

UNIVERZITET SINGIDUNUM
SAVREMENE INFORMACIONE TEHNOLOGIJE
MASTER STUDIJE

MASTER RAD
DIGITALNA FORENZIKA

**- Razvoj modela i forenzika alternativnih
računarskih uređaja-**

MENTOR:
Prof. dr Gojko Grubor

KANDIDAT:
Dumonjić Pegor
Br. ind. : 410114/2011

Beograd, Jul 2013

SADRŽAJ:

1. METODOLOGIJA IZRADE ISTRAŽIVAČKOG RADA	6
1.1. UVODNE NAPOMENE.....	6
1.2. PREDMET ISTRAŽIVANJA.....	6
1.3. CILJEVI RADA	7
1.4. ISTRAŽIVAČKE HIPOTEZE.....	7
1.5. METODE ISTRAŽIVANJA I TOK ISTRAŽIVAČKOG PROCESA.....	8
2. RAZVOJ MODELA DIGITALNE FORENZIKE	9
2.1.TAKSONOMIJA RAZVOJA MODELA DF ISTRAGE	13
3. AKTIVNA DIGITALNA FORENZIKA.....	13
3.1. ODGOVOR NA INCIDENT I POTVRDA	15
3.2. DIGITALNA FORENZIČKA ISTRAGA	16
3.3. ANALIZA	16
3.3.1. Faza analize	16
3.3.2. Faza rekonstrukcije događaja	17
3.3.3. Faza završetak.....	17
4. DISTRIBUTIVNA DIGITALNA FORENZIKA	17
5. DIGITALNA FORENZIKA VIRTUELNIH MAŠINA ILI VIRTUELNA MAŠINA KAO ALAT	20
6. DIGITALNI DOKAZI SU SVUGDJE	22
6.1. ŠTA JE TO DIGITALNA FORENZIKA?	22
6.2. ŠTA JE DIGITALNI DOKAZ?	22
6.3. KAKO JE DIGITALNI DOKAZ NASTAO I KAKO SE SKLADIŠTI	23
7. PODDISCIPLINE DIGITALNE FORENZIKE	26

7.1. KOMPJUTERSKA FORENZIKA.....	26
7.2. MREŽNA FORENZIKA	27
7.3. FORENZIKA MOBILNIH TELEFONA	27
7.4. FORENZIKA GPS UREĐAJA.....	29
7.5. FORENZIKA MEDIJSKIH UREĐAJA.....	30
7.6. FORENZIKA DRUŠTVENIH MREŽA.....	30
7.7. TELEFONSKE AUTOMATSKE SEKRETARICE	31
7.8. DIGITALNA FORENZIKA SLIKA	31
7.9. FORENZIKA DIGITALNIH KAMERA	32
7.10. FORENZIKA DIGITALNOG AUDIO DOKAZA.....	32
7.11. FORENZIKA MULTIPLEJER IGRICA.....	33
7.12. FORENZIKA KONZOLA ZA IGRE	33
8. ANDROID PLATFORMA.....	34
8.1. ISTORIJA ANDROIDA	35
8.1.1. Jelly Bean	36
8.2. DIGITALNA FORENZIKA ANDROIDA.....	37
8.2.1. Izazovi	38
8.3. ANDROID HARDVER PLATFORMA.....	38
8.3.1. Centralna procesorska jedinica (CPU)	39
8.3.2. Ekran.....	39
8.3.3. Ram memorija (Random access memory i NAND fleš memorija).....	40
8.3.4. GPS.....	40
8.3.5. SD memorijske kartice	41
8.3.6. Bluetooth	41
8.3.7. Kamera.....	42

8.3.8. USB	42
8.3.9. Zvučnik / Mikrofon	43
8.4. ANDROID FAJL SISTEM I STRUKTURA PODATAKA.....	43
8.4.1. Koji podaci su skladišteni.....	44
8.4.2. Kako su podaci sačuvani	45
9. STUDJA SLUČAJA	46
9.1. Digitalno forenzička istraga telefona	46
9.2. Instalacija virtuelne mašine	47
9.3. Mobiledit	51
9.4. EnCase.....	55
ZAKLJUČAK.....	62
LITERATURA	63

Abstrakt:

Korišćenjem naučnih metoda i alata forenzičar prikupi mnogo dokaza sa posmatranog računara ili medija, tako da modeli treba da budu standardizovani radi lakše istrage, tako da u toku istrage treba da se vodi računa o koracima modela i što kvalitetnijem dokumentovanju u toku istrage i da se izabere odgovarajući metod za istraživanje digitalnog kriminala. Izvršioci kompjuterskih kriminalnih radnji u računarskim mrežama mogu biti lokalni ili udaljeni korisnici. Treba voditi računa i dovesti nivo zaštite na sto veći nivo, da bi se spriječile neželjene posljedice i da bi sto lakše moglo dovesti do otkrivanja počinoca. Ali i pored svih dosadašnjih otkrića u zaštitama nije se došlo do idealnog rješenja. Povećanjem napada na informacione sisteme korporacija i institucija koje sadrže povjerljive i osjetljive podatke, pokazala je potrebu za propisivanjem pravila kojima će se zaštititi vrijednosti neke korporacije.

Ključne riječi: Forenzička analiza, Androdi forenzika, Virtuelizacija, Cloud Computing, digitalni dokazi, rootkit, malware, NAND flash, klaster, forenzika mobilnih uređaja

Abstract:

Using scientific methods and tools, forensic collects many evidences from the watched computer or the media, so that the models should be standardized in order to make investigation easier, so that during the investigation the attention should be paid to the steps of the model and to documentation that should be as quality as possible, and the appropriate method should be chosen for the investigation of digital crime. Perpetrators of computer fraud in computer networks can be local or remote users. Care should be taken and a level of protection should be set to the highest possible level in order to prevent undesirable consequences as well as to reveal the perpetrators. But in spite of all contemporary discoveries in protection the ideal solution is not achieved. By increasing of the attacks on the information systems of corporations and institutions, which contain confidential or sensitive data, the need for regulation of rules for protection of the corporation values is important.

Key words: *Forensic analysis, Android forensics, Virtualization, Cloud Computing, digital evidence, rootkit, malware, NAND flash, cluster, mobile device forensics*

1. METODOLOGIJA IZRADE ISTRAŽIVAČKOG RADA

1.1. UVODNE NAPOMENE

U ovom radu su opisani modeli digitalne forenzike, koji nastoje da standardizuju korake digitalne forenzičke istrage, radi olakšavanja same istrage i veće vjerodostojnosti dokaznih podataka. Ovo omogućava konzistentnu metodologiju za suočavanje sa prošlošću, sadašnnošću ili budućnosti digitalnih uređaja. U nastavku rada opisana je aktivna digitalna forenzika. Ona se koristi na aktivnim sistemima i udaljenim sistemima radi detekcije krivičnog djela počinjenog na tom uređaju. U nastavku rada je opisana distributivna digitalna forenzika, prvi suštinski korak u zapošljavanju distribuiranog računarstva je da distribicioni fajl obuhvata digitalni dokaz preko računarskog klastera. U nastavku rada je opisana oblast virtuelne mašine, koje su softverski proizvod i služe kao virtuelni računar na postojećem računaru, veoma su korisne u forenzičkoj istrazi i uzimaju sve više maha u istraživanju zločina u digitalnom svijetu.

U nastavku rada je opisana digitalna forenzika i ukratko je rečeno sta je to digitalna forenzika i nabrojane su neke od njenih poddisciplina koje su zasebno obješnjene. Prikazano je šta su to digitalni dokazi, kako nastaju i kako se skladište. U nastavku rada su objašnjene poddiscipline digitalne forenzike. Originalno polje digitalne forenzike samo uključuje kompjutere (personalne računare). Prije otprilike 20 godina, kada su kompjuteri bili povezani u male lokalne mreže i ultimativno kroz najveću mrežu (Internet), pojam digitalne forenzike je bio suviše ograničen da bi obuhvatio čitavo polje. Zbog toga većina koji rade sa računarskom forenzikom pozivaju se na digitalnu forenziku. Oblasti digitalne forenzike su se širile i danas su u tendenciji sve većeg širenja na električne uređaje, tako da danas možemo naći dokaze na skoro svim savremenim elektonskim uređajima koji posjeduju sopstvenu memoriju, npr. aparati za kopiranje, skeniranje, ruterima, mrežnim uređajima, čak i u domaćinstvu se mogu naći digitalni dokazi kao što su uređaji za pranje veša (vešmašina), mikrotalasnim, šporetima, televizorima i drugim uređajima.

I poslednja opisana oblast je Android platforma. Android je operativni sistem za mobilne uređaje zasnovan na Linux-u koji razvija udruženje Open Handset Alliance (OHA) na čijem čelu se nalazi kompanija Google.

1.2. PREDMET ISTRAŽIVANJA

Kompjuterski kriminal, iz godine u godinu, postaje sve sofisticiraniji i efikasniji. Kriminalni napadi su sve više usmjereni prema korporacijama, a sve sa ciljem pribavljanja osjetljivih podataka i druge materijalne dobiti. Krađa osjetljivih podataka i dalje je glavni uzrok nastajanja kompjuterskih krijumčarenja.

Predmet istraživačkog rada ima za cilj da objasni digitalnu forenziku modele digitalne forenzike, da prikaže šta su to dokazi i na koji način su oni skladišteni. Zatim, upoznavanje sa Android platformom, digitalnom forenzikom Android platforme i opisivanjem mjesta nastanka digitalnog dokaza i skladištenje digitalnog dokaza.

Tehnologije iz dana u dan sve više napreduju i digitalni dokazi se šire na sve više uređaja, tako da se danas dokazi mogu naći u mnogim elektronskim uređajima koji imaju memorije na sebi, tako da je danas nezamislivo da korisnik ovih uređaja ne napravi makar jedan digitalni dokaz u toku jednog dana.

1.3. CILJEVI RADA

Naučni cilj ovog rada je upoznavanje sa modelima digitalne forenzičke istrage, aktivne digitalne forenzike, distributivne digitalne forenzike, virtuelnih mašina kao alata digitalne forenzičke istrage, definisanje i približavanje terminologije potrebama korisnika. Predstavljanje digitalne forenzike, njene poddiscipline i digitalnu forenziku Android mobilnih telefona.

Konkretni cilj ovog rada je predstavljanje generičkog modela digitalne forenzičke istrage i funkcionalnosti modela i mogućnosti standardizacije modela. Ova standardizacija se može primijeniti na niz digitalnih uređaja, od kalkulatora do desktop računara ili čak nerealizovanih digitalnih uređaja budućnosti. Koristeći ove modele buduće tehnologije, tehničke detalje potrebne za forenzičku analizu mogu iz instanci da obezbjede doslednu i standardizovanu metodologiju za pružanje elektronskih dokaza. Te prikazati načine dobijanja digitalnog dokaza, objasniti gdje sve nastaju digitalni dokazi i gdje se skladište. Mnogo puta bez sopstvenog znanja kreiramo digitalne dokaze. U ovom radu sam pomenuo kako pametni telefoni skupljaju digitalne dokaze bez našeg znanja.

1.4. ISTRAŽIVAČKE HIPOTEZE

Generalna ili opšta hipoteza: Činjenica je da je na svijetu sve više digitalnih dokaza i da populacija na ovoj planeti ima sve manje svoje privatnosti, ali opet druga činjenica je da ti

dokazi mogu olakšati procese istraživanja. Tako da danas ne možemo provesti ni jedan dan, a da ne ostavimo neki digitalni dokaz.

Radna hipoteza: Prikazati načine dobijanja digitalnog dokaza, te objasniti gdje sve nastaju digitalni dokazi i gdje se skladište. Mnogo puta bez sopstvenog znanja kreiramo digitalne dokaze. U ovom radu sam pomenuo kako pametni telefoni skupljaju digitalne dokaze bez našeg znanja. Na osnovu prikupljenih digitalnih dokaza u forenzičkoj istrazi, digitalni forenzičar izrađuje prijedlog sigurnosne politike za korporaciju. Pored ispunjenja osnovnih ciljeva istraživanja, očekuje se da olakša i smanji vrijeme istrage i da se poveća vjerodostojnost dokaza.

1.5. METODE ISTRAŽIVANJA I TOK ISTRAŽIVAČKOG PROCESA

Osnovna metodologija prirodnih nauka je eksperimentalna metodologija. Treba je shvatiti kao istraživački proces kojeg čine dvije cjeline: istraživanje i prezentacija rezultata istraživanja. U toku istraživanja potrebno je proći kroz četiri faze: postavljanje problema, formulisanje hipoteze, provjeravanje hipoteze i potvrđivanje (verifikacija) hipoteze.

Osnovne metode koje smo primjenili u naučno-istraživačkom radu su [1]:

Analitičke čiju osnovu čine:

- analiza,
- apstrakcija (apstrahovanje),
- specifikacija i
- dedukcija

i *sintetičke (neanalitičke)*:

- sinteza,
- konkretizacija,

- generalizacija i
- indukcija.

Opštenaučne metode u ovom naučno-istraživačkom radu su [1]. :

1. *hipotetičko-deduktivna metoda,*
2. *statistička metoda,*
3. *metoda modelovanja i*
4. *komparativna metoda.*

2. RAZVOJ MODELA DIGITALNE FORENZIKE

Oslanjajući se iz prethodnih sudskih protokola, postoje uobičajne mjere koje mogu biti generički definisani da proizvedu model koji ne zavisi od određene tehnologije ili elektronskog kriminala.

Osnova ovog modela je da se odrede ključni aspekti navedeni protokolima, kao i ideje iz tradicionalnih forenzika, posebno protokol za FBI fizičku kriminalističku pretragu (FBI02).

Predloženi model se može posmatrati kao unapređenje DFRW model, jer je inspirisan od njega.

Ključne komponente ovog modela uključuju sledeće u tabeli br. 1.:

Tabela br. 1. Ključne komponente modela DFRW.

1.	Identifikacija – Prepoznavanje incidenta od počinioca i utvrđivanje tipa. Ovo nije eksplicitno u oblasti forenzike, ali je značajno zbog uticaja drugih koraka.
2.	Priprema - Priprema alata, tehnike, traženje naloga i ovlašćenja nadgledanja i menadžment podršku.
3.	Pristupna strategija – Dinamički formulisan pristup zasnovan na potencijalnom uticaju posmatranja i specifičnosti alata. Cilj strategije bi trebao da bude maksimalno prikupljanje nepromjenjenih dokaza, a minimalan uticaj na počinioca.

4.	Očuvanje – Izolovati, obezbjediti i sačuvati stanje fizičkog i digitalnog dokaza. Ovo sprečava ljude od korištenja digitalnih uređaja ili omogućavanju drugim elektromagnetnim uređajima koji se mogu koristiti u okviru zahvaćenog radijusa.
5.	Kolekcija – Snimate fizički događaj i duplirajte digitalni dokaz koristeći standardne i prihvaćene procedure.
6.	Ispitivanje – U dubokoj sistemskoj pretrazi dokaza, koji se odnose na osumnjičenog. To se fokusira na identifikovanje i pronalaženje potencijalnog dokaza. Izrada detaljne dokumentacije.
7.	Analiza – Odrediti značaj, rekonstruisati dijelove podataka i izvesti zaključke zasnovane na nađenim dokazima. To može da uzme nekoliko iteracija ispitivanja i analizu i da podrži teoriju zločina. Razlika analize je u tome da se ne zahtjevaju visoke tehničke vještine, da bi se moglo uključiti više ljudi u obavljanju na ovom slučaju.
8.	Prezentacija – Sumiranje rezultata, objašnjenje zaključka. Ovo bi trebalo biti napisano u terminima laika, koristeći apstraktnu terminologiju. Svi apstraktni termini trebaju biti referencirani na konkretne detalje.
9.	Povrat dokaza – Obezbeđivanje fizičke i digitalne imovine se odgovarajući vraća vlasniku, kao i utvrđivanje šta i koji kriminalni dokazi moraju biti uklonjeni. Opet nisu eksplicitni forenzički koraci, ali svaki model koji sakupi dokaze rijetko je usklađen sa ovim aspektom.

Imajte na umu da ovi koraci nisu isto što i obične metode prikupljanja fizičkih dokaza, ali u činjenici apstrakcija sadašnjih praksi primjenjuje se na zločine koji uključuju digitalne dokaze (FBI 02). Veliki dio dokazanih istraženih tehnika i metoda postoji u više tradicionalnih forenzičkih disciplina.

Najviše se primjenjuju u sajberprostoru, ali se još uvijek ne smatraju punovažnim. Takođe, primjećujemo da se vrsta digitalne tehnologije uključuje u ove korake generički definisane najviše do ovih tačaka. To je veoma važno zato što dozvoljava standardizaciju procesa da bi definisali bez specifičnih egzaktnih uključenih tehnologija. Ovo omogućava konzistentnu metodologiju za suočavanje sa prošlošću, sadašnnošću ili budućnosti digitalnih uređaja. Npr. ova metodologija se može primjeniti na niz digitalnih uređaja, od kalkulatora do desktop računara ili

čak nerealizovanih digitalnih uređaja budućnosti. Koristeći ove modele, buduće tehnologije, tehničke detalje potrebne za forenzičku analizu mogu iz instanci da obezbjeđe doslednu i standardizovanu metodologiju za pružanje elektronskih dokaza. To će povećati nauku forenzike, jer pruža osnovu za analiziranje novih digitalnih / elektronskih tehnologija, dok u isto vrijeme obezbjeđuje zajednički okvir za sprovođenje zakona i pravosudnog sistema za ostvarljiv rad u okviru suda.

Za dodatne postupke će biti neophodno da se definišu različite klase digitalnih tehnologija po ovom modelu. Ove tehnologije su analogne papirnim dokumentima, video snimci i audio snimci su veoma dobro prihvaćeni kao dokazni materijal. Koristeći definiciju ove kategorije, sudski član može koristiti ovaj generički model da bi dodjelio više kredibiliteta na njih nego možda u tehnologije kategorija sa nestabilnim storidžom. Naravno, postoje mnogi detalji specifični za određene tehnologije koji se moraju riješiti, ali ovaj model omogućava uvođenje tih detalja. Koristeći ovaj model, metode prikupljanja mogu se razviti za svaku pod-kategoriju tehnologije, a potom razmatrati i definisati u okviru tog podpostupka. U idealnom slučaju, jedna razvijena i prefinjena metoda može uticati na razvoj metoda za druge tehnologije.

Činjenica, da posebna metoda prikupljanja je dodata u modelu kojem daje kategoriju kredibiliteta i uvjerava lica koja nisu tehnički obrazovana da iskuse skup sličnih dokaza koje su primjenjene na konkretan slučaj u istoj kategoriji.

Nastavljajući sa stalnim primjerom skladištenja, razmotrite članstvo čvrstih diskova HDD (korištenih u tradicionalnim kompjuterskim sistemima) i ugrađenu nepromjenjivu fleš memoriju (korištenih radi pomoćnih digitalnih uređaja, kao što su digitalne kamere, MP3 plejeri, USB ili drugi digitalni uređaji).

U ovom pedagoškom primjeru, obje tehnologije mogu da sadrže dokaze korisne sudskim članovima i posmatrajući ga kao stalni digitalni storidž, omogućava da se održi povjerenje, da se sadržaj može naći. Naravno, vađenje podataka će biti tehnološki zavisno, ali ispitivanje sadržaja može ponovo pratiti standardizovani postupak, jer je generalno u binarnom formatu.

Prednosti ovog generičkog modela su većina digitalnih uređaja, bez obzira da li su računarski sistemi i lični digitalni uređaji, digitalne kamere ili drugi uređaji, sadrže neku vrstu trajnog skladištenja koje se mogu analizirati na potencijalne dokaze.

Shvativši to [3]. ,podržavaju procedure i alate koji mogu da se identifikuju za razvoj prethodno definisanih pristupa, mogu da se koriste kao polazna tačka za nove tehnologije.

Nema potpunog modela bez razmatranja prednosti i mana. Jer u tom stadijumu se razmatraju prednosti, ali je važno pomenuti neke nedostatke.

To pokušava da pruži tačku gledišta koja može unaprijediti razvoj digitalnih forenzičkih praksi u identifikovanju sličnosti digitalnih tehnologija i rad unazad da uspostavi čvrste forenzičke procese koji se primjenjuju na mnogim digitalnim tehnologijama od pomoći.

Razmatranje mora da se sprovede, kako bi spriječili generičke korake koji daju nikakvu vrijednost procesa, jer nema praktične koristi od njih.

Drugo, ovaj model trebalo je da se primjeni na digitalnim uređajima. Tehnologije koje nisu digitalne nisu razmatrane u ovom radu, ali takođe mogu zahtijevati forenzičku analizu.

Pregled modela prednosti i nedostaka

Predloženi modeli prednosti:

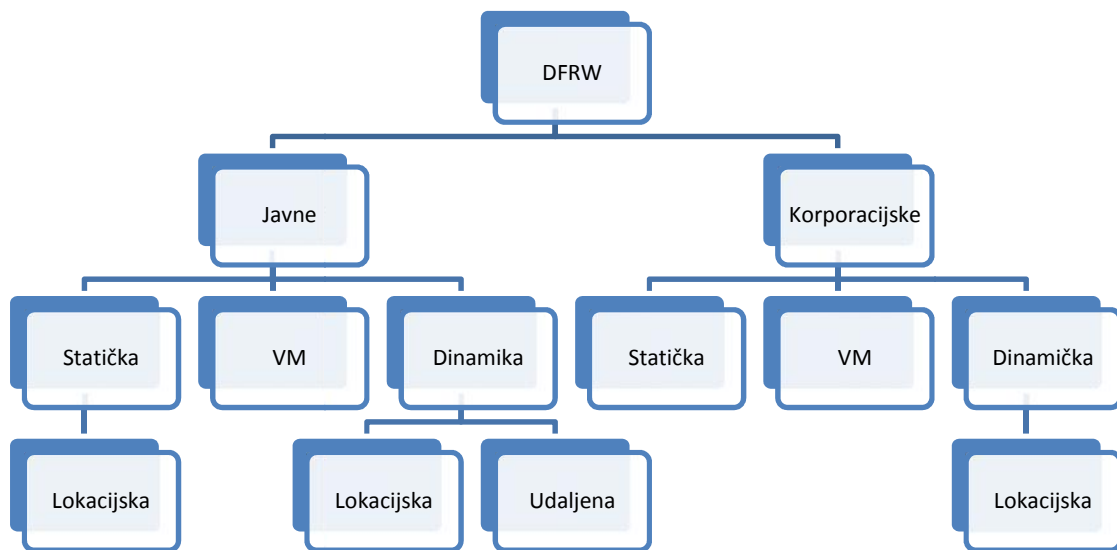
- Napravite dosledan i standardizovan okvir za razvoj digitalne forenzike.
- Mehanizam za primjenu istih okvira za buduće digitalne tehnologije.
- Generalizovana metodologija koju sudski članovi koriste da se odnose na terminologiju nestručnih posmatrača.
- Identifikujte potrebu za određenim tehnologijama definisanih alata u istoj kategoriji.
- Potencijal za uvođenje nedigitalne elektronske tehnologije u generičke.

