ARTICLE TYPE: Professional Paper

Summary:

The article gives an overview of the possibilities of digitized mobile (portable) devices, and the methods of analysing data from them. Although the emphasis is placed on the forensic investigation of mobile phones, other media for digital processing, transmission and storage of information are covered as well.

A special emphasis is put on the software tools in carrying out the digital data acquisition, with the aim of informing the reader on the methods of data protection, sorces where they can be found and how they can be misused for criminal purposes.

Introduction

Owing to the development of scientific thought and a significant increase in number of technical and technological innovations in communications between both individuals and institutions, computers have inevitably become a base where the data on almost all human activities is kept.

Notion and the basic concepts of the forensics of mobile devices

All the possibilities of smart phones, iPods, MP3 players, Blackberries, and PDAs (Personal Digital Assistants) have not been widely recognized yet by most of their users. Nowadays mobile phones or PDAs are as powerful as computers.

Today's mobile phones are equipped with processors in gigahertz, working memories of 1GB and higher and hard disks of several GB. All mobile phones are fully functional as wireless and they include Bluetooth, infrared and 802.11 technologies.

Mobile devices in terms of forensic investigation

Most mobile devices have the ability to use external storage media such as SD cards. They are often used for data transfer from PCs to mobile devices and vice versa, thus representing an important source of potential evidence.

Aim of the use of forensic software

The goal to be achieved when using forensic software is two-fold:
1. Protection of the existing data on the original device - this process ensures the integrity of the collected data, and
2. Installment of a mechanism that confirms integrity by calculating hash values.

Forensics of mobile phones and SIM cards

Forensic acquisition and extraction of data from mobile phones is one of the most demanding procedures of investigation, due to rapid changes in hardware and software structures and a large number of non-standard devices on the market.

Forensics of mobile networks

The most important for a forensic scientist to know is which type of network a mobile phone is connected to.

Forensics of mobile devices

After establishing a network in which a particular mobile phone works, the next step is to identify a type of the mobile device in order to determine its features and capabilities.
The identification of the mobile phone type is conducted by searching manufacturers, device serial numbers to be usually found under the battery, the synchronization software and manufacturer codes. Manufacturer codes contain data on manufacturer's name, model, country of production and they are usually found in the same area where the serial number is.

Forensics of SIM cards

SIMs (Subscriber Identity Modules) are used in GSM and IDEN networks. They allow the user to transfer data such as phonebooks, messages and user authentication between mobile phones. The user can change mobile phones, but he can still be tracked through his SIM card. To avoid contamination of evidence, it is not recommended to access the phone using another SIM card.

Forensics of digital cameras and camcorders

Nowadays digital cameras and camcorders are the same device. During their inspection, the most important is the area for storing photos and videos. Although there are numerous manufacturers of digital cameras and camcorders, the mode of communication and the used equipment are standardized.

The choice of tools for forensic processing

The area of mobile forensics is still relatively new; therefore, there is no single tool or a set of tools to cover all possible situations.

Digital forensics is divided into two data acquisition modes: physical and logical acquisition.

Devices used in mobile forensics

The choice of a type of forensic equipment to be used for mobile forensics is quite different from standard equipment for computer forensics due to numerous different types of mobile devices for wireless communication.

Isolation of mobile devices

A mobile device under investigation must be isolated not only from other mobile phones, but also from any communication via Bluetooth, WiFi, or infrared communication. It is also necessary to avoid data contamination on the device after it has been seized.

Finding mobile data

The next step after the phone isolation is to keep the battery full in order to avoid the risk of losing data stored in the working memory (ROM). The particular information is searched for afterwards.

Conclusion

Digital forensics emerged as a challenge to new methods, algorithms and tools for crime in the area of digital media. It aims at preventing or making criminal actions less possible, and, if a criminal activity has already happened, it enables a fast rsponse of competent insistutions. Antiforensic tools and criminal activities are on the constant increase in a still abstract field of digital media.

Key words: *forensics, digital forensics, mobile communications, mobile devices.*

Datum prijema članka/Paper received on: 04. 01. 2012.

Datum dostavljanja ispravki rukopisa/Manuscript corrections submitted on: 27. 01. 2012.

Datum konačnog prihvatanja članka za objavljivanje/ Paper accepted for publishing on: 29. 01. 2012.