Predloženi modeli nedostataka:

- Kategorije mogu biti definisane kao suviše uopštene za praktičnu upotrebu.
- Nema jednostavan ili očigledan način za testiranje modela.
- Svaka podkategorija dodana modelu će postati komplikovana za korištenje.

Ovo je važan aspekt bilo forenzičkog ili istražnog modela.

2.1.TAKSONOMIJA RAZVOJA MODELA DF ISTRAGE



3. AKTIVNA DIGITALNA FORENZIKA

Kada se desi incident, sistem za detekciju upada od organizacije će detektovati to i odgovor na incident i protokol (IR) organizacije će biti aktivan. Međutim, postaje neophodno da se integrišu aktivni forenzički protokoli istrage sa protokolom (IR) odgovornim za incident kako bi se osiguralo da su relevantni i prihvatljivi aktivni digitalni kompjuterski dokazi, da je dostupan ako je to potrebno za istraživačke svrhe. IR protokol se ne odnosi na značajne dokaze identifikacije, prikupljanja i čuvanja aktivnih podataka.

Razni alati i metodologije postoje za sprovođenje aktivne istrage, kao što je novo polje, koji se suočavaju sa brojnim izazovima. Prema [4]. aktivna forenzička istraga je otežana zbog

nedostatka definicija aktivne forenzike, odsustvo standardnih procedura u aktivnim istragama i sertifikacije i izopačenosti aktivnih dokaza.

Aktivna analiza je često povezana sa protokolom (IR) i sistemom za detekciju upada, ali je pomoćni program. Virusni program kao npr. od aktivnih alata za anliziranje. Većina aktivnih istraživačkih alata i tehnika su programski bazirani, međutim trenutna istraživanja su u razmatranju da koriste hardverske uređaje za dobijanje dokaza [5].

Aktivne forenzičke istrage se trenutno vrše pomoću daljinskog forenzičkog ispitivanja i nabavke alata, kao što su EnCase Enterprise edition i Pro Discover. Ovi alati koriste realne tehnike analize koje će koristiti program koji već postoji na sistemu tokom roka početka istrage [6]. Ciljana mašina je posmatrana sa udaljene lokacije.

Tipične aktivnosti uključuju ključne riječi pretrage, kopiranjem i raspakivanjem fajlova i zapisa sa aktivne udaljene posmatrane lokacije. Korisnik nije svjestan procesa i istraga sa može nastaviti bez njegovog znanja o tome. Istražitelj može steći dokaze u aktivnom proizvodnom okruženju.

Istraživač takođe može koristiti mrežnu forenziku da identifikuje izvore, aktivne mrežne dokaze. Nije moguće da prođe sve aktivnosti na mreži, ali to je suština tokom aktivne istrage da bi identifikovali potencijalni izvor, npr. DNS i koji je server, vebisajt, ftp servlet, local Ethernet server, server baze podataka, chat server, mrežne rutirane tabele ili da vrati poruku od SOAP servleta. Dokazi koji mogu biti sakupljeni su npr: klevetnički vebisajtovi, ilegalni fajlovi, saobraćaj iz port skeniranja, rutirane tabele, jačina bežičnog signala i njegova detekcija.

Druge softverske tehnike identifikovane od [5]. da okupe aktivne dokaze uključujući virtualne mašine i psihičke memorije uređaja, hibernaciju i proces lažnog fajla. Sve ove gore navedene tehnike su bazirane na softveru i oslonjene na operativni sistem, ali kernel operativnog sistema nije povjerljiv resurs kao što može biti zaražen kernel. Ovo predstavlja prijetnju pouzdanosti dokaza . Drugi problem je u tome što operativni sistem mora izvršiti komandu i stoga treba upisati u memoriju i onda uništiti dokaze o radu. Carrier [5]. je predložio hardver na bazi memorije postupka akvizicije. On je predložio da koriste razvoj hardvera gdje je kartica instalirana već u PCI bus koji će sakupiti dokaze i upisati ih u sadašnji storidž uređaj. Obrazloženje raznih tehnika razlike kao daljinska online forenzička istraga, snimiti podatke

mimo redosleda [4]. . Druge aktivne tehnike istrage će razmotriti redosled volatilnosti dokaza. Autori su proučavali struje, „ aktivne ili daljinske u realnom vremenu“, metodologije i predlažu da uključe aktivne forenzičke alate i tehnike, istraga u realnom vremenu kao što je daljinska istraga aktivne digitalne forenzike [7]. , [4]. , [8]. , [9].

Ne postoje ili su veoma ograničene metodologije za aktivne digitalne forenzičke istrage. Rad predlaže sledeću definiciju za aktivnu digitalnu forenziku: Aktivna digitalna forenzika je sposobnost organizacije da prikupi(identifikuju, sakupljaju i čuvaju) CDE u aktivnom okruženju i da obezbjedi uspešnu istragu.

Ciljevi za Aktivnu DF su:

- Prikupiti sve relevantne CDE (uključujući dokaze) u aktivnom sistemu ili proizvodu okruženja korištenjem prikladnog alata i tehnologije.
- Minimizirati efekte i uticaje u toku incidenta
- Obezbediti značajnu polaznu tačku za reaktivnu istragu u parametrima rizika kontrole okvira od organizacije.

Rad identifikuje sledeće faze za aktivnu digitalnu forenziku iz literature [7]. , [4]. , [8]. , [9].

Bitno je primjeniti na relevantne incidente i protokol krivičnog uviđaja [10]. npr. uzeti u obzir zahtjev fizičkih krivičnih uviđaja. Formulirane su sledeće faze nezavisne od bilo kojeg alata ili tehnologije.

3.1. ODGOVOR NA INCIDENT I POTVRDA

Istražitelj se mora držati utvrđenih koraka za ovu fazu naznačenu u Reaktivnoj digitalnoj forenzici, ali mora odrediti koji neodređeni ili aktivni dokaz mora biti stečen da bi se uspešno istražio incident kao što je to prepisano od strane proaktivne DF, komponente ili nedostajući potencijalni dokazi za nove ili nepoznate incidente, formulirati plan istrage aktivne digitalne forenzike. Ako polise rizika upravljanja dopuste da nastavi istraga aktivne digitalne forenzike, početi drugačiju reaktivnu istragu. To može biti unaprijed definisan okidač događaja da bi počelo aktivno praćenje ili druge procedure čim se aktivira upozorenje za incident.

Kao što se aktivna digitalna forenzika bavi tekućim ili incidentom u realnom vremenu, obuzdavanje strategije i plana je veoma važno, jer će sistem ostati aktivan i ne može biti ugašen.

3.2. DIGITALNA FORENZIČKA ISTRAGA

Sticanje dokaza – Sakupite dodatne aktivne nedostajuće dokaze ili zahtjevati od korištenjem CDE mapi koristeći odgovarajuće alate, tehnike ili aplikacije koje će biti potrebne da profilisu napadača, prikupiti nepromjenjive dokaze ili utvrditi izvor napada. Osigurati autentičnost svih ekstraktovanih podataka usitnjavanjem dokaza odmah nakon prikupljanja procesa, da sačuva prije analize. Bitno je da se dokumentuju sve radnje, zahtjevano da dokažu da mrežni nadzor bi stekao održive dokaze.

Važno je da se automatizuju i aktiviraju odgovarajuće alatke za prikupljanje dokaza, tehnologije ili aplikacije što je prije moguće (Po mogućnosti odmah nakon što je incident izazvan) :

- Nametnuti minimalnu intervenciju korisniku;
- Obezbjediti da sve zahtjevano neophodne akcije obavljaju i da nisu nametljive;
- Obezbjediti minimalne modifikacije od statičkog digitalnog dokaza;
- Prikupljanje podataka treba da prati naredbu promjenjivih i prioritet sakupljanja digitalnog dokaza.

Dobiti neprioritetne ili promjenljive dokaze putem tradicionalnog pribavljanja dokaza i kopija ekstraktovanih podataka treba da se vrši samo kada originalni podaci i vremenski identifikatori ne utiču. [4].

3.3. ANALIZA

3.3.1. Faza analize

- Analizirajte preliminarne dokaze kako bi se utvrdilo da li postoji dovoljno dokaza za rekonstrukciju incidenta i da podrži početnu hipotezu;

- Dokumentovati sve aktivnosti u svim vremenima da bi se obezbijedio integritet svih dokaza;
- Održavati lanac dokaza i čuvati ga i procese validacije tokom čitavog vremena, faza dokazne istrage aktivne digitalne forenzike. Važno je da se obezbijedi pouzdanost i prihvatljivost rezultata.

3.3.2. Faza rekonstrukcije događaja

- Ova faza koristi rezultate iz analize koraka da uradi ograničenu rekonstrukciju događaja.
- Cilj je utvrditi da li nedostaje ili se aktivno zahtjeva stečeni dokaz, da odredi kada da prekine aktivnu istragu digitalne forenzike.
- Prestanak uslova će biti propisan od Risk menadžmenta framework, npr. koštaće preskupo, procijenice uticaj, itd.

Ponovite fazu dva ako aktivni dokaz još uvijek nedostaje.

3.3.3. Faza završetak

Ako je dovoljno dokaza prikupljeno ili istraga prekinuta zbog drugih razloga, istražitelj će dokumentovati slučaj sa sakupljenim digitalnim dokazima za reaktivnu istragu tima da završi istragu. Čim se aktivno digitalno forenzička istraga okonča, reaktivna komponenta će nastaviti da analizira i rekonstruiše događaj koristeći sve sakupljene dokaze (uključujući statične sakupljene digitalne dokaze ili fizičke dokaze) potrebne da zaključi istragu.

4. DISTRIBUTIVNA DIGITALNA FORENZIKA

Većina digitalno forenzičkih poslova je prirodno fajlcentrična sa nekoliko veoma zavisnih poslova među drugačijim fajlovima. Tako odabran individualni fajl kao primarna distribucija

jedinice minimalne sinhronizacije i komunikacije među nodovima u klasterima. Konsekventno, prvi suštinski korak u zapošljavanju distribucionog računarstva je da distribicioni fajl obuhvata digitalni dokaz preko računarskog klastera.

Iz perspektive keširanja, fajl treba raširiti tako da se mnogi od njih mogu čuvati u RAM-u tokom obrade. Velike datoteke koje su znatno veće od raspoložive fizičke memorije, na datoj mašini mogu da se podijele na dijelove ili obrađuju odvojeno. Poželjno je, ali ne presudno da postoji dovoljno fizičke memorije da kešira sve korisne fajlove tokom obrade. Ali RAM će biti automatski obrađen od strane hosta virtualne memorije sistema. Iako ne postoje eksperimentalni rezultati kao objavljeni, zajedničko iskustvo iz opšte upotrebe operativnog sistema predlaže, zavisno od pristupa obarscima, preopterećenje od čak 50 % može imati skroman uticaj na performanse.

Maksimalno iskorišćenje procesora je malo komplikovanije. Jedan od pristupa je da se raspodjele fajlovi određenog tipa ravnomijerno tokom obrade nodova. Obrazloženje je da kad god je izdata operacija, npr. traži se regularni izraz, svi nodovi će imati sličanu količinu posla da odrade, dakle procesorska iskorišćenost će biti maksimalna. Međutim više sofisticirana obrada koja pokušava da dovede u vezu različite predmete (kao što su tehnika klasifikacije slike) može sputati ovaj obrazac datoteke distribucije i povećava potrebu za mrežnim komuniciranjem.

U ovom slučaju, koncentrišući fajlove u manje nodova odgovarajući komunikacioni obrazac može dati bolje rezultate. Drugi trend upotrebe višeprocorskih sistema posebno u visokim izračunima performansi klastera. U SMP svi procesori imaju jedinstven pristup zajedničkom memoriskom kešu koji su povećali brzinu komunikacija između procesora. Da bi optimizovali performanse, karakteristike arhitekture moraju biti uzete u obzir prilikom faze obrade i distribucije. Distributivni alati digitalne forenzike su još u povoju, preliminarni rezultati istraživanja jasno pokazuju prototipove i prednosti pristupa. Distributivna okruženja za velike istrage pružaju pogled na to kako su distributivni sistemi prihvaćeni u digitalnoj forenzici. [11]. Istraživač kontroliše istragu na jednoj radnoj stanici preko GUI sličnim drugim forenzičkim alatima u opštoj upotrebi. Iza GUI-a, međutim, operacije digitalne forenzike se sakupljaju od nodova u klasterima ili vraćaju sabrani rezultat i dinamički predstavlja korisniku čim postanu dostupni. Tako da bi izvršili komplikovanu regularnu pretragu izraza naspram velikog cilja.

Npr. Istraživač uđe u jedan izraz i pretražuje paralelno preko svih keširanih dokaza. Kako podaci akumuliraju oni se prikazuju za korisnika. Postoje tri značajne razlike u korisničkom iskustvu između Distributivnih okruženja za velike istrage i većine tradicionalnih, alat digitalne forenzike je jedna mašina.

Prvo, sistem ne obavlja nikakvu predobradu, već jednostavno učitava forenzički imidž i spreman je da izvrši upite. Sistem podržava dva različita načina za učitavanje ciljnih imidža. Prvi je keš mod, u kome centralni koordinirani čvor čita cijeli uneseni imidži distributivne podatke preko mreže za pomoćne računare. U drugom slučaju učitavanja koordinator upućuje pomoćne računare da učitavaju određene podatke iz ciljnog imidža, koji je na zajedničkom serveru. Preliminarni eksperimenti su pokazali istovremena učitavanja, modul učitavanja ima mnogo veće iskorištenje čitanja visokog skladištenja RAID performansi, više od 30 % u nekim slučajevima. Nodovi mogu koristiti svoj lokalni disk za keš, tako da naknadna opterećenja imidža uzmu samo dio originalnog vremena. Druga razlika je u tome, jer sve radnje se obavljaju daljinskim putem, reaguje na ostatke i raspoloživo praćenje rada na parcijalnim rezultatima (npr. otvorite odgovarajuću datoteku) čim postanu dostupne. Takođe je moguće da se postavi novi upit, npr tekstualna pretraga, će pokazati, period prvog prikazivanja je i dalje prekinut, sa malo primjetnim promjenama u ukupnim performansama. To je zbog činjenice da su mnoge operacije, kao što su tekstualna pretraživanja, su I/O granice. Kada I/O usko grlo preovlada kroz keširanje, procesor može lagano upravljati istovremenim upitima. Opštije to je razlog da se očekuje vrijeme izvršenja preklapanja I/O graničnih operacija da budu veoma blizu tom jednom upitu. Konačna razlika je u istraživačkoj operaciji koja se izvršava u dijeliću vremena zahtijevanog na jednoj radnoj stanici.

Posebno eksperiment u 8 čvoru [11]. u trenutku super linearnog ubrzanja za I/O – graničnih forenzičkih operacija. Ubrzanje u tom slučaju vjerovatno će biti konstantan faktor koji se ne odnosi na konkurentne faktore tj. brojeve nodova ali reflektuje vrijeme nepristupanja iz diska. Pored toga, još između klastera i perforanse radne stanice rastu kao funkcija ciljane veličine.

To se događa zato što neslaganje između resursa jedne radne stanice i ciljane obrade zahtjeva raste, druge štetne nus pojave poput virtualne sistemske memorije i suparništvo za RAM resurse između indeksa strukture i ozbiljnog dokaza degradira preformanse. Za CPU vezanim

operacijama i kao detektovanje steganografije, posmatrano ubrzanje DELV je približno jednako konkurentnom faktoru.

Jedno važno pitanje je dokazati vrijeme obrta istrage. Npr. ako se cijela meta može zadržati keširana u RAM-u. Skup procesiranja (kao što su string indeksiranje), dizajnirani da ubrzaju I/O granične operacije, kao što je pretraga stringova, može biti kompletno eliminisana u korist na zahtjev distributivnog izvršavanja operacije. Još jedna atraktivna mogućnost je obavljanje koraka predobrade paralelno na klasteru i zatim koristiti rezultat na lokalnoj radnoj stanici. Ovo može biti nemoguće ako specifični procesi trebaju samo dostupni vlasnički softverski paket, kao što je FTK. Međutim to još uvijek može biti moguće u skladištu RAM-a, resursa klastera i napraviti distribuirani RAM disk. Predpostavljajući dovoljno brzu mrežu (npr. gigabitnu ili bolju) kao što bi mrežni dražv trebao nadgraditi lokalni disk kada značajan dio funkcija diska operacija nisu sekvencijalni. Gledajući unaprijed, distributivni kompjuting takođe dopušta sofisticiranu istragu operacija da bitno poboljšao. Npr. automatizovano sklapanje fragmenata (dijelova) imidža [12]. i analize digitalnih imidža da utvrdi da li su neovlašćeno ili gdje kompjuterski generisani [13]. , automatska detekcija steganografije dokumenta [14]. .

Sofisticirana imidž analiza je jedan od primjera, gdje dublje analize imidža možete sačuvati, značajnu količinu ljudskog napora, ali analiza može samo biti izvodljiva ako se mogu primjeniti dovoljni računarski resursi.

5. DIGITALNA FORENZIKA VIRTUELNIH MAŠINA ILI VIRTUELNA MAŠINA KAO ALAT

Virtuelna mašina ili VM je softverski proizvod koji omogućava korisniku da kreira jedno ili više okruženja (platformi) od kojih svako simulira svoj skup hardverskih komponenti (CPU „Procesor“, HDD „Hard disk“, RAM „Random access memory“, mrežne komponente i druge hardverske komponente) i sopstveni softver. Idealno je kada se svaka virtuelna mašina ponaša i radi kao potpuno nezavistan računar sa sopstvenim operativnim sistemom i hardverom. Korisnik može kontrolisati svako okruženje nezavisno i ako je potrebno, umrežiti virtualne računare zajedno ili ih spojiti na eksternu fizičku mrežu.

Virtuelno okruženje je samo po sebi kompleksno, a virtualne mašine inherentno dinamične i kreću se između brojnih fizičkih servera. U ovakvom dinamičnom okruženju ranjivosti i greške konfiguriranja mogu se širiti slučajno i neotkriveno. Teško je nadgledati log datoteke i održavati stanje bezbjednosti ovih virtualnih mašina.

Virtuelno okruženje omogućava forenzičaru da pristupi kompletnom stanju ciljnog sistema ne oslanjajući se na to da ciljni sistem obezbijedi informacije. Takođe, ovaj tip aktivne forenzičke analize može biti ekstremno težak za antiforenzičku detekciju, ako se uopšte i može otkriti. Pretpostavimo da je na računarskom sistemu aktivna virtualna mašina koju nadgleda monitor virtualne mašine. Računarski sistem ima mrežne konekcije, na očigled u svakom pogledu izgleda kao regularni računarski sistem. Napadač koji upadne u sistem pokušava sve kao na regularnom sistemu. Kada se napad odbije ili se sumnja u napad, analitičar zaštite ne aktivira programe zaštite na napadnutom sistemu da analizira napad. Umjesto toga uključi monitor virtualne mašine ili drugu virtualnu mašinu pod kontrolom monitora virtualne mašine i pogleda unutar napadnute virtualne mašine. Ova tehnika naziva se virtualna mašinska introspekcija.

Monitor virtualne mašine ima potpun pristup svim memorijama u virtualnoj mašini i može čitati i po potrebi mijenjati njihov sadržaj. Moguće je da neki program iskoristi monitor virtualne mašine da rekonstruiše sadržaj iz memorijskog prostora procesa, pa čak i određene sadržaje iz memorije kernela virtualne mašine, koristeći master partition tabele monitora virtualne mašine za dobijanje imidža memorije virtualne mašine. Odatle program pristupa memoriji kernela virtualne mašine da locira procese od interesa i njihove memorijske stanice. Program zatim može tačno rekonstruisati šta da radimo sa ovim informacijama. Ovaj pristup ima dodatne prednosti u odnosu na standardne metode forenzičke analize:

- U statičkoj forenzičkoj analizi imidža forenzičar gubi sadržaj RAM memorije, koji može biti kritičan za rekonstrukciju događaja.
- U dinamičkoj, aktivnoj forenzičkoj analizi sistema u radu, dobijeni podaci mogu biti pogrešni, ako su kernel biblioteke ili sami programi kompromitovani.
- Ako se forenzička analiza vrši sa monitorom virtualne mašine, bilo koja kompromitovana komponenta operativnog sistema, biblioteka, programa, na virtualnoj mašini, biće irelevantna pošto je alati zaobilaze i rade samo na monitoru virtualne mašine. U ovom

slučaju forenzičar dinamičkom analizom može gledati u memoriju, ali zato što virtuelna mašina nije isključena, ona je praktično statička jer je sadržaj memorije zadržan.

6. DIGITALNI DOKAZI SU SVUGDJE

6.1. ŠTA JE TO DIGITALNA FORENZIKA?

Izraz forenzika je naziv za primjenu širokog spektra naučnih grana za utvrđivanje činjenica u sudskim ili upravnim postupcima. Izraz dolazi od latinskog pridjeva *forensis* ("pred forumom", odnosno "pred sudom") [22]. Najprihvatljivija definicija Digitalne Forenzike dolazi od definicije kompjuterska forenzika. Kompjuterska forenzika je sakupljanje, čuvanje, analiza i prezentacija elektronskih dokaza. Konkretno, digitalna forenzika je primjena kompjuterske tehnologije po pitanju zakona, gdje dokazi uključuju stavke koje su kreirane i stavke koje su kreirane od strane tehnologije. Kao rezultat interakcije, podaci kreirani od tehnologije zahtjevaju da procesi tehnologije programima stvaraju podatak. Podatak kreiran kao rezultat izazvan akcijom koju vrši lice ili korisnik treba da rezultira čuvanjem podatka manualno i automatski. Razlika u ove dvije vrste podataka iz dokaznog stanovista je, da automatski bude izvršen nezavisno od interakcije korisnika, kada računar ili drugi uređaj bilježi podatke kroz neki proces koji je dizajniran. Kada se podaci čuvaju ili se vode kao odgovor na akcije korisnika, to je kreiranje ličnih podataka.

To su lični podaci koji bi na kraju trebalo da budu pripisani pojedincu. Međutim pripisivanje podataka pojedincu je teško zbog prisustva ili odsustva individualnosti korisnika računara, sigurnosti da zaštiti svoj korisnički nalog i stvarnog postavljanja osobe na istom mjestu u vrijeme kada su podaci stvoreni.

6.2. ŠTA JE DIGITALNI DOKAZ?

Digitalni dokaz počiva kao elektronski podatak, bilo u formi transakcije dokumenta ili neke vrste medija, kao što su audio i video snimci. Transakcioni uključuju finansijske transakcije kreirane tokom nekog procesa stvaranjem usluge, uobičajnog plaćanja, putem interneta ili nekih drugih načina plaćanja. Skoro svaka današnja transakcija je digitalizovana u nekom trenutku i postaje

digitalni dokaz, npr. plaćanje računa u bankama, podizanja novca sa računa, plaćanje kreditnim karticama i mnogi drugi načini transakcije.

U današnjem povezanom svijetu je skoro nemoguće da na neki način ne ostavite elektronski trag putem plaćanja.

Sve većom pojavom socijalnih mreža i sve većom pojavom različitih društvenih medija stvorila se potpuno nova oblast rasprostranjenih elektronskih dokaza. Ljudi danas sve više dijele svoja svakodnevna dešavanja na socijalnim mrežama, njihove lične slike, stihove, pjesme, aktivnosti, političke stavove, političke opredjeljenosti, dnevne događaje, pa čak i njihove lokacije preko društvenih mreža kao što su Google+, Facebook , Twiter-a i mnogih drugih[17] .

Da bi elektronski podatak postao digitalni dokaz, mora se negdje skladištiti da bi na kraju bio dostupan i on mora biti u mogućnosti da se povрати kada ga traži forenzički ispitivač. Jedan od velikih izazova danas nije da li može postojati digitalni dokaz, pitanje je gdje je taj dokaz smješten, kako dobiti pristup tom skladištu i konačno da se oporavi i obradi digitalni dokaz.

Potencijalne lokacije skladištenja elektronskih dokaza se šire svakog dana, na osnovu podataka koji se nalaze u mobilnim telefonima i kompjuterima, koji se skladište u oblaku gdje se usluga nezavisnog skladištenja obezbjeđuje na HDD na internetu za ljude i preduzeća. Sve više usluga i kompjuterskih procesa ide na Internet gdje kompanije nude softverske usluge. Npr. gdje kompanije nude kao uslugu softver na svojim serverima gdje vas oslobađaju kupovanja računarske opreme i time vam nude jeftinije mogućnosti, npr. nude MIS ili ERP i još dosta mogućnosti ili online igrice koje se potpuno igraju preko interneta bez instalacije na vašem računaru.

6.3. KAKO JE DIGITALNI DOKAZ NASTAO I KAKO SE SKLADIŠTI

Kad god neko kreira e-mail poruku, piše dokument pomoću Notepad ili Word-a ili nekog programa za obradu, vozi automobil sa uključenim (GPS) uređajem ili nešto plaća preko interneta, on stvara digitalni dokaz. Rad na računaru, surfovanje internetom i telefoniranje sve ovo stvara digitalne dokaze. Digitalni fotoaparati, digitalne video kamere, web kamere i audio digitalni snimači prave digitalne dokaze.

To su više poznati oblici digitalnih dokaza. Međutim, lako je predvidjeti mnogo načina na koje mi stvaramo digitalne dokaze, ali mnogo puta bez znanja da to radimo. Ako igrate igrice preko interneta (online) sa drugim igračima, gledate video sa interneta, kupujete preko raznih online prodavnica vi stvarate digitalni dokaz. I ne zaboravite da ako posjedujete foto kopir, skener, fax ili neki sličan uređaj koji posjeduje sopstvenu memoriju moguće je da kreirate digitalne dokaze. Sigurnosne kamere kada ulazite u neki objekat prave digitalni zapis vaše posjete. Ovih dana je skoro nemoguće da ne napravite vid nekog digitalnog dokaza.



Slika br. 1. Kamere na putu

Čak i ako ste daleko od vašeg računara ili mobilnog uređaja, vas može da snimi neka kamera koja je postavljena na određenom mjestu (put za motorna vozila, objekti , centar grada itd.) ističući vašu lokaciju ili ako vozite automobil i prekoračite brzniu i napravite neki prekršaj, na osnovu digitalnog dokaza snimljenog kamerom o vašem prekršaju, poslaće ga na vašu adresu i koristiti kao digitalni dokaz. U početku razvoja računara, jedini uređaj za skladištenje je bila floppy disketa ili audio kaset. Kada želite da podjelite fajl ili dokument sa nekim morali ste snimiti na floppy disketu ili na audio kasetu.

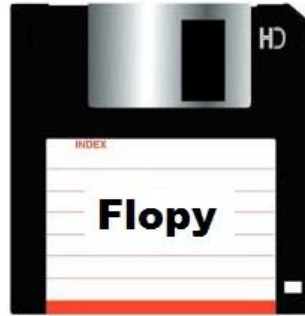
U današnje vrijeme skladištenje ne predstavlja više problem, današnji prosječni korisnik računara ima više načina skladištenja kao što su HDD, USB, prenosivi HDD, prostor u oblaku(Cloud computing), CD, DVD, itd. Floppy diskete su skoro izbačene iz upotrebe zbog malog kapaciteta, a zamjenio ih je USB[17].

Kao rezultat ovog nevjerovatnog rasta i mogućnosti skladištenja, danas se digitalni dokazi mogu naći od diskete, USB, HDD, pa do ogromnih storidža na nekim web serverima.

Visoke gustine, 3,5 inčni floppy disk mogao je da sačuva 1,44 megabajta podataka. Danas korisnik može da priključi HDD na USB port, gdje HDD od 1 TB zamjenjuje 728.177,77 Flopy disketa Slika br. 2.



HDD



1 HDD (1TB) = 728.177,77 Flopy (1.44 MB)

Slika br. 3. Poređenje memorijskih uređaja.

Kao što sve više ljudi koristi udaljena skladišta za rezervne kopije koristeći online backup servise kao što su Carbonite, Mozy Pro i niz drugih online backup rješenja koja nude čuvanje podataka na Internetu putem računara u oblaku, postaje sve veći izazov za trag gdje svi podaci mogu da borave u forenzičkom slučaju.

Govoreći o oblaku, sada postoji mnogo aplikacija i skladišta na raspolaganju kroz usluge skladištenja kao Google Apps, Google Docs, Microsoft's Windows Live Skydrive, Apple's Mobile Me, Dropbox[17].

Najčešće korištena aplikacija za korisnike koji žele da se povežu jedni sa drugima je e-mail. E-mail je takođe jedan od najčešće traženih oblika digitalnog dokaza u svim vrstama predmeta istrage.

7. PODDISCIPLINE DIGITALNE FORENZIKE

Originalno polje digitalne forenzike uključuje samo kompjutere (personalne računare). Prije otprilike 20 godina, kada su kompjuteri bili povezani u male lokalne mreže i ultimativno kroz najveću mrežu (Internet), pojam digitalne forenzike je bio suviše ograničen da bi obuhvatio čitavo polje. Zbog toga većina koji rade sa računarskom forenzikom pozivaju se na digitalnu forenziku.

Oblasti digitalne forenzike su se širile i danas su u tendenciji sve većeg širenja na električne uređaje, tako da danas možemo naći dokaze na skoro svim savremenim elektronskim uređajima koji posjeduju sopstvenu memoriju, npr. aparati za kopiranje, skeniranje, ruterima, mrežnim uređajima, čak i u domaćinstvu se mogu naći digitalni dokazi kao što su uređaji za pranje veša(vešmašina), mikrotalasna, šporet, televizor i drugi uređaji.

Sa uvođenjem kompjuterske obrade na drugim uređajima, kao što su GPS, automobilski kompjuteri, kamionske crne kutije, avionske crne kutije, mobilni uređaji, tablet računari i još mnogi drugi uređaji, polje digitalne forenzike se proširilo na poddiscipline digitalne forenzike. Svaka poddisciplina je dio digitalne forenzike.

7.1. KOMPJUTERSKA FORENZIKA

Kompjuterska forenzika je najstarija poddisciplina koja čini digitalnu forenziku. U mnogim slučajevima, prakse se samo fokusiraju na ovu oblast. Kompjuteri su često glavni izvori digitalnih dokaza u predmetu i to sa dobrim razlogom. Kompjuter može da sadrži velike količine korisnih informacija u predmetu o sebi. Može sadržati korisne informacije o drugom uređaju kao što je USB, mobilni telefon, digitalni fotoaparat i prenosni HDD, jer svi ovi uređaji se povezuju na računar i ostavljaju tragove. Npr. da napravite rezervnu kopiju podataka na mobilnom

telefonu, on mora da bude povezan sa računarom. Isto važi i ako želite da uklonite slike sa digitalnog fotoaparata ili USB stika.

Kompjuterska forenzika je primarna u ispitivanju dokaza pronađenih na računaru: HDD, korisničkom nalogu, log datotekama, slikama, e-mail porukama i neke instance za pregled podataka na drugim hardverskim komponentama na kompjuteru, kao memorije. Temelj kompjuterske forenzike je spašavanje podataka i veći dio ove poddiscipline se zasniva na tom aspektu.

7.2. MREŽNA FORENZIKA

Neki smatraju da mrežna forenzika treba da bude zasebna poddisciplina digitalne forenzike, dok je drugi smatraju kao samostalnu disciplinu. Postoji mnogo aspekata mrežne forenzike kojoj su posvećene mnoge knjige poddisciplina mrežne forenzike koje obrađuju: bezbjednosti, hakovanje, detekciju upada, zlonamjernih programa i rootkita.

Ovi napadi mogu doći od hakera, personalnih organizacija, malicioznih programskih kodova (malicioznih programa), crv, trojanac ili neki drugi malver. Eksperti mrežne forenzike rade na pronalaženju mogućih napadača na mreži i otklanjanju istih.

Mrežna forenzika uključuje analizu mrežne opreme kao što su ruteri, svičevi (eng. *switch*), habovi (eng. *hub*), NIC (eng. *Network Interface Card*), te razni mediji poput parica, optičkih kablova i sl.[19].

Mrežni alati sakupljaju podatke iz već postojećih dnevnika aktivnosti komponenti mreže ili se instaliraju na mrežu radi sakupljanja podataka u realnom vremenu.

7.3. FORENZIKA MOBILNIH TELEFONA

U ogromnom broju korisnici i ne shvataju sve mogućnosti pametnih telefona (Smart phones), iPod-a, 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 mobilni telefoni su 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 mijenjaju veoma brzo, tako da snalažljivi korisnici često otkriju metode prikrivanja podataka i upotrebe novih uređaja za nenamjenjene svrhe pre nego što forenzički istražiocu u potpunosti uspiju da analiziraju uređaje i pronađu njihove slabosti i mogućnosti.

U većini računarskih područja ovaj je problem prisutan, ali je posebno izražen na području mobilnih tehnologija, jer je brzina promjene tako velika. Bez obzira što korisnici često povećavaju količinu HDD i radne memorije(RAM) na svom računaru, oni u suštini koriste istu tehnologiju u toku cijelog vijeka upotrebe. Pri vršenju istrage mobilnih uređaja treba imati na umu da se oni razlikuju od računara u tri važne činjenice[18]:

1. Veoma česte, brze i lake promjene 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.

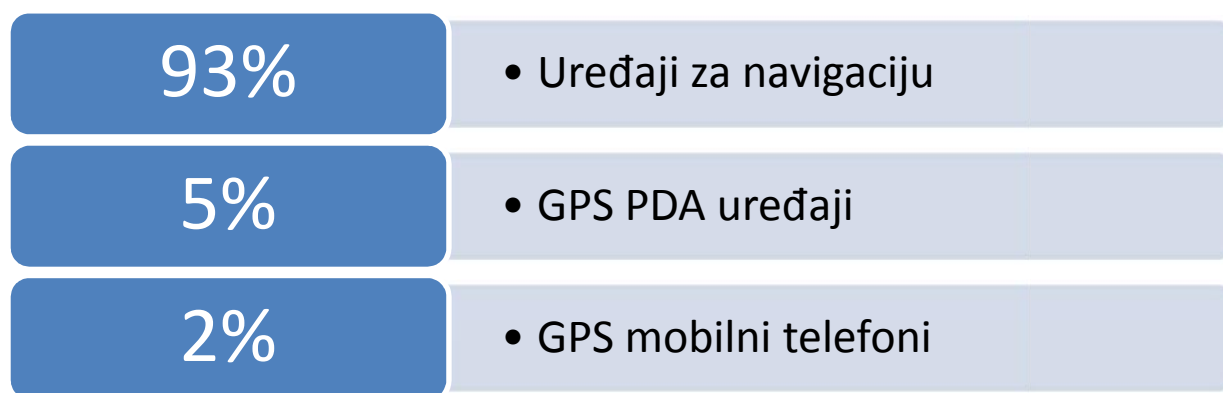
Postoje tri osnovna načina na kojima mobilni uređaji komuniciraju i koji koriste sve kompanije koje proizvode mobilne uređaje:

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 koristi na malim razdaljinama, do 50 metara.
3. IC (Infracrvena komunikacija): koristeći stariju metodu komuniciranja mobilni uređaji mogu razmjenjivati informacije koristeći infracrveni dio svijetlosnog spektra. Ova je metoda usmjerene prirode za komunikaciju među uređajima, njihovi infracrveni portovi moraju biti okrenuti jedan prema drugome.

7.4. FORENZIKA GPS UREĐAJA

Prije nekoliko godina bilo je neobično vidjeti auto sa GPS (global positioning system) uređajem u njemu. Kada je cijena opala i tehnika napredovala, GPS uređaj pojeftinio, postao je mnogo zastupljeniji, tako da danas je uobičajno vidjeti auto sa GPS uređajem[17]. Mada GPS uređaji imaju široku primjenu: avioni, brodovi, kamioni, biciklisti, motociklisti, planinari i još u mnoge druge svrhe se kroiste. GPS forenzika koristi dokaze od GPS zapisa. Kao dokaz se može koristiti informacija kao što je skoro posjećena lokacija, omiljene lokacije, lokacije navođene adresama ulica, takođe je moguće vratiti obrisane informacije sa GPS uređaja.

Tabela br. 2. procentualni prikaz upotrebe GPS-a preko uređaja.



GPS zapisi su validni kao dokazi i ako ne možete doći do GPS uređaja. Zapis može biti korišten da bi se vidjelo kretanje osobe ili vozila. Uvidom u podatke dostupne sa GPS uređaja, moguće je procijeniti koliko brzo je neko vozio, a ako su pravili pauze moguće je ustanoviti gdje su pravili pauze i koliko su se dugo zadržali. Ako je osoba osumnjičena za zločin, GPS zapisi mogu biti od pomoći kao dokaz, ako je ta osoba otišla na mjesto gdje se desio incident.

Npr. pretpostavimo da se osumnjičeni tereti za izvršenje ubistva na jednom mjestu, a zatim baca tijelo na drugom mjestu u nekom vremenskom razdoblju. Ako je potrebno određeno vremensko razdoblje od destinacije gdje se ubistvo desilo do destinacije gdje je pronađeno tijelo. Na osnovu pretpostavke da se do tog mjesta stiže u tom ili sličnom vremenskom razdoblju i ako se lokacije

poklapaju sa vremenom događaja, dokazi mogu poslužiti kao vjerodostojni. Ali takođe je bitno napomenuti da GPS uređaji nisu savršeni.

7.5. FORENZIKA MEDIJSKIH UREĐAJA

Kao što su: digitalni muzički plejeri, digitalni audio snimači, USB, eksterni HDD. Dokazi sa ovih medija mogu da pruže dosta korisnih podataka, uključujući i one podatke koji su obrisani sa tog uređaja. Kada su priključeni na kompjuter, ovi uređaji ostavljaju trag o sebi, kao što su fajlovi koji su prebačeni, vrijeme i datum kada je taj transfer urađen.

Postoji mnogo načina za pronalaženje podataka evidentiranih na tom uređaju. Npr. na digitalni audio snimač, obrisani audio zapis se može povratiti. Muzički plejer, kao iPod, može se koristiti kao eksterni HDD da se ukradu ili sakriju podaci. Samo zato što ovaj uređaj može biti dizajniran sa namjerom da pušta muziku, na svom osnovnom nivou su i dalje uređaji za skladištenje, sa većinom funkcija istih kao kod normalnog HDD kada je priključen na kompjuter.

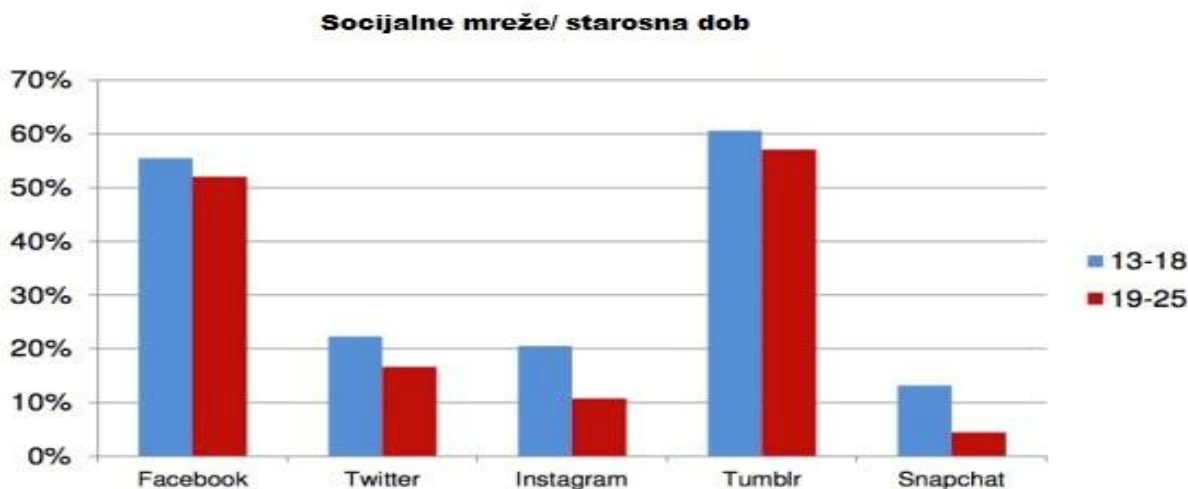
7.6. FORENZIKA DRUŠTVENIH MREŽA

U protekloj deceniji vidjeli smo eksploziju interesa u broju popularnosti društvenih mreža, sajtova i programa. Sajtovi kao što su MySpace, Facebook, Twiter, Google+, LinkedIn su najčešće korištene društvene mreže, te je uobičajno za ljude da imaju više naloga na socijalnim mrežama. Npr. neko bi mogao da ima nalog na Facebook-u da komunicira sa svojim prijateljima, a da ima nalog na LinkedIn-u da održi korak sa svojim poslovnim saradnicima i drugim stručnjacima.

Društvene mreže su željeni način komunikacije za mnoge, prevazišle su čak i komunikaciju putem e-mail-a svojom popularnošću. Ovo naročito važi za mlađe generacije Slika br. 3. , koji u mnogim slučajevima komuniciraju preko društvenih mreža.

Svaka vrsta komunikacije dovodi do mogućnosti dokaza. Popularnost društvenih mreža dovela je do potrebe forenzike društvenih mreža. Ova poddisciplina digitalne forenzike fokusira se na mogućnosti da locira i ispita društvene medije komunikacija na Internetu i da ostavi predmet na HDD ili mobilnom telefonu.

Npr. kada se forenzičko istraživanje vrši na računaru, programi društvenih medija mogu biti instalirani ili podaci sa sajtova kao što su MySpace, Facebook, Google+ mogu se naći[17]. Ova informacija može se koristiti za obavljanje istrage na društvenim mrežama da pronađu aktivnosti na mrežnim komunikacijama koja su načinila lica.



Slika br. 3. Prikaz dijagrama korištenja socijalnih mreža po starosnoj dobi

7.7. TELEFONSKE AUTOMATSKE SEKRETARICE

Pregled i akviziciju podataka s digitalne automatske sekretarice potrebno je pristupiti mikročipu za pohranu podataka, preslušati govorne poruke ili spojiti uređaj s kompjuterom. Današnje su sekretarice zapravo digitalni audio snimači spojeni na telefonsku liniju. Većina ih dolazi s USB portom, kako bi se uređaj mogao spojiti s kompjuterom zbog dohvata ili pohrane važnih poruka. Sekretarice s USB priključcima smatraju samo još jednim medijem za pohranu podataka. Korisnici veoma jednostavno dokumente, podatke slike te ostale informacije mogu sakriti upravo na digitalnu automatsku sekretaricu. Pregled, akvizicija i analiza podataka obavljaju se kao i kod bilo kojeg medija za pohranu podataka.

7.8. DIGITALNA FORENZIKA SLIKA

Digitalne slike nastale upotrebom raznih uređaja koriste se u sve većem broju područja od vojnih i nadzornih do medicinskih dijagnoza te komercijalne upotrebe i privatne fotografije. Skladno tome, niz novih forenzičkih problema proizlazi iz tako ubrzanog rasta napretka i

raširenosti uređaja koji mogu generisati digitalnu sliku. Npr., možemo se zapitati kakvi se tipovi sklopovskih i programskih komponenti koriste u tim uređajima. Analizom digitalne fotografije utvrđujemo korišteni senzor. Kako je dobijena slika? Je li nastala u mobilnom telefonu, kameri, video kameri, fotografskim skenerom ili je stvorena umjetno korištenjem softvera za obradu fotografija? Je li slika manipulirana nakon stvaranja, je li autentična ili modificirana na neki način? Sadrži li sakrivene podatke ili steganografski sakrivene informacije? Mnoga se forenzička pitanja mogu odgovoriti pronalaskom mjesta nastanka digitalne fotografije ili njenog procesa stvaranja. Znanje o metodama akvizicije slika mogu pomoći pri odgovaranju na buduća forenzička pitanja koja se tiču prirode dodatnog procesiranja kojima je slika mogla biti podvrgnuta nakon nastanka.

7.9. FORENZIKA DIGITALNIH KAMERA

Digitalni fotoaparati i kamere u današnje se vrijeme zapravo svode na isti uređaj. Prilikom njihovog pregleda najbitnije je naravno područje za skladištenje fotografija i snimaka. Iako je broj proizvođača digitalnih fotoaparata i kamera sve veći, način komunikacije opreme većinom je standardizovan. Većina digitalnih kamera koristi standardni ili mini USB priključak za spajanje s kompjuterom, te standardne memorijske kartice kao što su MiniSD ili CompactFlash, za proširenje kapaciteta skladištenja. Većina trenutno dostupnih sistema prilikom istrage tretira se kao samo još jednu jedincu za skladištenje podataka olakšavajući time posao istražiocima, jer je moguće korištenje standardnih metoda i alata za digitalnu forenziku. Ako se analize i istrage izvode preko USB porta, potrebno je omogućiti opciju zabrane pisanja po mediju, kako se prilikom analize podaci ne bi slučajno modifikovali. Isto pravilo vrijedi i za čitanje ili prenos podataka s memorijskih kartica.

Kao i kod digitalnih kamera, većina digitalnih audio uređaja kao što su MP3 plejeri ili iPod-ovi, tretira se kao medij za skladištenje podataka te se shodno tome i obrađuje forenzičkim alatima.

7.10. FORENZIKA DIGITALNOG AUDIO DOKAZA

Digitalni Audio dokazi čine unapređenje i analizu audio zapisa kreiranih sa bilo kojim tipom digitalnog uređaja za snimanje. Audio dokazi mogu da se koriste za provjeru integriteta audio zapisa ili da se pokaže da je audio snimak neovlašćen. Ako je snimak lošeg kvaliteta, te se takođe može koristiti da se poboljša kvalitet audio snimka, tako da glasovi postaju vidljiviji ili da smanji ili pojača pozadinsku buku koja je od interesa da se lakše čuje.

Takođe je moguće da se izvrši prepoznavanje glasa, obrazac sa specijalizovanim forenzičkim softverom. Ovi programi omogućavaju moguću identifikaciju glasova sa određenim ljudima u vidu audio zapisa.

Drugi metod za prepoznavanje glasa je priručnik za ispitivanje spektrografa. Spektrograf je vizuelna predstava slušnih podataka. Baš kao što se nota koristi da objasni kako treba da se vrši pjesma pomoću muzičke note i koliko dugo treba da bude pjesma, spektrograf predstavlja različite zvučne talase tokom vremena na učestalosti i intenzitetu.

7.11. FORENZIKA MULTIPLEJER IGRICA

Najpopularniji oblik igara danas su multiplejer igrice, posebno masivno multiplejer onlajn igranje (MMORPG igrama). Postoje desetine miliona ljudi koji igraju MMORPG igre. Ove igre se obično sastoje od lica koje stvaraju lik, sa kojim zatim istražuju u online svetu, na višem nivou stvaraju klanove koje čine drugi ljudi koji se pretplate na igru. To nije neobično za ljude da igraju online igre do čak 60 sati nedeljno. Videli smo slučajeve gde su ljudi igrali MMORPG više od 100 dana u toku jedne godine. 100 dana nije život lika iz igre, to je, u stvari, stvarna količina vremena koje čovek sedi ispred kompjutera, prijavljen u svom liku iz igre i igrajući igru. Stvarni iznos koji je proveo igrajući neku igru može se prikazati u samoj igri kucanjem određenih komandi u interfejsu[17].

Ove igre prate mnogo informacija o ljudima koji ih igraju. Programi čuvaju podatke o svakoj sesiji u igri i dužinu te sesije i čet logove likova povezanih sa nalogom.

Ovi zapisi kreirani od igrača mogu da se koriste za izradu vremenskog okvira, da uspostave alibi i da pronađu u četovima igara neke poruke potrebne da bi se iskoristile kao dokaz.

7.12. FORENZIKA KONZOLA ZA IGRE

Konzolne igre danas kao Xbox, Nintendo Wii, Sony PlayStation su svi u osnovi računari: oni sadrže hard disk isto kao i računar, a funkcionišu na operativnim sistemima, baš kao kompjuter.

Budući da su u osnovi računari, oni skladište informacije na sličan način. Mnogi ljudi koriste svoj igrački sistem da pretražuju Internet i gledaju filmove, a ne samo za igranje igara. Ove informacije se čuvaju na hard disku unutar u igračkoj konzoli. To znači da podaci mogu da se povrate, uključujući izbrisane informacije iz igrajuće konzole.

Da igra igre na mreži pomoću konzole, osoba mora da kreira online nalog. Sa Xbox-om, npr., osoba mora da se pretplati na Xbox Live. Na taj način kreira informacije koje se mogu koristiti kao dokazi, jer ta osoba sada ima i online identitet, a dijelovi tih informacija se čuvaju na igračkoj konzoli.

Konzola i kompjuter se mogu koristiti kao dokaz u vezi. Sa nekim igrama postoji opcija da vam se pošalje e-mail i detaljni učinak na meču. Npr., Madden fudbalske igre, možete da imate e-mail poruku po završetku utakmice sa detaljima vaše utakmice i performansama utakmice.

Informacije ovako mogu izgledati beznačajno, ali može da se koristi kao dokaz u svom igračkom sistemu kreiranjem datuma i vremena kada je igrač bio aktivan, a samim tim uspostaviti alibi.

8. ANDROID PLATFORMA

Android je operativni sistem za mobilne uređaje zasnovan na Linuxu koji razvija druženje Open Handset Alliance (OHA) na čijem čelu se nalazi kompanija Google.

Prvobitnog razvijачa, istoimenu kompaniju, otkupio je Google 2005. godine. Prvobitno predstavljanje distribucije Android je najavljeno zajedno sa osnivanjem Open Handset Alliance (OHA), konzorcijuma od 86 kompanija koje se bave hardverom, softverom i telekomunikacijama, a koji je posvećen unapređivanju otvorenih standarda za mobilne uređaje. Android je zasnovan na izmenjenoj verziji Linux jezgra. Po broju prodatih pametnih telefona, zasnovanih na „android“ OS u SAD, u drugom kvartalu 2010.godine, android se nalazi na prvom mestu sa udjelom od 33 procenta.

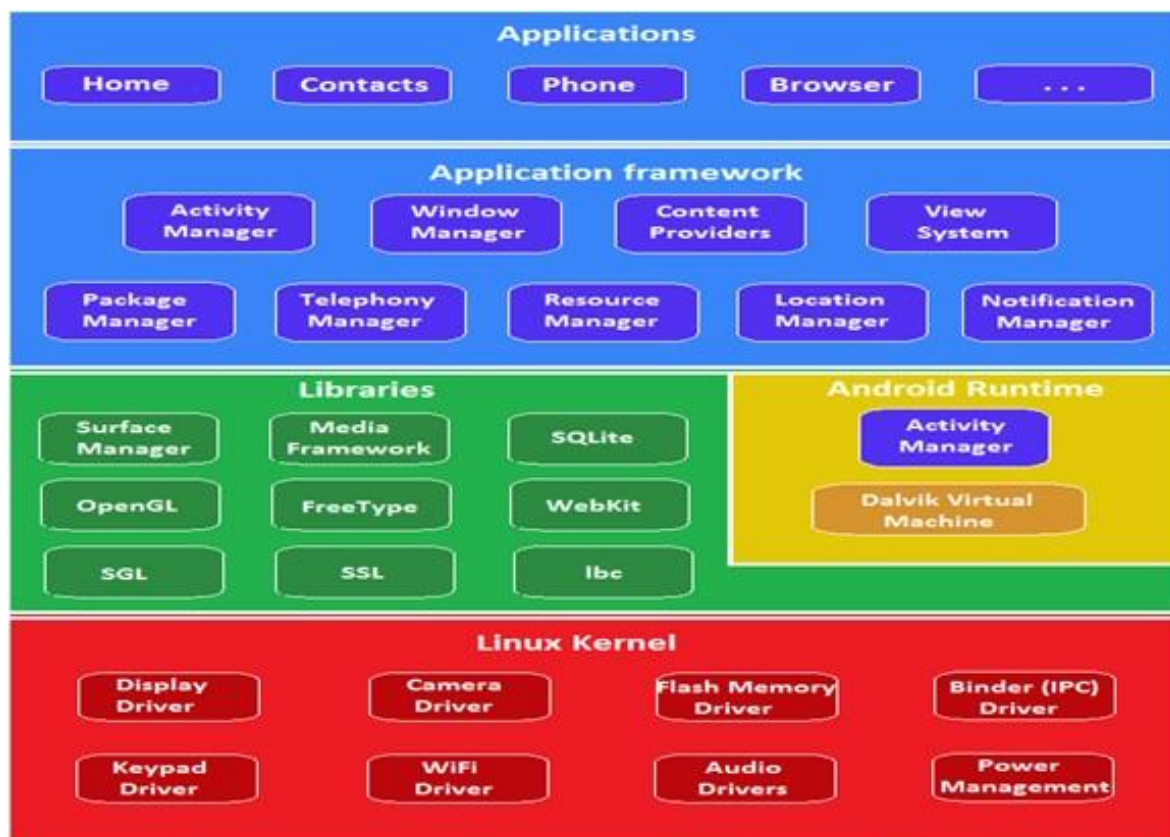
Android ima veliku zajednicu programera za pisanje aplikativnih programa koji proširuju funkcionalnost uređaja. Trenutno postoji preko 250.000 aplikacija dostupnih za android. Programeri pišu kontrolisani kod u Java jeziku, kontrolišući uređaj preko Google razvojne Java biblioteke.

Početak android distribucije najavljen je 5. novembra 2007. godine zajedno sa osnivanjem Open Handset Alliance, udruženja 78 kompanija posvećene unapređenju otvorenih standarda za mobilne uređaje. Google je veći dio android koda objavio pod Apache licencom, licencom slobodnog softvera i licencom otvorenog koda.

Android OS se sastoji od 12 miliona linija koda; uključujući 3 miliona linija XML koda; 2,8 miliona linija C koda; 2,1 miliona linija Java koda i 1,75 miliona linija C++ koda.

Aplikativno okruženje (application framework) obezbeđuje interfejs pomoću kojeg programeri aplikacija mogu koristiti razne biblioteke integrisane u Android kao i mnoge funkcionalnosti koje su takođe već razvijene i ugrađene u vidu nekih standardnih funkcija[21]:

- Activity manager – upravlja životnim ciklusom aktivnosti.
- Telephony manager – obezbeđuje pristup telefonskim uslugama i vezanim informacijama kao što su brojevi telefona.
- View system – rad sa elementima koji čine korisnički interfejs.
- Location manager – daje trenutnu geografsku lokaciju uređaja.



Slika br. 4. Aplikativno okruženje.

8.1. ISTORIJA ANDROIDA

Android Inc. su osnovali Andy Rubin, Rich Miner, Nick Sears i Chris White u Oktobru 2003. godine kako bi razvijali programe za pametne mobilne uređaje koji bi uzimali u obzir korisnička podešavanja te njegovu lokaciju. Nakon dvije godine gotovo tajnog rada (jedino što je bilo poznato bilo je da se radi o softveru za mobilne), Google je odlučio kupiti Android te počinju spekulacije o ulasku Google-a na tržište pametnih telefona. Osnivači i ključni programeri, osnaženi Google-ovim programerima, na tržište donose mobilnu platformu temeljenu na linux-ovom kernelu koja bi trebala biti potpuno prilagodljiva zahtjevima korisnika.

U Novembru 2007. godine osnovana je Open Handset Alliance (OHA) s ciljem stvaranja javnog standarda za mobilne uređaje. Glavni inicijator i ovoga puta bio je Google koji je okupio 34 kompanije iz različitih domena mobilne industrije poput proizvođača mobilnih telefona, programera aplikacija, mobilnih operatera i sličnih.

Istoga dana, 5. Novembra 2007. godine, OHA otkriva mobilnu platformu otvorenog koda baziranu na Linux kernelu – Android. Ovo je prvo javno predstavljanje Androida kao operativnog sistema, a prvi komercijalni uređaj u koji je bio ugrađen Android OS bio je T-Mobile G1, tajvanskog proizvođača pametnih telefona HTC (poznat i pod nazivom HTC Dream). Osnivanjem ovog saveza, Android je bačen u trku sa ostalim mobilnim platformama na

tržištu: iOS (Apple), Windows Phone (Microsoft), Symbian (Nokia, Sony Ericsson), Palm (HP), Bada (Samsung)[21].

Od samih početaka Android je zamišljen kao projekt otvorenog koda (open source project) te je od 21. Oktobra 2008. godine dostupan cjeloviti kod pod Apache licencom. S druge strane, proizvođačima uređaja nije dozvoljeno korištenje Android zaštićenog imena ukoliko Google ne sertifikuje uređaj kao kompatibilan prema Compatibility Definition Document (CDD). Takođe, uređaji moraju zadovoljavati kriterijume iz ovog dokumenta kako bi dobili pristup aplikacijama zatvorenog koda poput Android Market aplikacije. Ona služi za pretraživanje i instalaciju aplikacija koje su na tržištu, a ne dolaze ugrađene u sami uređaj. Jedini izuzetak od politike otvorenog koda jesu verzije 3.0, 3.1 i 3.2 kodnog imena (Honeycomb) kako ne bi došlo do instaliranja istih na mobilni uređaj, iz razloga što je ta verzija namjenjena upotrebi na tablet računarima. Kod verzija 3.x će biti dostupan nakon izlaska verzije Ice Cream Sandwich koja će biti mješavina trenutne verzije za mobilne uređaje (2.3 – Gingerbread) i Honeycomb verzije.

Trenutna verzija Android platforme je Jelly Bean Android 4.2.

8.1.1. Jelly Bean

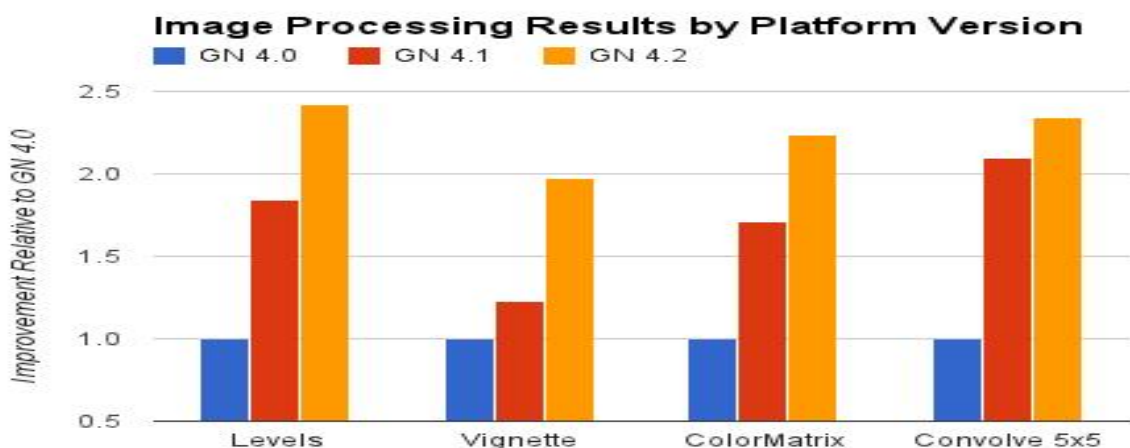
Android 4.2. ima poboljšane i optimizovane performanse, osvježeni UI sistem i bolju budućnost za korisnike i developere.

Svako Android izdanje uključuje desetine bezbjednosnih poboljšanja u cilju zaštite korisnika.

Evo nekih od poboljšanja na Androidu 4.2. Jelly Bean[27]:

- Aplikacija za verifikaciju – Korisniku mogu da biraju da li će da aktiviraju aplikaciju za verifikaciju i da imaju prikaz aplikacije za verifikaciju kada instaliraju aplikacije, prije instalacije aplikacija za verifikaciju prikaže upozorenje da aplikacija može biti štetna, ako je aplikacija loša on može da blokira instalaciju.
- Veća kontrola premium SMS – Android će vas obavjestiti ako aplikacija pokuša da pošalje SMS na kratki broj koji koristi premium usluge koje mogu izazvati dodatne troškove. Korisnik može da izabere da li da dozvoli aplikaciji da blokira stanje ili da dopusti slanje istog SMS-a.

- Uvijek na VPN-u – VPN se može konfigurirati da aplikacija ne dozvoli pristup mreži dok se ne obezbijedi VPN konekcija. Ovo sprečava slanje podatka kroz druge mreže.
- Poboljšanje prikaza permisa – Permise ili dozvole su organizovane u grupe koje su uređene radi lakšeg shvatanja korisnika. Tokom pregleda dozvola, korisnik može da klikne na permisu da vidi više detalja o permisama i da ih mjenja po potrebi.
- Bezbjedonosne ispravke – Unaprijeđen open source biblioteke sa poboljšanjima sigurnosti koje uključuju WebKit, libpng, OpenSSL i LibXML. Android 4.2 takođe uključuje ispravke za određene slabosti Androida. Informacije o ovim ranjivostima će biti proslijeđene Open Handset Alliance članovima i ispravke će biti dostupne u Android Open Source Projektu.



Slika br. 5. Renderovanje procesa slike, reperi pokrenuti na različitim Android platformama (Galaxy Nexus telefon)[27].

8.2. DIGITALNA FORENZIKA ANDROIDA

Postoji potreba za Android forenzikom. Pametni telefoni globalno najviše imaju digitalnih informacija o individualnoj osobi. Za većinu ljudi njihov smartfon je na nekoliko meta od njih čak i kada spavaju. Što znači da na osnovu pametnog telefona veoma je lako doći do informacija o kretanju korisnika. Uređaj kombinuje lične i korporativne informacije i ima mogućnost za skladištenje ogromne količine podataka, uključujući tekstualne poruke, e-mail poruke,

informacije socijalnih mreža, GPS lokacije, slike, video itd. Ljudi imaju tendenciju da budu iskreni prema pametnim telefonima od bilo koje druge osobe ili uređaja. Zašto ? Zato što ljudi osjećaju da je uređaj bezbjedan i mogu da im daju odgovore o mnogim informacijama i da ih ne podjele sa drugima. Više od jednog primjera pokazalo je, “vi ste ono što Googlate” jasno se vidi iz prve ruke nusprodukt iskrenosti sa kojom ljudi koristite pametne telefone.

8.2.1. Izazovi

Mobilna forenzika i Android forenzika posebno imaju niz izazova koji se moraju prevazići.

Fundamentalni cilj digitalne forenzike je da predstavi modifikaciju cilja uređaja - ispitivač. Međutim mobilni telefoni imaju tradicionalni nedostatak hard diskova koji mogu biti ugašeni, povezan sa blokerom upisivanja i sliku u forenzičkom zvučnom načinu. Svaka ireracija sa pametnim telefonima će napraviti promjenu na neki način. Kao takve, ispitivači moraju koristiti svoj sud kada razmatraju mobilni uređaj i da li je uređaj modifikovan, ispitivači moraju da objasne kako je modifikovan i žasto je taj izbor napravljen. Neki ispitivači forenzike izuzimaju ovaj pristup debate.

Međutim, tehnike koje mogu da upozore o kompjuterskom cilju za forenzičko ispitivanje bile su korištene ponekad. Npr., ponudite pretragu memorije koja je neophodna za istragu napada malvera. Slično tome, ako je hard disk šifrovan, ispitivač mora napraviti imidž uređaja, ali postoji rizik da neće imati pristup podacima na disku. Ostali dobri primjeri su sistemi koji moraju ostati na mreži, zbog složenih okruženja, obično se nalaze u slučajevima koji uključuju veće korporativne servere. Svaki istraživač treba da teži da ne promjeni uređaj koji se istražuje, a to je rijetko moguće u mobilnom svijetu. Dakle, ukoliko uređaj ne može da bude modifikovan, onda bi jedini drugi izbor bio da se ne ispita uređaj. Jasno je da ova opcija nije prihvatljiva za dokaz iz mobilne forenzike, jer je kritična komponenta u mnogim ispitivanjima i čak je riješio mnoge slučajeve zločina.

Dodatna komplikacija Android forenzike je raznovrsnost uređaja, Android verzija i aplikacija. U permutacijama uređaja i Android verzija samo su hiljade pojedinih uređaja plus jedinstvene karakteristike platforme. Dok je logična analiza Android telefona dostižna, poslednje kombinacije čine punu fizičku akviziciju svakog Android uređaja vjerovatno neostvarivom, čak male razlike u Android verziji mogu da zahtjevaju obimna testiranja i validaciju u slučajevima visokih uloga.

8.3. ANDROID HARDVER PLATFORMA

Android je dizajniran da bude kompatibilan sa mnoštvom hardvera. Ovo se postiže u velikoj mjeri kroz Linux kernel, koji je tokom godina evoluirao da podržava sve veći broj hardvera.

Ovo je važna karakteristika platforme koja dopušta proizvođačima slobodu dizajna, nabavku ili da na drugi način integrišu idealne komponente na Android uređaju. Ova strategija je dovela do

razvoja moćnih dual-core i quad-core procesora za Android uređaje, tako da su ovi uređaji u mogućnosti da obrade značajne zahtjeve. Iako je hardverska kompatibilnost odlična za proizvođače bežičnih uređaja i ne kraju potrošače, raznolikost predstavlja izazov za forenzičke analitičare i inženjere bezbjednosti. Razumjevanjem hardverskih komponenti, uređaja i pokretanja procesa za Android će vam pomoći u vašem ukupnom razumjevanju Androida.

8.3.1. Centralna procesorska jedinica (CPU)

Centralna procesorska jedinica je termin prilično poznat većini forenzičkih analitičara i nema iznenađenja u svojoj ulozi na Android uređajima. CPU je odgovoran za izvršavanje operativnog sistema i aplikativnog koda i koordinaciju ili kontrolu drugih komponenti, uključujući mreže, skladištenje, prikaze i ulazne uređaje.

U početku većina, ali ne bas svi Android uređaji su koristili ARM procesore kao svoj CPU, koji je bio moćan dovoljno za mobilne platforme ali je dizajniran za malu potrošnju energije.

Međutim, korporacije i entuzijasti su Android preveli na druge platforme. Na korporativnom planu, Intel je ponudio Androidu svoj atom procesor. Slično tome, Google je podržao Android u svom Google TV proizvodu. To su projekti kao što su Android x86 koji su pušteni u verziji Androida pokrenutih na Intelovoj x86 arhitekturi[21].

8.3.2. Ekran

Android uređaji imaju ekran osjetljiv na dodir koji otvara puno mogućnosti za dizajniranje korisničkog interefejsa. Hardverski dugmići se više ne koriste već se interfejs može napraviti sa bilo kojim oblikom i rasporedom kontrola na ekranu. Korisnici mogu da dodirrom selektuju i prevlače objekte na ekranu, a pošto Android podržava i multitouch moguće je koristiti i kombinacije kada više prstiju istovremeno dodiruje ekran kao što je "štipanje" ekrana za zumiranje[16].

Interfejs sa ekranom osjetljivim na dodir je znatno napredniji i privlačniji korisnicima i čini veoma važnu stavku u svetu pametnih telefona pa i Android uređaja doprinoseći značajno njihovoj popularnosti.

8.3.3. Ram memorija (Random access memory i NAND fleš memorija)

Android uređaji su na nekom nivou prosto računari, potrebne su im razne vrste memorije da rade. Dve osnovne vrste memorije su promenljiva (Radna memorija [RAM]) i trajna (NAND flash) memorija.

RAM je korišten kao sistem za učitavanje, izvršavanje i manipulisanje ključnih dijelova OS-a, aplikacija ili podataka. RAM je nestabilan, što znači da on ne čuva svoj sadržaj bez struje. Međutim, NAND fleš memorija (što će se odnositi na ovu memoriju jednostavno kao NAND flash) je trajna i na taj način, podaci su sačuvani nakon isključenog napajanja uređaja. NAND fleš se koristi za skladištenje pokretačkih procesa, OS i podataka korisnika. Zbog toga je kritična komponenta svake forenzičke istrage i liči na hard disk u forenzičkoj istrazi laptopa, desktopa ili servera. NAND fleš ima jedinstvene osobine koje ga čine idealnim za mobilne uređaje, a istovremeno predstavlja brojne izazove za programere (što često daje jedinstvenu priliku za forenzičke analitičare)[21].

Sa stanovišta hardvera, mobilni uređaji očigledno imaju značajan prostor ograničenja. Često, RAM i NAND fleš memorija se proizvode kao jednostavna komponenta nazvana Multichip paket (MCP). Prilikom ispitivanja Android uređajnih komponenti, uglavnom NAND fleš i RAM-a će se ispitivati kao MCP.

Iako je specifičan za proizvođača Hynix memorije (koriste Dell Streak i ostali Android uređaji), ova ukupna arhitektura je dobar prikaz MCP komponenti koje obuhvataju ne samo NAND fleš i RAM, ali i upakovane opcije tako da odgovaraju različitim uređajima.

8.3.4. GPS

Svi Android telefoni imaju ugrađene GPS prijemnike pomoću kojih je uvijek dostupna lokacija korisnika. Navigacija i korištenje mapa postaje dostupno u svakom trenutku i veoma je pogodno za putovanja, a i mnoge druge aplikacije koriste GPS kao što su social networking aplikacije. Jedna od takvih aplikacija je Foursquare kojom možete svoju trenutnu lokaciju da podelite sa prijateljima, možete videti gde se trenutno nalaze vaši prijatelji i koja javna mesta možete posetiti koja su u blizini.

Za posećena mesta se mogu ostaviti komentari, preporuke ostalim prijateljima, fotografije, a i moguće je povezati aplikaciju sa Facebook-om i Twitter-om kako bi se automatski trenutna lokacija korisnika prosleđivala i tamo, što mnogo znači forenzičarima u njihovim istragama[16].

8.3.5. SD memorijske kartice

takođe SD standard podržavaju i mnogi drugi uređaji kao što su kompjuteri, fotoaparati i telefoni drugih operativnih sistema. Aplikacije mogu pristupati fajlovima sa SD kartice ili mogu da čuvaju svoje podatke na njoj. Upotreba portabilne memorije dolazi do izražaja pri korištenju bilo kojih aplikacija za rad sa audio i video fajlovima, fotografijama, tekstualnim dokumentima. Aplikacije uz pomoć kojih možemo da generišemo fajlove takođe moraju da te fajlove negde sačuvaju i tada se najčešće za to koristi SD kartica.

8.3.6. Bluetooth

Android uređaji posjeduju Bluetooth primopredajnik koji omogućava bežičnu razmjenu informacija sa drugim Bluetooth uređajima. Najčešće se koristi za prenos fajlova sa jednog uređaja na drugi i za to se može iskoristiti aplikacija Bluetooth File Transfer koja pruža dobru organizaciju prenosa podataka.

Veza sa drugim uređajem se može uspostaviti samo ukoliko to potvrde obje strane i na ovaj način se pruža neki vid sigurnosti. Kod prenosa fajlova je bitan pregled i pretraga fajlova radi lakšeg obavljanja transfera i ovde je to dobro riješeno. Moguće je prilagoditi interfejs po svojoj želji, mogu se pretraživati arhive fajlova, mogu se slati kontakti sa brojem i ostalim informacijama.

Još jedna česta upotreba Bluetooth-a je za hands free razgovore najčešće pri vožnji automobila. U ovom slučaju Bluetooth se koristi za prenos zvučnih talasa od telefona do bežičnih slušalica i tako omogućava razgovaranje telefonom bez upotrebe ruku koje mogu da ostanu na volanu[8].

Primer aplikacije koja ima ovu funkciju je Auto Bluetooth koja pri dolazećem pozivu aktivira Bluetooth i spaja se sa bežičnim slušalicama na koje prenosi zvuk. Takođe po završetku razgovora automatski gasi Bluetooth i tako štedi bateriju.

8.3.7. Kamera

U početku, kamere na smart telefonima su korištene za fotografisanje. Iako je uzbudljiv razvoj u to vrijeme, takođe je došlo do značajne inovacije u ovoj oblasti. Većina uređaja sada takođe podržava snimanje videa (neki u visokoj definiciji HD). Naravno, na kamerama su povećali njihov kvalitet, a sada često uključuju integrisani blic.

Od nedavno, neki uređaji sadrže dve kamere. Prva, na zadnjoj strani uređaja, se koristi za spoljne slike i video zapise. Druga, prednja kamera omogućava nove aplikacije kao što su video konferencije.

Većina Android uređaja takođe kombinuje funkcionalnost kamere sa GPS uređajem, stoga možete snimiti ne samo datum i vrijeme slike nego i GPS koordinate. Tada možete lako uploadovati ili podijeliti sliku koristeći internet ili možda da ih pošaljete kroz servis razmjene multimedijalnih poruka (MMS) mobilnog provajdera.

Interesantan razvoj u ovoj oblasti je upotreba kamera za čitanje bar kodova. Specijalizovane aplikacije iskoriste kameru da slikaju bar kod, a zatim analiziraju podatke. To može pregledati proizvode i odrediti najbolju cijenu.

Možda u budućnosti, čak i ove aplikacije omoguće vam da platite za stavke koje želite da kupite.

Rana primjena ove aplikacije je Google aplikacija nazvana Googles. Korisnik može da uzme sliku bilo čega, a aplikacija pokušava da identifikuje objekat. Zanimljiv primjer, pruža Google, npr. turista koji koristi aplikaciju za identifikaciju znamenitosti koju je posjetio.

8.3.8. USB

Većina Android uređaja podržavaju nekoliko Universal Serial Bus (USB) interfejsa kojima se može pristupiti sa računara. Kablovi mogu da se razlikuju od uređaja, ali uopšte, USB interfejs omogućava najmoderniju OSs vezu sa uređajem.

Slijede neki uobičajeni interfejsi izloženi od Android uređaja[21]:

1. Punjenje: uređaji mogu da se pune preko USB kablova

2. Disk interfejs: delovi uređaja, uključujući i SD kartice, imitirane SD kartice i drugi disk interfejsi, predstavljeni su i pristupačni operativnom sistemu kao Masovni Skladišteni Uređaji.
3. Prodavači specifičnih interfejsa: uključuju namjenski sinhronizovane protokole, imitaciju CD-memorija samo za čitanje (ROM) uređaja za softverske instalacije i specijalizovane veze za dijeljenje Internet veze telefona.
4. Android Debug Bridge (ADB): interfejs koji omogućava korisnicima pristup shell prompt na uređaju, kao i druge napredne funkcije.

8.3.9. Zvučnik / Mikrofon

Konačno, smart telefon ili tablet nije toliko interesantan bez sposobnosti da čuje ili proizvodi zvuk. Kao i ostale komponente, zvučnik i mikrofon i dalje dopijevaju u svakoj iteraciji.

Npr., neki Android uređaji sadrže dva ili tri mikrofona koji u kombinaciji sa Android softverom, imaju sposobnost da detektuju i poništavaju buku iz pozadine da bi se obezbijedio bolji kvalitet zvuka.

Neki od najljepših tehnoloških razvoja ove decenije, je govorni telefoni koji su se razvili do tačke gdje se oni zapravo mogu koristiti u stvarnom razgovoru!

8.4. ANDROID FAJL SISTEM I STRUKTURA PODATAKA

Dok su osnovni hardver i softver pokrenuti Android uređajem, primarni fokus forenzičkih analitičara i bezbjedonosnih inženjera je da dobiju, analiziraju, razumiju i uskladište podatke na uređaju. Kao i u drugim temama gdje ima mnogo nijansi koje su važne za razumjevanje i efikasnu analizu uključujući vrste podataka za skladištenje, gdje se oni nalaze, kako se čuvaju i karakteristike fizičkih medija gdje se oni čuvaju. Svi ovi faktori imaju važnu ulogu radi toga da se ustanovi koji podaci mogu biti vraćeni i kako oni mogu biti analizirani.

Forenzička analiza je primarno koncentrisana na podatke predmeta koji mogu biti povraćeni iz uređaja koji se istražuje. Android je u kombinaciji sa oba poznata predmeta, kao što su oni koji se nalaze u Linux-u i potpuno novih, kao što je Dalvik VM i YAFFS2 fajl sistem. Dodavanje složene i varirajuće arhitekture koje su različiti proizvođači prihvatili. Iako ni jedna knjiga niti ispitivač ne bi mogli pokriti ovu temu iscrpno, postoje određeni osnovni pojmovi Android uređaja. Sistem datoteke, fajlovi i drugi predmeti koji su u srži onoga što forenzički analitičari moraju da shvate o Androidu, kako bi se povećala njihova efikasnost istrage.

8.4.1. Koji podaci su skladišteni

Android uređaji skladište ogromne količine podataka, obično kombinujući lične i poslovne podatke. Aplikacije su primarni izvor ovih podataka, a tu su i brojni izvori za uključene aplikacije[21] :

- Aplikacije koje se isporučuju sa Androidom
- Aplikacije instalirane od strane proizvođača
- Aplikacije instalirane od bežičnog operatera
- Dodatne Google / Android aplikacije
- Aplikacije instalirane od strane korisnika, obično sa Android Marketa

Uzroci podataka se nalaze na Android uređajima uključujući sledeće :

- Tekstualne poruke (SMS – MMS)
- Kontakti
- Logovi poziva
- E- mail poruke
- Instant mesendžeri i čatovi
- GPS koordinate
- Slike i Video
- Web istorija
- Istorija pretraživanja

- Uputstva za vožnju
- Facebook, Twiter i druge socijalne mreže
- Fajlovi sačuvani na uređaju
- Muzičke kolekcije
- Kalendar
- Finansijske informacije
- Istorija kupovine
- Dijeljenje fajlova

8.4.2. Kako su podaci sačuvani

Android omogućava sa pet metoda skladištenje podataka na uređaju, sudski ispitivači mogu otkriti podatke u najmanje četiri od pet formata, dakle, to je važno da razumijemo u detalje. Podaci se čuvaju ili na NAND fleš memoriji ili na SD kartici ili na mreži. Pet metoda je[21] :

1. Dijeljena podešavanja
2. Interna memorija
3. Eksterna memorija
4. SQLite
5. Mreža

Pored podataka koji programerima aplikacija stižu iz Android marketa, Linux kernel i Android stek pružaju informacije putem logova, otklanjanja grešaka i drugim standardnim inforamtivnim servisima.

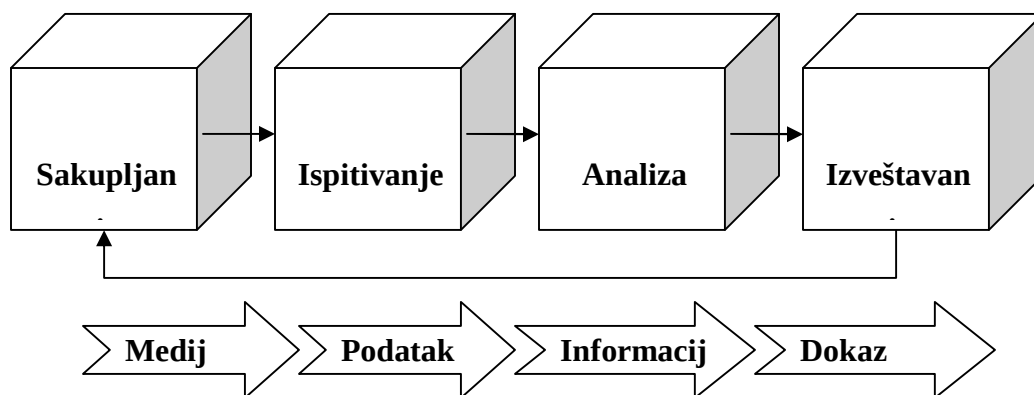
9. STUDJA SLUČAJA

9.1. Digitalno forenzička istraga telefona

U ovoj studiji slučaja prikazaćemo digitalno forenzičku istragu izvršenu nad uređajem (Mobilni telefon, SonyEricsson Xperia X8, Android OS 2.1). Ovaj telefon je u vlasništvu osumnjičenog za malverzaciju baze podataka sa servera korporacije Asteroid softver. Osumnjičeni je zaposlen u ovoj korporaciji kao radnik komercijalne službe. Osumnjičeni se od ranije dovodi u sumnju da je nepodoban za firmu. Osumnjičeni je otkriven pomoću sigurnosnih kamera, koje se nalaze u serverskoj sali, te kako spaja svoj telefon sa serverom i nakon toga obavlja razgovor.

Po uočenom snimku na sigurnosnim kamerama došlo je obezbjeđenje u server salu i pretreslo osumnjičenog, kod kojeg su našli navedeni telefon marke SonyEricsson Xperia X8. Nakon pretresa zaplijenili su mu mobilni telefon. Pripadnici obezbjeđenja su odmah obavjestili rukovodioca obezbjeđenja kome su dali uređaj. Rukovodioc obezbjeđenja je pozvao tim forenzičara za digitalnu forenziku kojima je predao uređaj radi ispitivanja.

Proces digitalne forenzike obuhvata četiri glavne faze, sakupljanje (akvizicija), ispitivanje, analiza i izveštavanje (slika br. 6.).



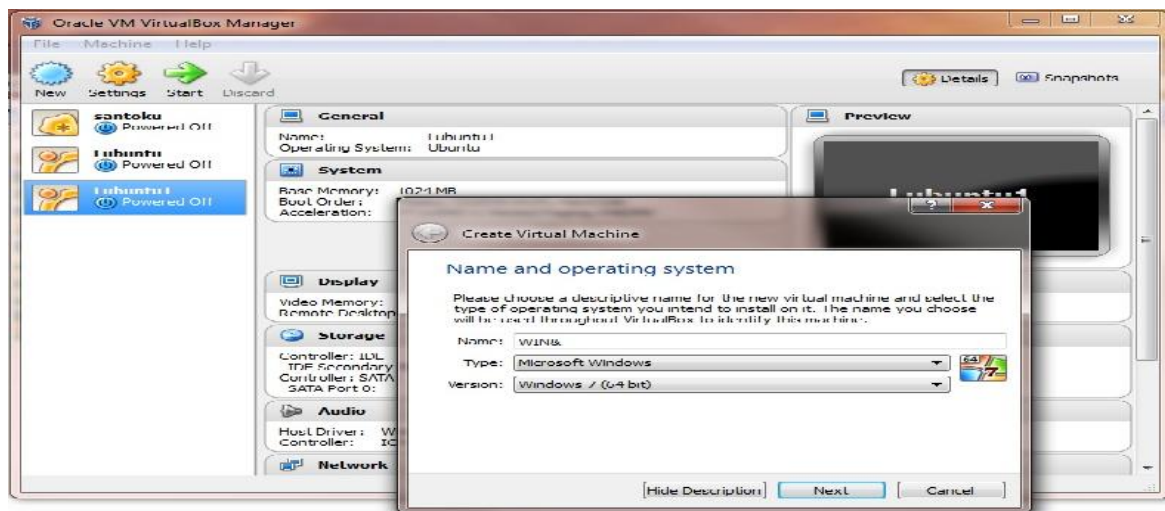
Slika br.6.Proces digitalne forenzike

Tim forenzičara sljedeći propisane procedure i principe zaplijenjen uređaj prebacio u laboratoriju radi ispitivanja i analiza. U ovom ispitivanju tim forenzičara odlučuje da će koristiti određene alate :

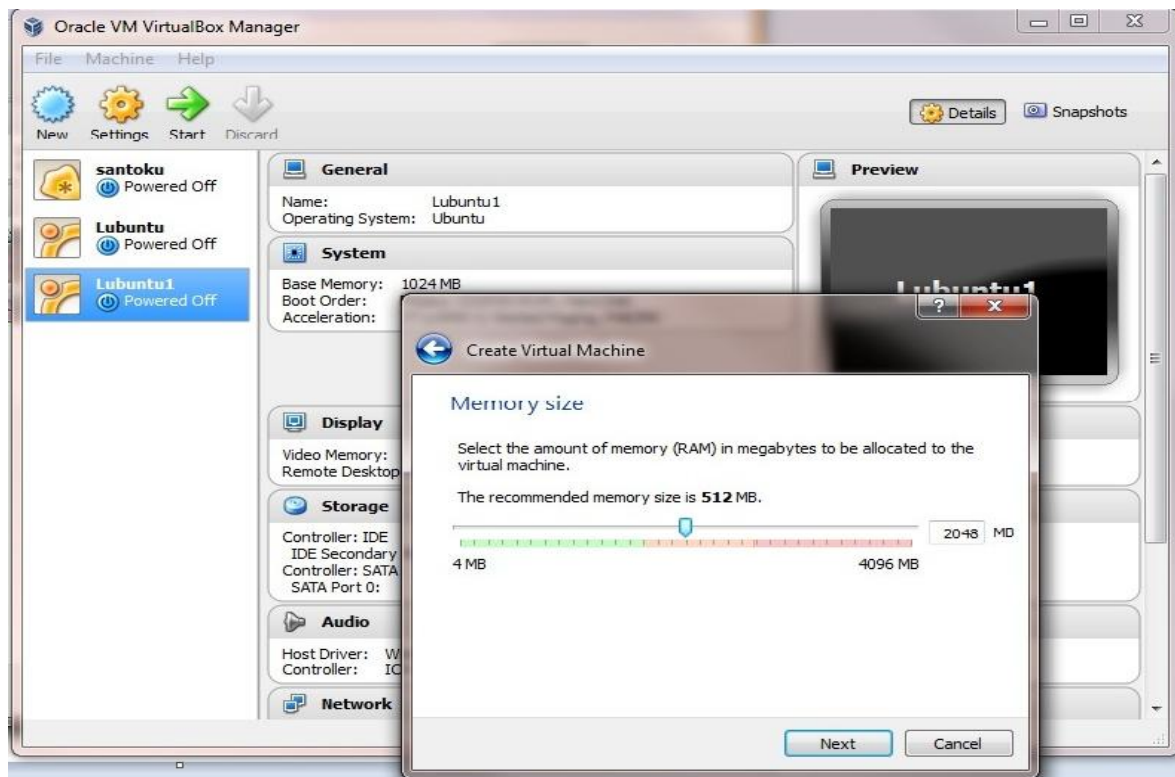
- Virtelnu mašinu Oracle VM VirtualBox– radi sigurnosti istrage
- Mobiledit- radi uvida u pozive, SMS poruke i kontakte
- EnCase - radi pronalaženja mogućih kompromitovanih fajlova sa servera

9.2. Instalacija virtuelne mašine

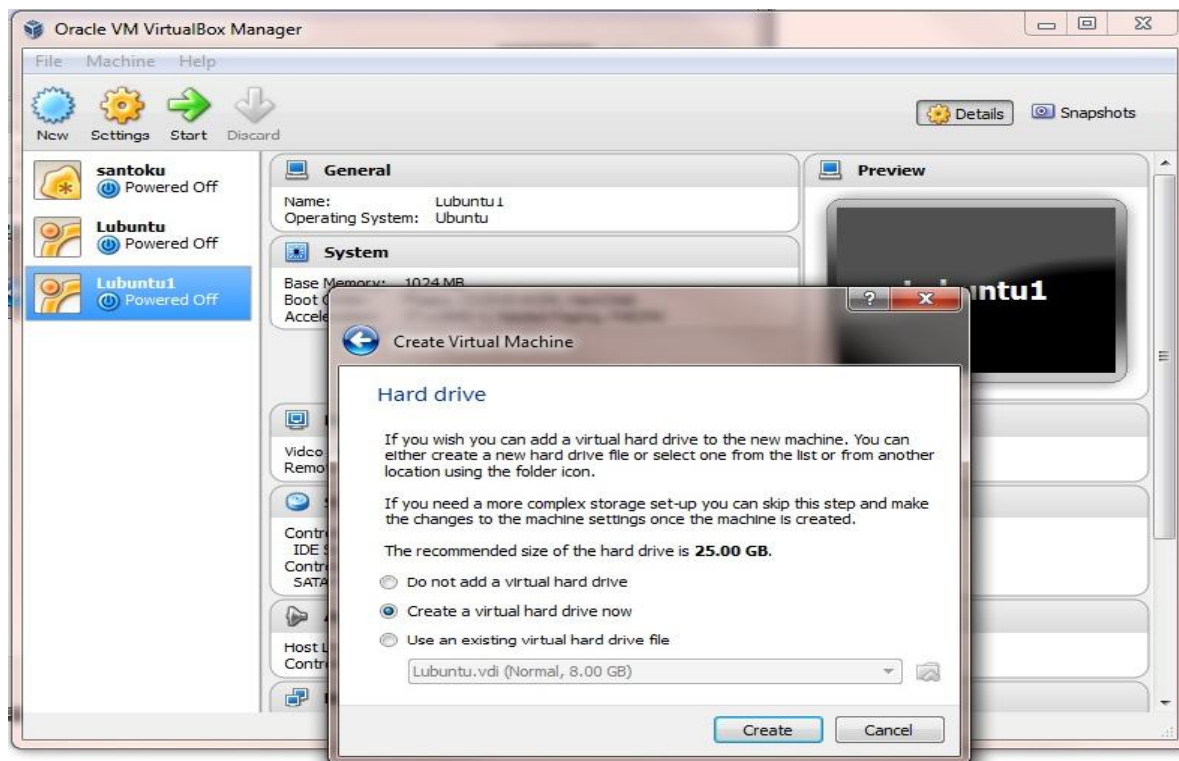
- Klikom na dugme New kreiramo novu virtuelnu mašinu, u ovom slučaju izabran je operativni sistem Windows 7 Slika br.7., kada smo izabrali određene opcije pritisnemo dugme Next.
- Tada dobijamo opciju da izaberemo koliko rama želimo za naš operativni sistem Slika br.8.. U ovom slučaju je određena veličina rama je 2048 MB pošto se radi o operativnom sistemu Windows 7, kada smo izabrali određene opcije pritisnemo dugme Next.
- Zatim kreiramo Virtuelni čvrsti drajv Slika br.9. i zatim odaberemo tip fajla Slika br.10., u ovom slučaju je odabran tip fajla VDI (VirtualBox Disk Image), kada smo izabrali određene opcije pritisnemo dugme Next.
- Zatim biramo vrstu fizičkog čvrstog drajva Slika br.11., u ovom slučaju je ostavljena defaultna vrijednost Dynamically allocated zatim pritisnemo dugme Next.
- Zatim izabrimo lokaciju gdje želimo da instaliramo vitruelnu mašinu Slika br.12., kada smo izabrali određene opcije pritisnemo dugme Next.
- Zatim pritisnemo dugme Start i krenemo sa instalacijom Windows 7 operativnog sistema Slika br.13..



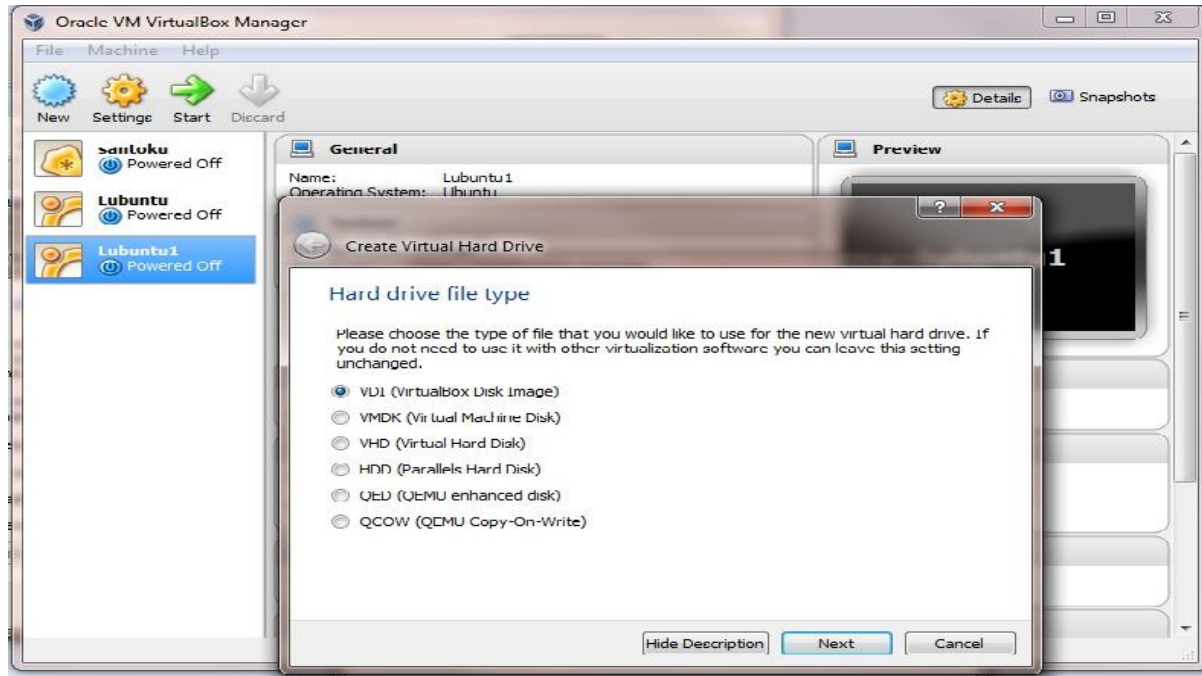
Slika br.7.Odabir operativnog sistema



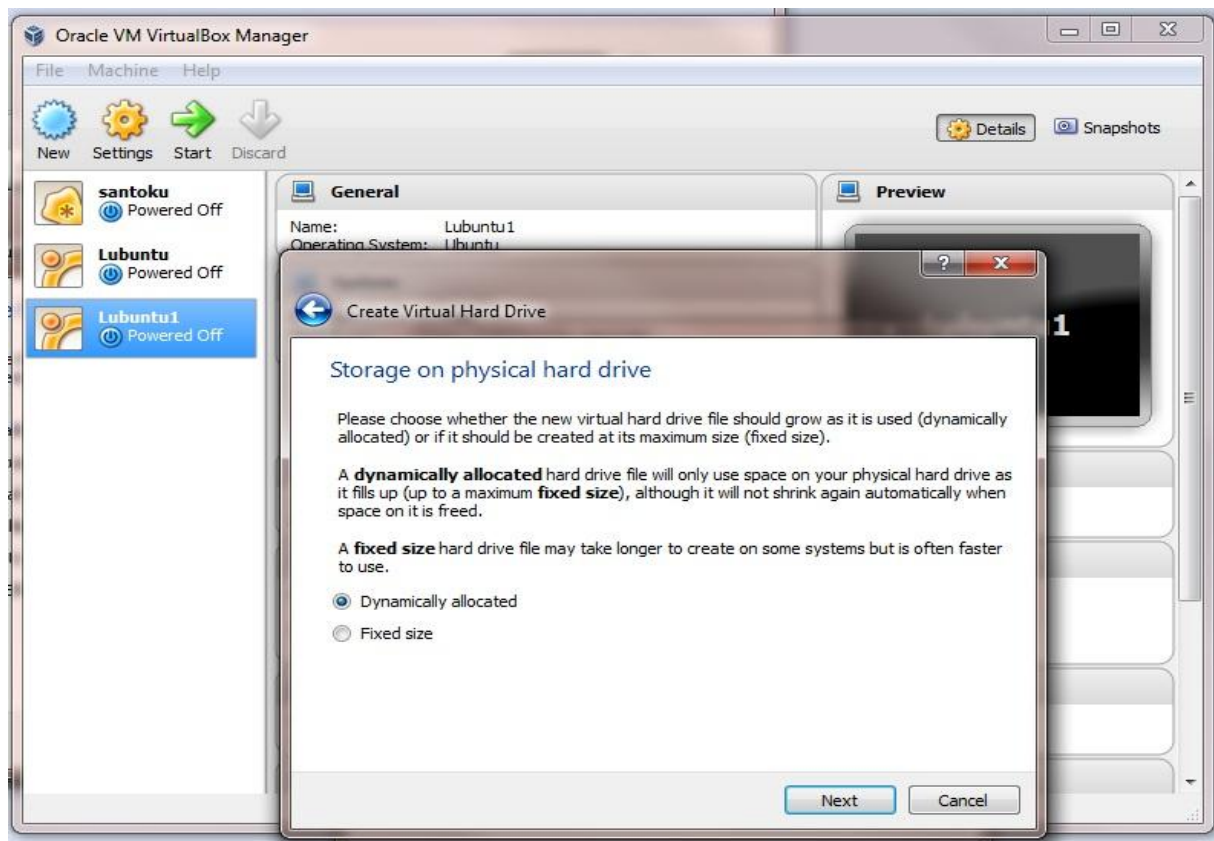
Slika br.8 .Dodjeljivanje rama



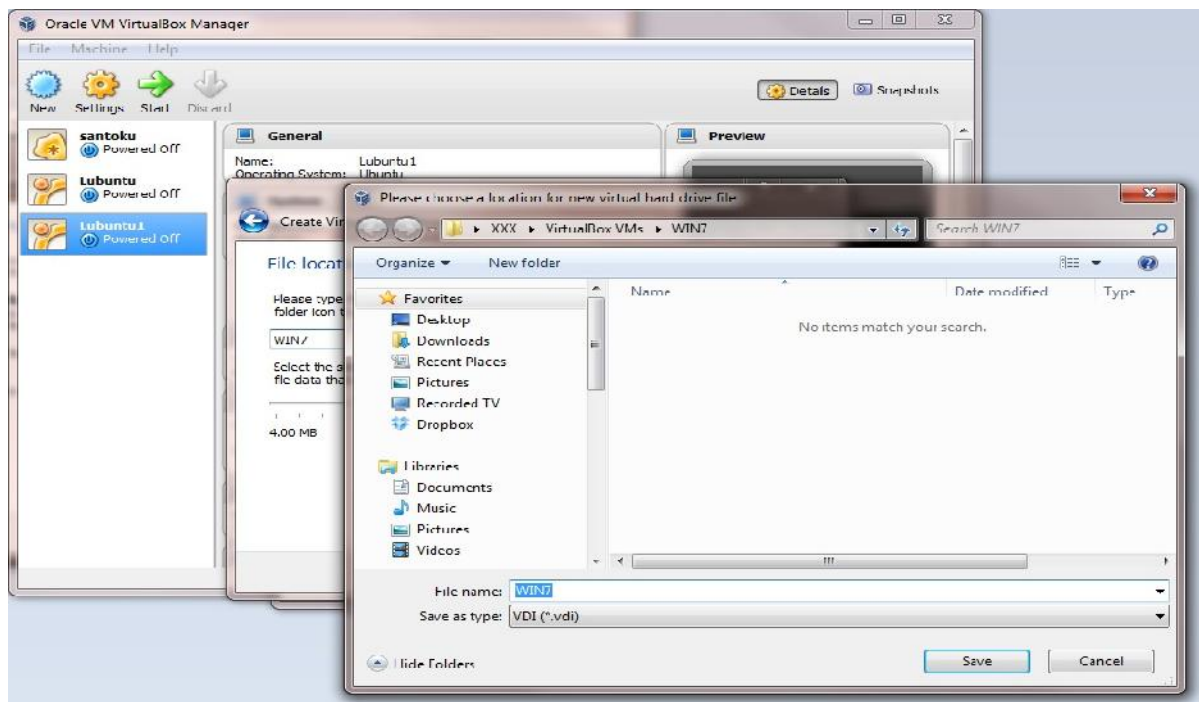
Slika br.9. Kreiranje virtualnog čvrstog dravja



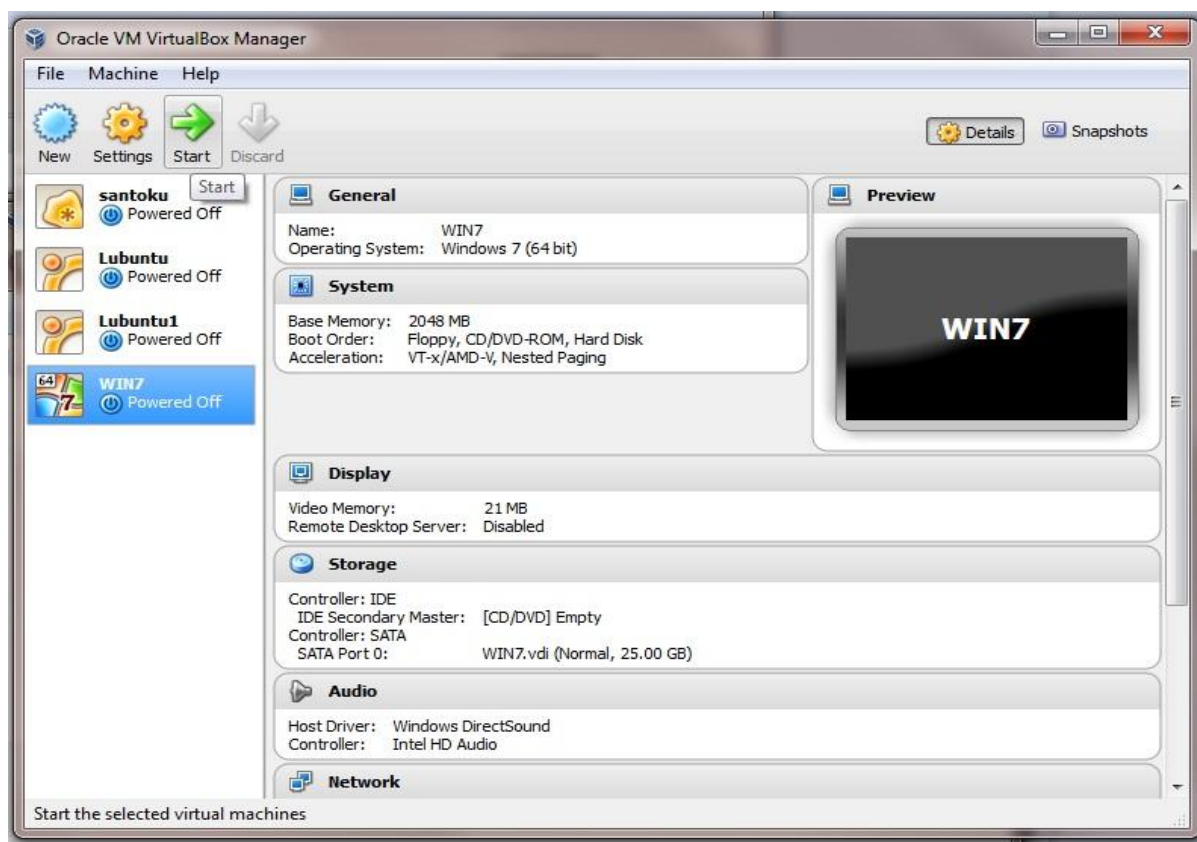
Slika br.10.Biramo tip čvrstog dravja



Slika br.11. Biramo vrstu fizičkog drajva



Slika br.12.Odabir lokacije na kojoj će biti instalirana viruelna mašina



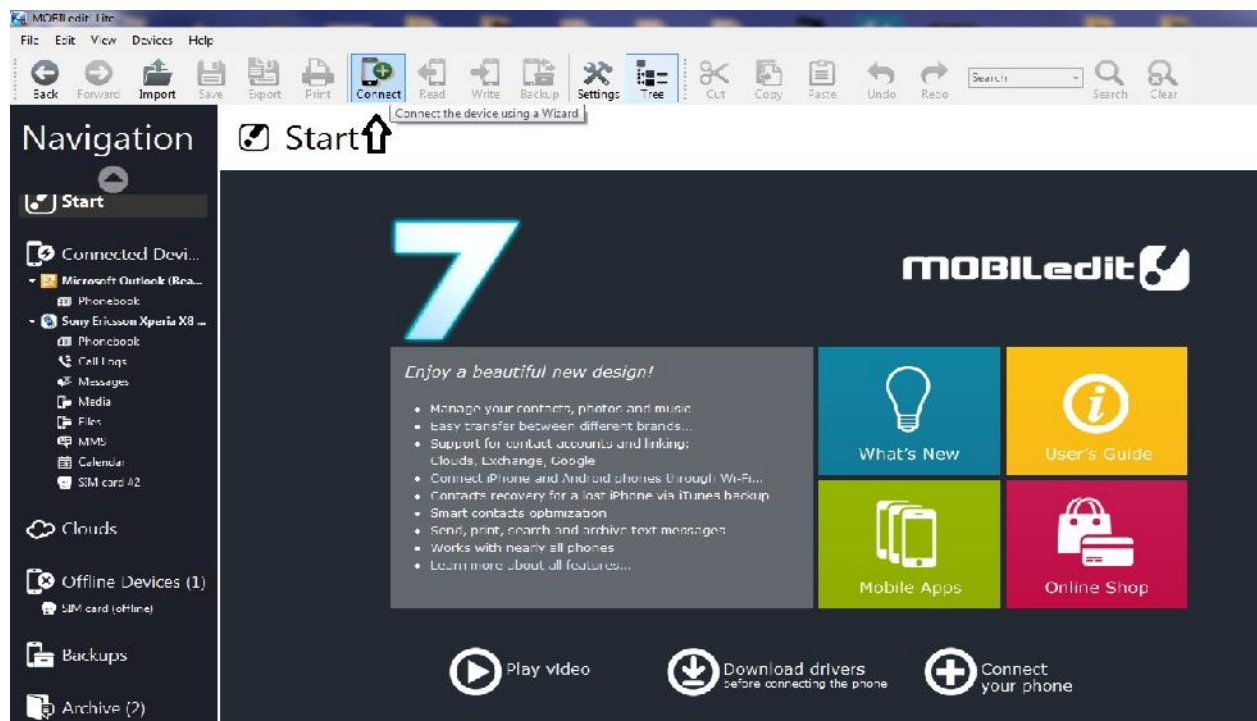
Slika br.13.Pokretanje vrituelne mašine

Virutelnu mašinu kroristimo radi veće sigurnosti. Ova virtuelna mašina nije priključena na internet tako da je omogućena veća bezbjednost, te su određeni servisi isključeni radi sigurnosti.

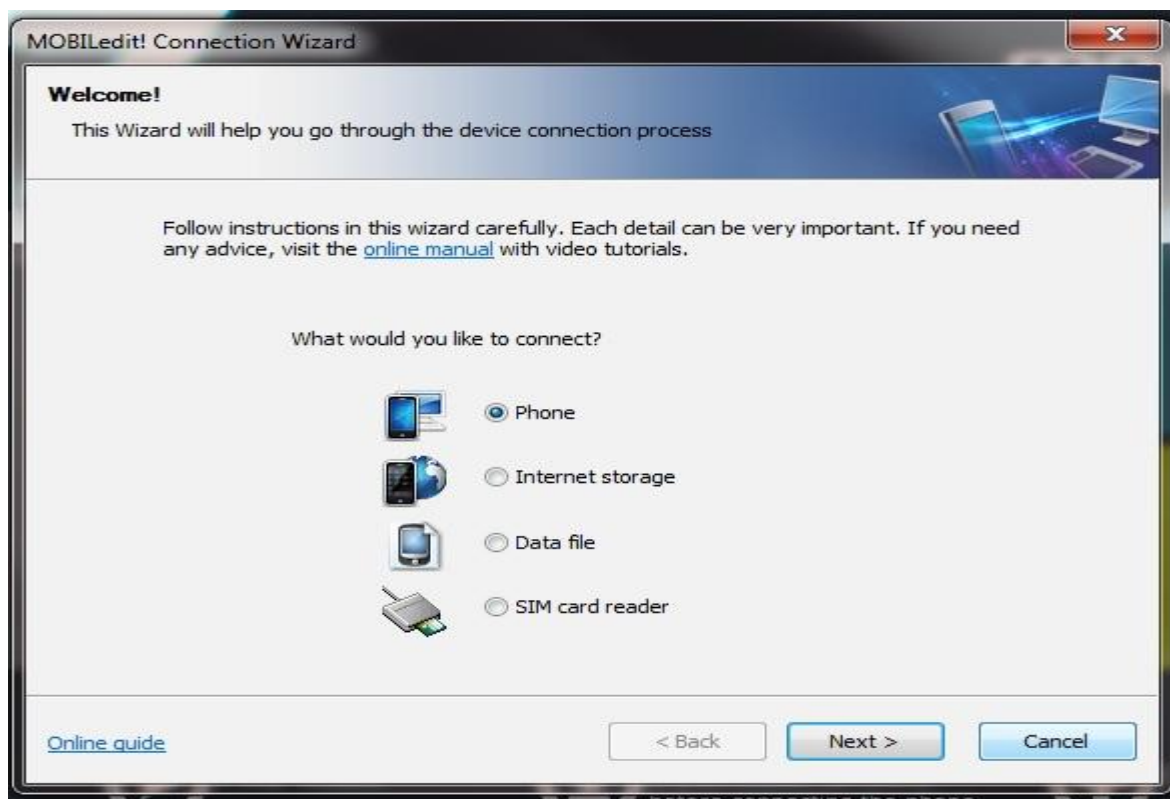
9.3. Mobiledit

Mobiledit je aplikacija koja obezbjeđuje vezu između mobilnog telefona i računara. Dizajnirana je da poboljša produktivnost i komunikaciju dozvoljavajući korisniku računara da preuzme podatke sa telefona. Ona se koristi za očitavanje SMS poruka, logova poziva, fotografija i drugih važnih podataka sa mobilnog telefona. Mobiledit forenzika je dizajnirana da pomogne u forenzičkim istragama. Ova aplikacija omogućava konekciju između računara i telefona pomoću Bluetooth, Infrared ili USB kabla, u zavisnosti od modela telefona. U ovom slučaju je korišten USB kabal za povezivanje telefona sa aplikacijom.

- Prvo povežemo telefon sa računarom i ako je potrebno instaliramo drajvere za računar.
- Kada smo pokrenuli aplikaciju Mobiledit, kliknemo na dugme Connect da bi smo povezali aplikaciju sa telefonom Slika br.14..
- Zatim odaberemo uređaj u ovom slučaju to je uređaj telefon (Phone) i pritisnemo na dugme Next Slika br.15..
- Kada smo odbrali uređaj, biramo način konektovanja u ovom slučaju korišteno je povezivanje pomoću kabla i zatim pritisnemo na dugme Next Slika br.16..
- Kada je očitao uređaj sa lijeve strane će se pojaviti meni, za uređaj koji je aplikacija očitala Slika br.17.. U ovom slučaju nas interesuju pozivi i SMS poruke.
- Prvo će mo pretražiti SMS poruke Slika br.17., u ovom slučaju pronašli smo SMS koji je poslan osumnjičenom Slika br.17., zatim će mo pogledati pozive Slika br.18., gdje smo ustanovili da je lice odgovorno za počinjeno djelo kontaktiralo više puta osobou kojoj je poslao SMS.



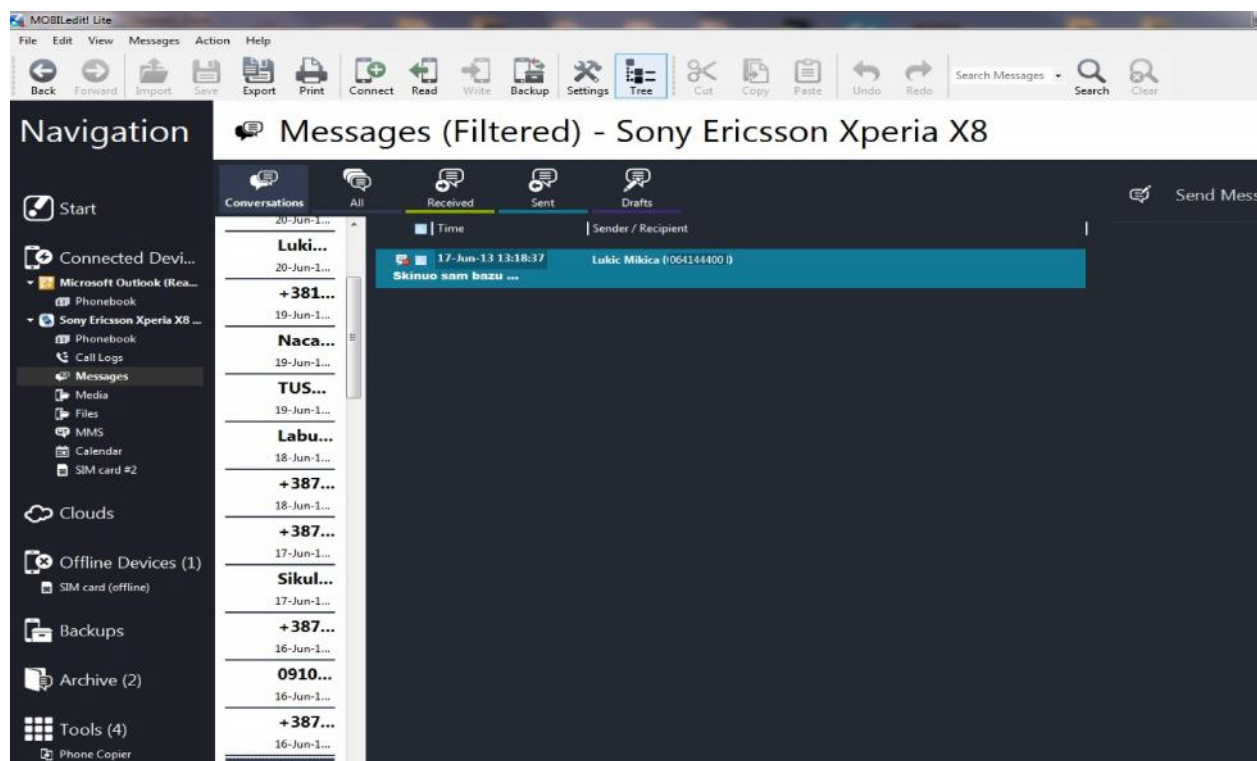
Slika br.14. Povezivanje aplikacije sa mobilnim uređajem



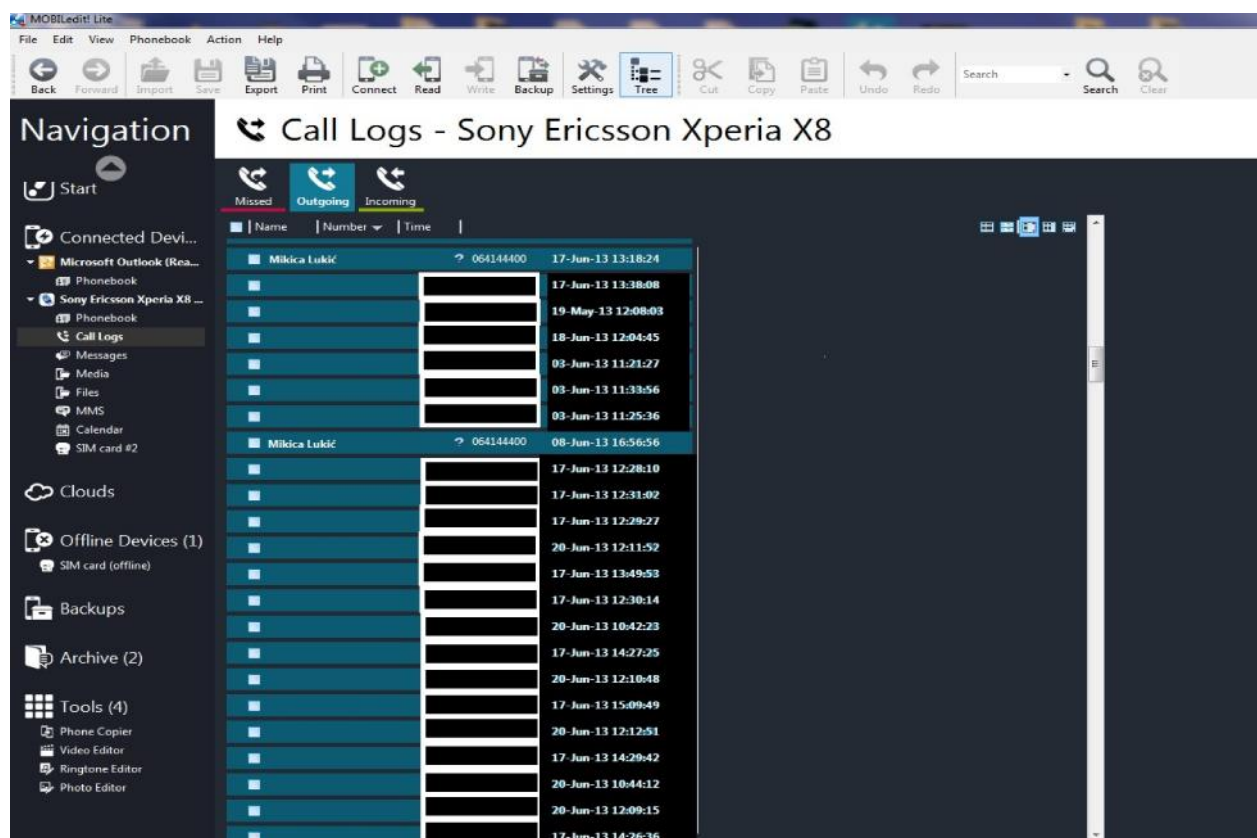
Slika br.15.Biranje uređaja



Slika br.16.Biranje načina povezivanja aplikacije sa uređajem



Slika br.17. Čitanje SMS poruka



9.4. EnCase

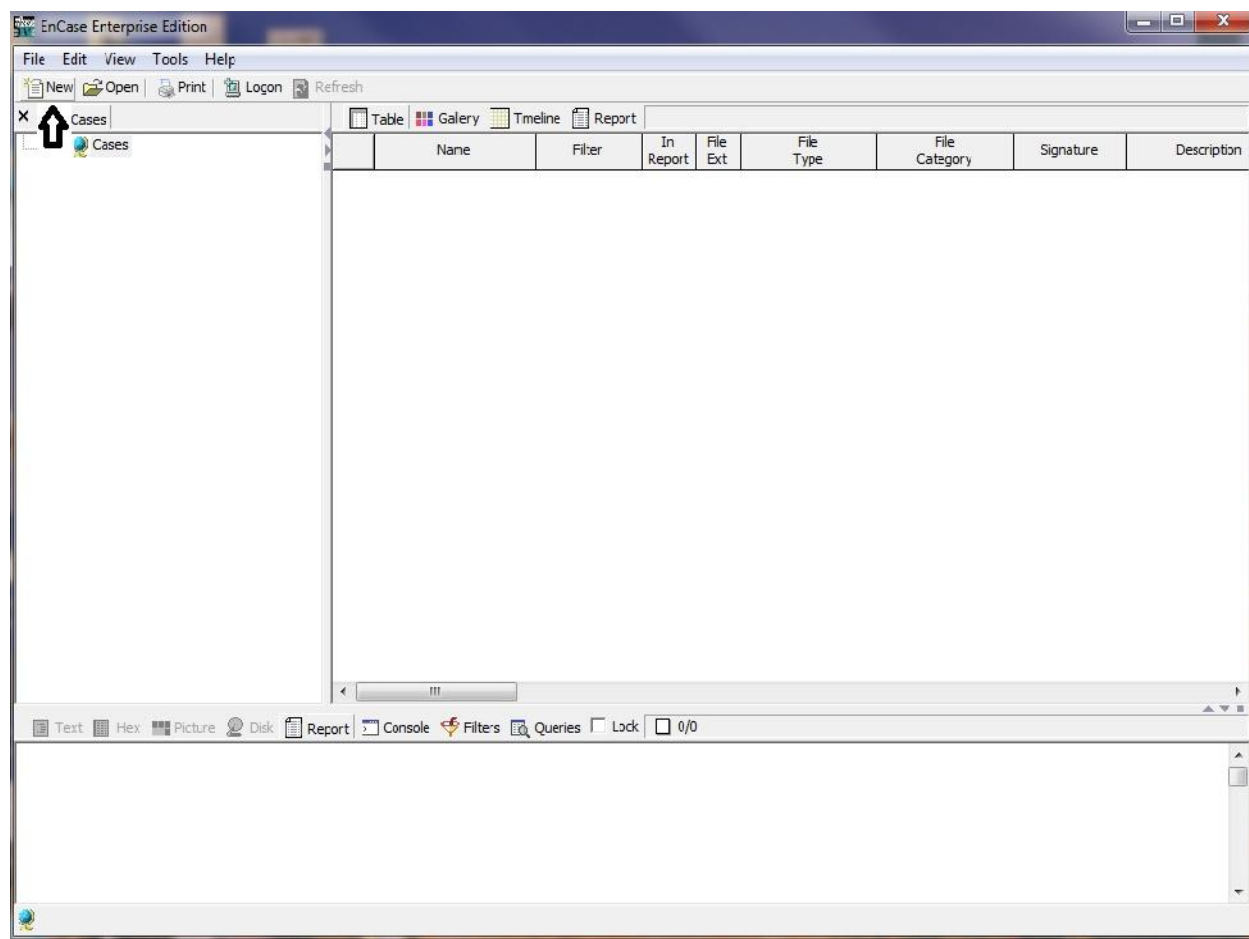
EnCase je računarski program za digitalnu forenziku, čiji je proizvođač američka kompanija Guidance Software. Program su prihvatile sudske ustanove širom svijeta.

Osim u sudsko-policijskim istragama, program je popularan i u privatnom sektoru. Široku primjenu nalazi i na području vojno-obavještajnih, ali i drugih sigurnosnih institucija.

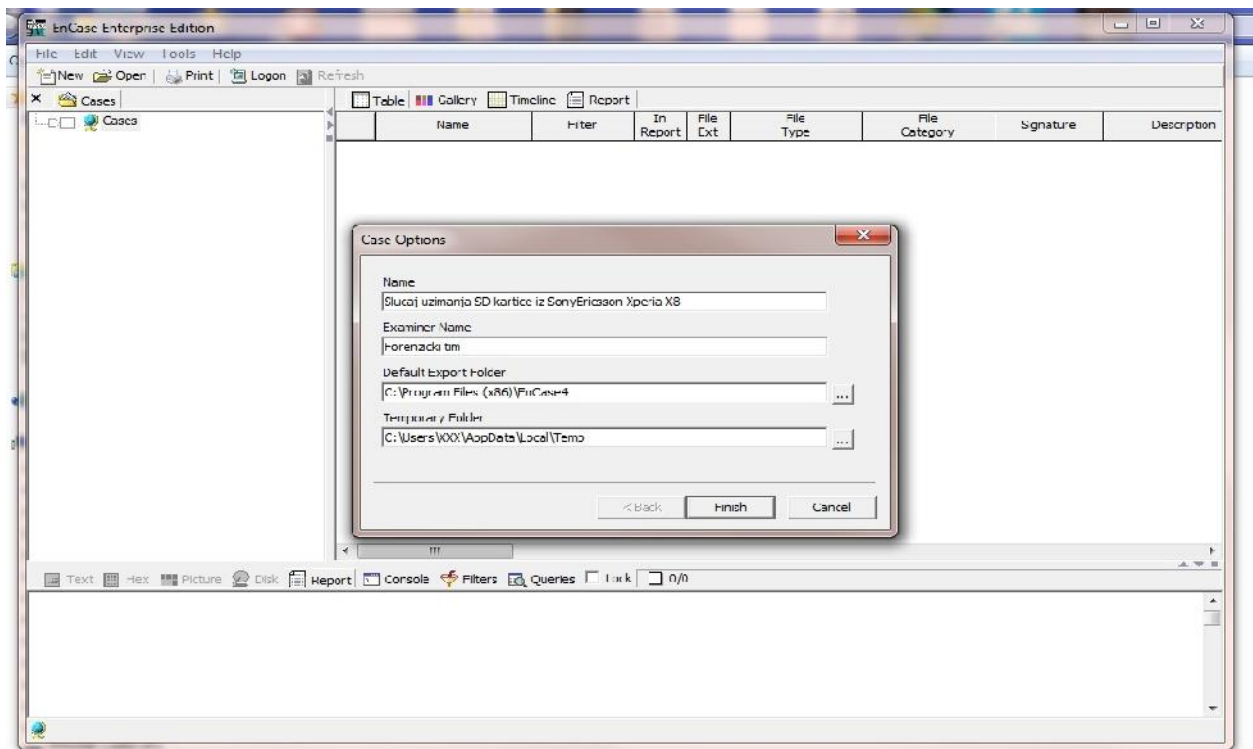
Može se reći da je EnCase industrijski standard u digitalnoj forenzici. Između ostalog, odlikuje ga dobra podrška korisnicima i velika baza korisnika. Korišćenjem programa može se uraditi kompletna forenzička analiza, počevši od akvizicije do konačnog izvještaja.

EnCase radi na Windows platformi, a postoji LinEn verzija koja se bazira na Linux-u.

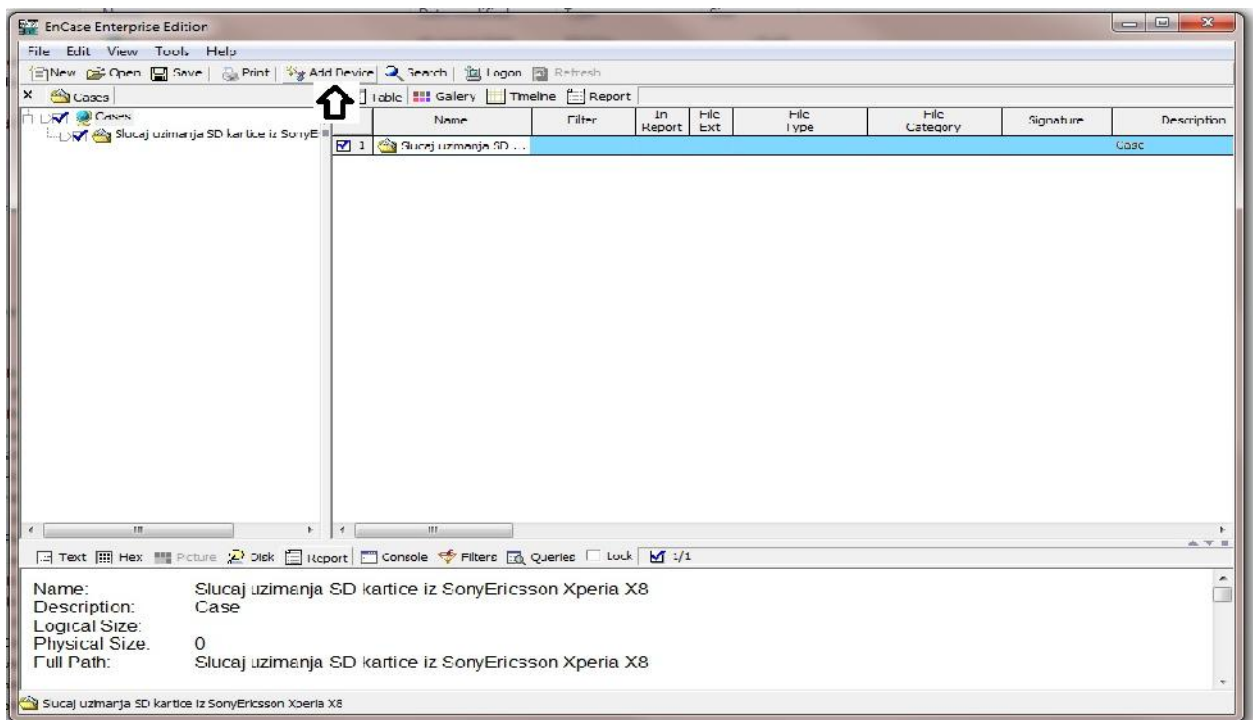
- Izaberemo dugme New za kreiranje novog slučaja Slika br.19..
- Zatim upišemo odgovarajuće podatke u odgovarajuća polja i pritisnemo dugme Finish Slika br.20..
- Kada smo to uradili kreirali smo slučaj, zatim pritisnemo dugme Add Device Slika br.21., izaberemo Local Drives Slika br.22., i izaberemo medij koji istražujemo Slika br.23., Slika br.24..
- Zatim odemo na stablo Slika br.25.
- Pronađeni fajl se nalazio na Kartici Slika br.26.
- Ustanovljeno je da je fajl identičan sa onim koji se nalazi na serveru Slika br.27., na osnovu datuma kreiranja fajla Slika br.28..



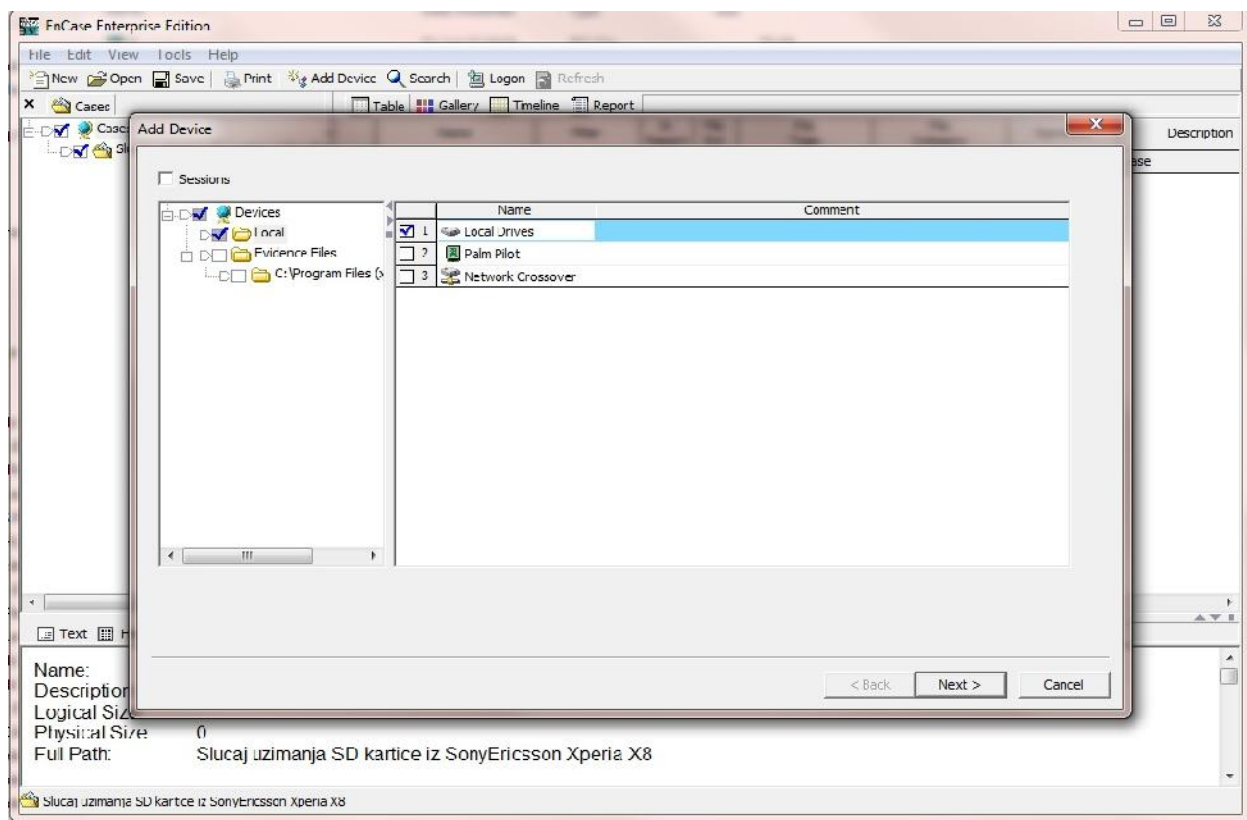
Slika br.19.Kreiranje slučaja



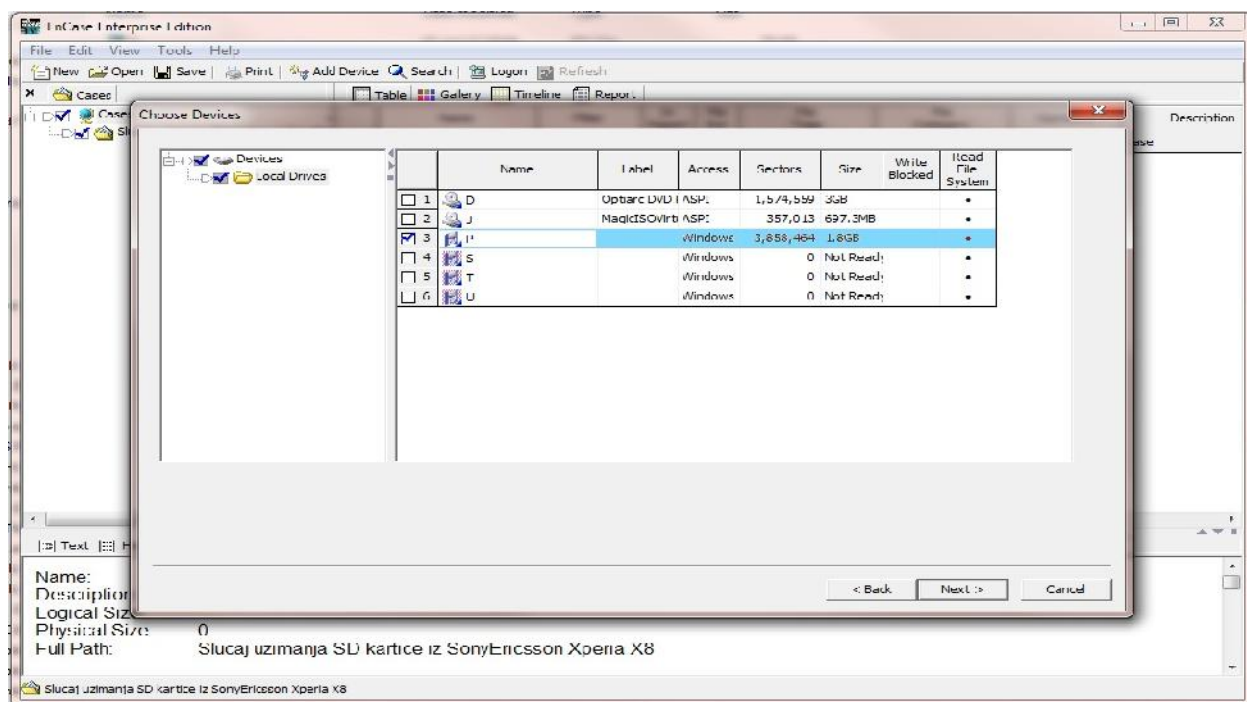
Slika br.20. Kreiranje slučaja, unošenje podataka



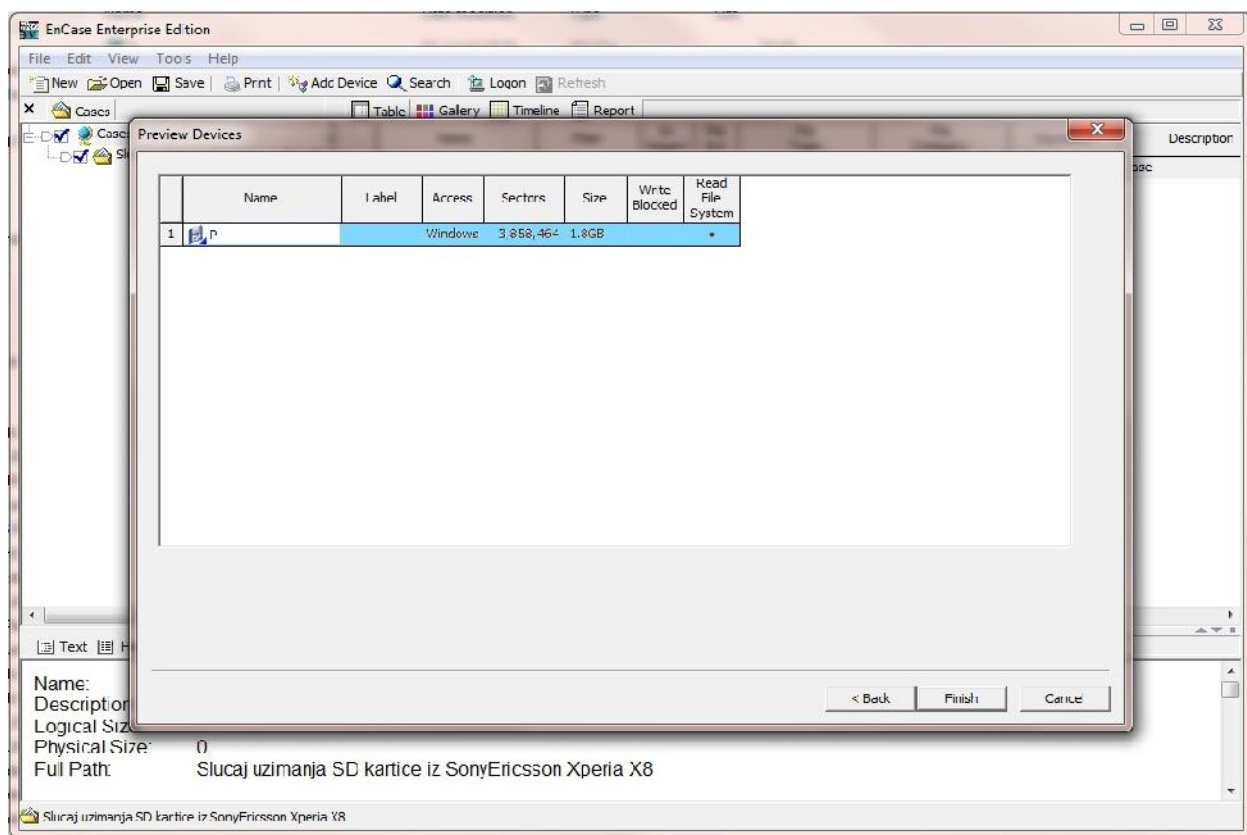
Slika br.21.Dodavanje uređaja



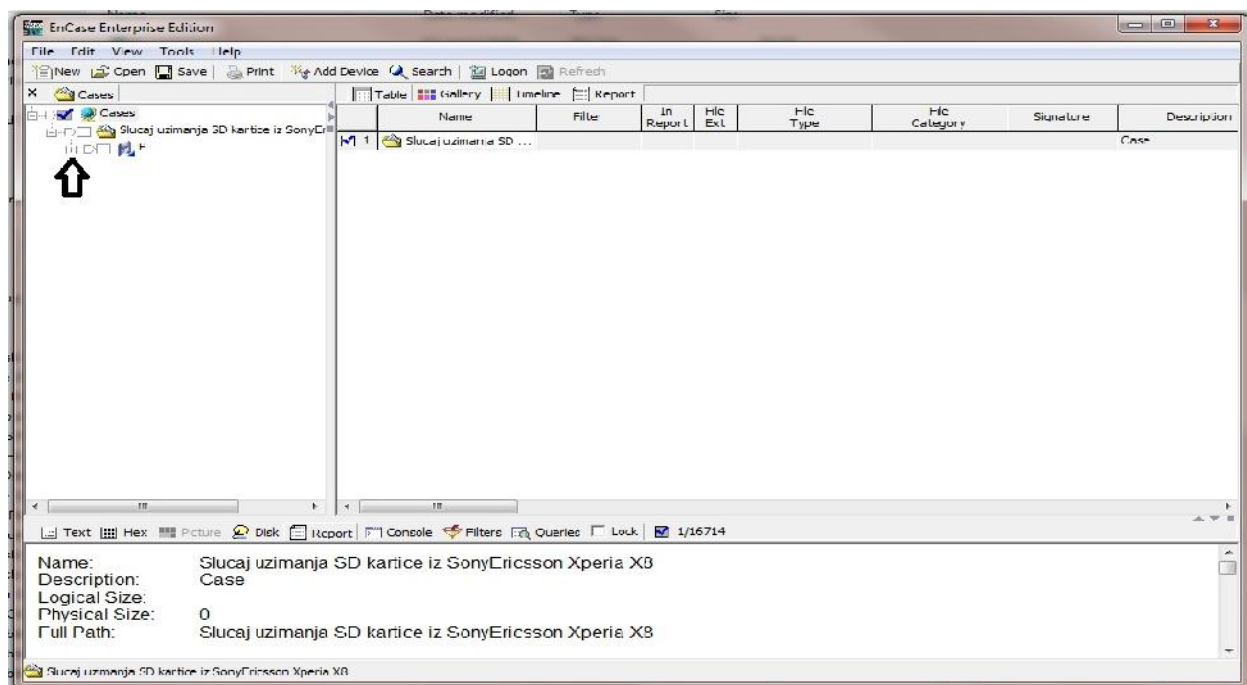
Slika br.22. Biranje Drajva



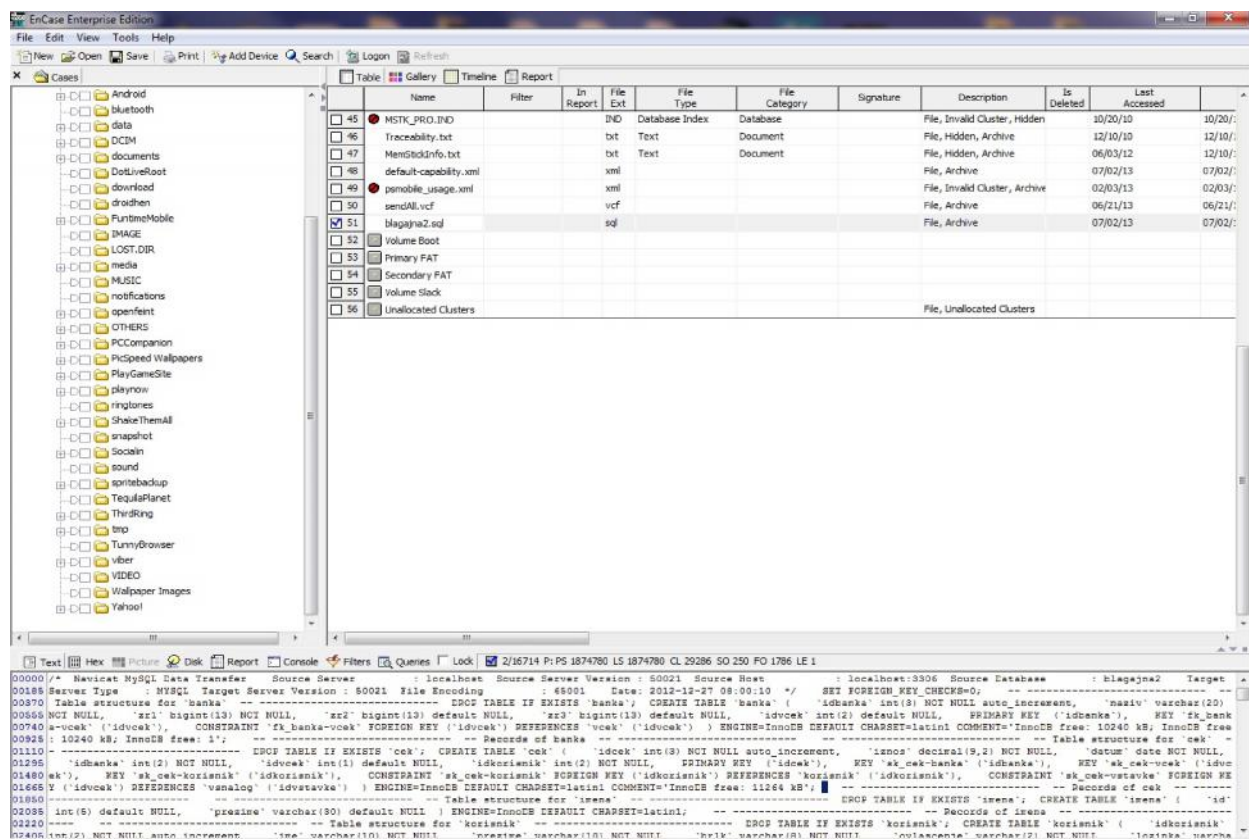
Slika br.23. Odabir medija



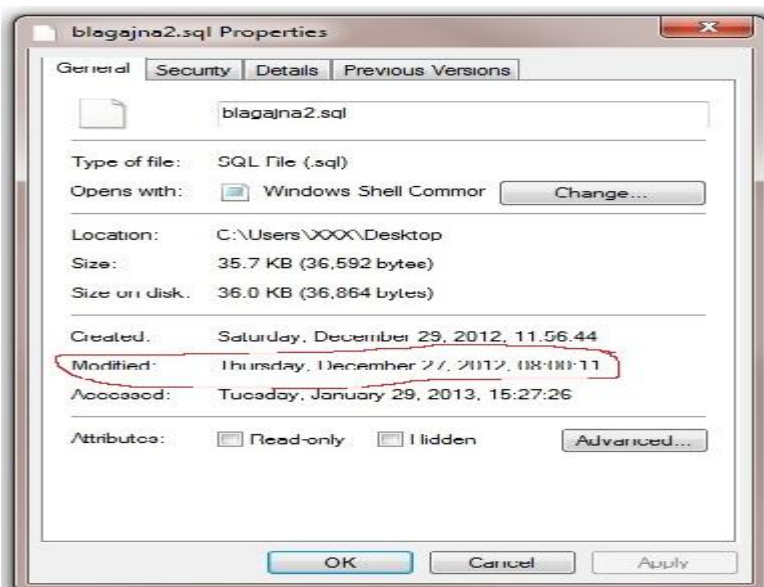
Slika br.24. Izabrani medij



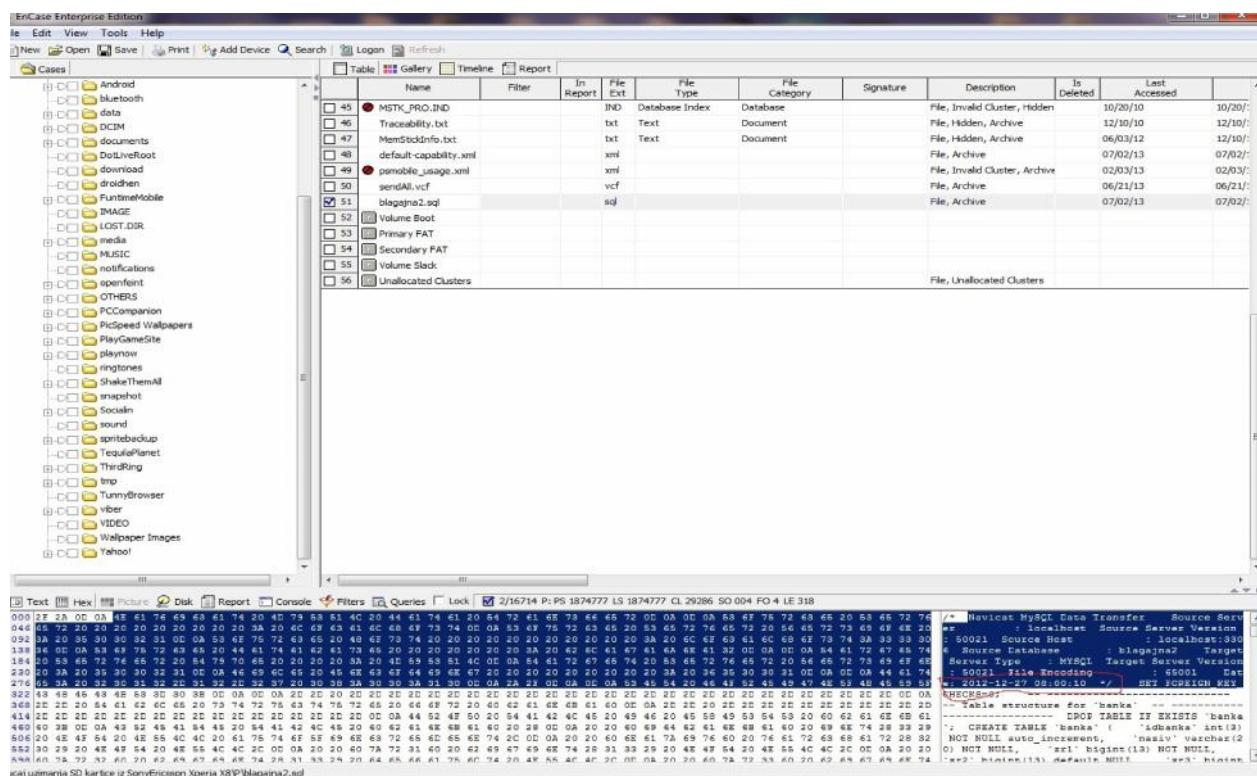
Slika br.25. Stablo



Slika br.26. Pronadeni fajl



Slika br.27. Originalni fajl sa servera



Slika br.28. Očitavanje vrijednosti pronađenog fajla

Nakon obavljene forenzičke istrage pronađeni su optužujući dokazi koji upućuju na osumnjičenog u čijem se posedu našao uređaj (Mobilni telefon, SonyEricsson Xperia X8, Android OS 2.1). Izveštaj o izvršenoj istrazi kompjuterskog incidenta je dostavljen rukovodiocu obezbjeđenja i on dalje odlučuje o sudbini istrage, tj. da li će proslediti izvještaj zvaničnim organima za dalji pravosudni postupak ili će odlučiti da ova istraga ostane na korporacijskom nivou unutar organizacije i pronaći kompromis sa osumnjičenim. U slučaju da korporacijska istaga pređe u zvaničnu i da se pokrene dalji pravosudni postupak softverska kuća bi izgubila ugled i veliki broj klijenata i snosila bi ogromne finansijske gubitke.

ZAKLJUČAK

Sprovođenje zakona je u stalnoj trci sa kriminalcima u primjeni digitalnih tehnologija i sa povećanjem digitalnih uređaja raste i potreba za usavršavanjem i standardizovanjem modela forenzičke istrage. Razni alati i metodologije postoje za sprovođenje aktivne istrage, kao što je novo polje aktivne istrage, koji se suočavaju sa brojnim izazovima. Aktivne forenzičke istrage se trenutno vrše pomoću daljinskog forenzičkog ispitivanja i alata, kao što su EnCase Enterprise edition i Pro Discover. Virtuelno okruženje omogućava forenzičaru da pristupi kompletnom stanju ciljnog sistema ne oslanjajući se na to da ciljni sistem obezbijedi informacije. Takođe, ovaj tip aktivne forenzičke analize može biti težak za antiforenzikčku detekciju, ako se uopšte može i otkriti.

Digitalni dokazi su svuda oko nas, stvaramo ih na mnoge načine, a da nismo ni svjesni da ih stvaramo. Imaju svoje prednosti, a i svoje mane. Globalno ljudi gube svoje privatnosti jer danas se može doći do njihovih digitalnih podataka veoma lako, čak mnogima su ukradeni digitalni podaci kao što su brojevi kartica za plaćanje, Pay pal računi, nalozi na socijalnim mrežama itd.. Ali imaju i prednosti ove tehnologije koje prate aktivnosti korisnika, jer na osnovu ovih informacija mogu da zaštite onoga ko koristi ove usluge i da pronađu počinioca krivičnog djela.

Svaki forenzičar bi trebao da zna, da se digitalna forenzika sastoji od poddisciplina i da se digitalna forenzika širi svakim danom na sve više električnih uređaja koji imaju memoriju. Te na jednu od danas najpopularnijih poddisciplina digitalne forenzike koju sam opisao, a to je digitalna forenzika Android platforme. Danas preko mobilnih telefona ostavljamo dosta digitalnih dokaza, kao na primer lokacije kuda se krećemo, sa kim razgovaramo, posjete putem Web pretraživača, logovi poziva, tekstualne poruke, multimedijalne poruke itd.

LITERATURA

- [1] Miljević I. M (2007), *Metodologija naučnog rada - Skripta*, Filozofski fakultet Univerziteta u Istočnom Sarajevu, Pale.
- [2] Mark Reith, Clint Carr, Gregg Gunsch Department of Electrical and Computer Engineering Graduate School of Engineering and Management Air Force Institute of Technology.
- [3] Zajedništvo www.ijde.org 8Internacional časopis digitalne evidencije jeseni 2002. broj – 1. , izdanje 3.
- [4] leong, R & Leung, H 2007, 'Deriving Cse-specific Live Forensics Investigation Procedures from FORZA', paper presented to Symposium on Applied Computing archive.
- [5] Carrier, BD & Grand, J 2004, 'A Hardware-Based Memory Acquisition Procedure for Digital Investigations', Digital Investigation Journal, no. 1(1).
- [6] Carrier, B 2006, 'Risks of live Digital Forensic analysis', Communications of the ACM, vol. 49, no. 2, pp. 56 - 61.
- [7] Foster M, WJ 2004, 'Process Forensics: A pilot study on the use of checkpointing technology in computer forensics', International journal of Digital Evidence, vol. 3, no. 1.
- [8] Payer,U 2004,'Realtime Intrusion-Forensics Aproptotype implementation',paper presented to Terena Networking conference.
- [9] Ren, W & Jin, H 2005, 'Honeynet Based Distributed Adaptive Network Forensics and Active Real Time Investigation', paper presented to 2005 ACM Symposium on Applied Computing, Santa Fe, New Mexico, USA., March 13-17. 2005.
- [10] Casey, E 2004, Digital Evidence and Computer Crime, 2nd ed, Elsevier Academic Press.

- [11] Roussev, V. & Richard, G. G. III. (2004). Breaking the performance wall: The case for distributed digital forensics. In Proceedings of the 2004 Digital Forensics Research Workshop (DFRWS 2004). distributivna
- [12] Shanmugasundaram, K. (2003). Automated reassembly of fragmented images. In Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing.
- [13] Farid, H. & Lyu, S. (2003). Higher-order wavelet statistics and their application to digital forensics. IEEE Workshop on Statistical Analysis in Computer Vision.
- [14] Chandramouli, R., Kharrazzi, M., & Memon, N. (2004). Image steganography and steganalysis: Concepts and practice. Lecture notes in computer science. SpringerVerlag, Vol. 2939. distrib
- [15] Grubor G., Milosavljević M. (2008), Digitalna forenzika.
- [16] Miloš J., Milan L. (2012), Projektovanje Informacionih sistema.
- [17] Larry E. Daniel, Lars E. (2012), Daniel Digital Forensics for Legal Professionals.
- [18] Milorad S. Markagić, (2013), Univerzitet odbrane u Beogradu, Vojna akademija, Katedra telekomunikacija i informatike, Beograd.
- [19] Ratimir Đ. Đokić, Milorad S. Markagić, (2013), Univerzitet odbrane u Beogradu, Vojna akademija, Katedra telekomunikacija i informatike, Beograd.
- [20] Christian Backer, (2009), Digital Forensics on Small Scale Digital Devices.
- [21] Andrew Hoog, (2011), Android Forensics Investigation, Analysis, and Mobile Security for Google Android.

Internet izvori:

[22] <http://hr.wikipedia.org/wiki/Forenzika>

posjećen 11.06.2013.

[23] <http://scindeks-clanci.ceon.rs/data/pdf/0042-8469/2013/0042-84691301136D.pdf>

posjećen 18.06.2013.

[24] <http://scindeks.ceon.rs/article.aspx?artid=0042-84691301136D&redirect=ft>

posjećen 21.06.2013.

[25] http://en.wikipedia.org/wiki/Global_Positioning_System

posjećen 21.06.2013.

[26] http://os2.zemris.fer.hr/ostalo/2010_marceta/Diplomski.htm

posjećen 22.06.2013.

[27] <http://developer.android.com/about/versions/jelly-bean.html>

posjećen 22.06.2013.