



UNIVERZITET SINGIDUNUM

**-MASTER STUDIJSKI PROGRAM-
SAVREMENE INFORMACIONE TEHNOLOGIJE**

Zaštita informacionih sistema i digitalna forenzika tablet računara

Mentor:
Prof dr. Mladen Veinović

Student:
Nenad Stefanović
2013/410752

Zaštita informacionih sistema i digitalna forenzika tablet računara

Sažetak: U ovom radu razmatrani se pojmovi informacije, informatike, informacionih sistema, njihova zaštita, mere bezbednosti, unapređenje bezbednosti sistema i prikupljanje dokaza u slučaju kompjuterskog kriminala, digitalna forenzika, istraga kompjuterskog kriminala i uređaji koji koriste Android platformu i smeštanje podataka u uređajima sa Android platformom. Pored navedenog, biće razmatrana primena kriptografije u zaštiti telekomunikacionih kanala informacionih sistema.

Ključne reči: podatak, informacija, informacioni sistem, kriptografija, zaštita informacionih sistema, digitalna forenzika, Android, tablet.

PROTECTION OF INFORMATION SYSTEMS AND DIGITAL FORENSIC OF TABLET

Abstract: This project considers the concepts of information, informatics, information systems, protection, safety measures in order to improve system security and the collection of evidence in the case of cyber crime, digital forensics, computer crime investigation and devices using the Android platform, the storage of data in Android-powered devices . In addition, we discuss the application of cryptography to protect the telecommunication channels of information systems.

Keywords: data, information, information systems, cryptography, protection of information systems, digital forensics, Android, Tablet.

SADRŽAJ

1. Metodologija	1
1.1 Uvodne napomene.....	1
1.2 Predmet istraživanja.....	1
1.3 Hipoteza	1
1.4 Ciljevi istraživanja	1
1.5 Naučne metode	2
2. UVOD.....	3
2.1 Podatak, informacija, informatika, računarstvo	3
2.2 Informacioni sistem.....	4
2.3 Kriptografija	6
2.4 Digitalni potpis	9
2.5 Forenzika kao nauka	9
2.6. Digitalna forenzika.....	10
2.6 Uređaji koji koriste Android platformu	10
2.7 Alati za digitalnu forenziku	12
3. ZAŠTITA INFORMACIONIH SISTEMA	13
3.1 Glavni enteti problema zaštite	14
3.1.1 Objekti.....	14
3.1.2 Pretnje	14
3.1.3 Posledice	16
3.1.4 Mere	17
3.1.5 Politika	17
3.2 Analiza i procena rizika	17
3.3 Sigurnost.....	18
3.4 Metode zaštite.....	19
4. PRIMENA KRIPTOGRAFIJE U ZAŠTITI INFORMACIONIH SISTEMA	

4.1	Primena simetričnih algoritama.....	21
4.2	Primena asimetričnih algoritama.....	21
4.3	RSA algoritam.....	22
4.4	Hibridni algoritmi.....	23
4.5	Digitalni potpis i sertifikat	24
4.6	Kriptoanaliza	25
5.	FORENZIČKA ISTRAGA RAČUNARA	26
5.1	Istraga i akvizicija digitalnih podataka	26
5.2	Isključivanje računara i SWAP fajl.....	26
5.3	Korišćeni termini u forenzičkoj istrazi	27
5.4	Standardizovana procedura.....	28
5.5	Lica koja se bave upravljanjem kompjuterskim incidentom.....	29
6.	DIGITALNA FORENZIKA ANDORID UREĐAJA.....	30
6.1	Karakteristike android uređaja	30
6.2	Hardver android uređaja	31
6.3	Procesi tokom startovanja Android uređaja.....	34
6.4	Android fajl sistem i struktura podataka.....	35
7.	ADB I FORENZIČKI ALATI	38
7.1	Android Debug Brige (ADB)	38
7.2	Forenzički alati	39
8.	TABLET RAČUNARI KARAKTERISTIKE.....	43
9.	NIVOI BEZBEDNOSTI ANDROID UREĐAJA I PREDLOZI ZA POBOLJŠANJE.....	45
10.	STUDIJA SLUČAJA.....	46
11.	ZAKLJUČAK.....	55
	Literatura	57

1. Metodologija

1.1 Uvodne napomene

U ovom istraživanju obuhvaćene su metodologije zaštite informacionih sistema kroz primenu mera zaštite od telekomunikacionih kanala do organizacijskih mera kao i metodologija digitalne forenzike i razumevanje procesa u Android uređajima, radi uspešnog sprovođenja istrage kompjuterskog kriminala.

Sve većim korišćenjem širokopojasnog interneta u svakodnevni život i poslovne procese, javlja se i sve veća potreba za zaštitom ličnih i poslovnih podataka a koji se obrađuju kroz razmenu u informacionom sistemu. To potvrđuje i strategija razvoja informaciono-telekomunikacionih sistema u Republici Srbiji do 2020.godine, gde se akcenat stavlja na primenu mera zaštite ličnih podataka uz primenu drugih zakonskih i podzakonskih propisa.

Težnja za uvođenjem malih prenosnih računara u svakodnevnu upotrebu i procese automatizacije svakako ukazuje na potrebu njihovog bližeg izučavanja, posebno kada su u pitanju uređaji sa Android platformom. Isti tako postaju meta krađe podataka kao i sredstvo kojim može biti izvršena krađa. Razumevanje pretnji i mogućih scenarija napada će omogućiti bezbednosnim procesima i programerima utvrđivanje odgovarajuće kontrole za ublažavanje rizika.

1.2 Predmet istraživanja

Predmet ovog istraživanja su bezbednosni izazovi i moguća rešenja, vezana za funkcionisanje informacionih sistema i njihovu zaštitu kroz zaštitu telekomunikacionih kanala. Obuhvaćeni su pojmovi podataka, informacije, informacionog sistema, kriptografije i zaštite informacionog sistema, kao i standardizacija istrage kompjuterskog kriminala posebno uređaja na Android platformi.

1.3 Hipoteza

Opšta hipoteza: Razvoj informaciono-telekomunikacione tehnologije doveo je do ekspanzije u razvoju malih, prenosnih računara, koji se polako uvode u velike informacione sisteme i često u sebi sadrže podatke poverljive prirode.

Posebna/radna hipoteza: Postoji veliki broj pretnji po bezbednost podataka i samog funkcionisanja Android uređaja, što je dovelo do razvoja različitih tehnika i modela koji su u široj ličnoj primeni, a očekuje se i njihova primena u trgovini i posebno obrazovanju.

1.4 Ciljevi istraživanja

Naučni cilj: Istraživanje i definisanje bitnih pretnji po bezbednost informacionih sistema, zatim istraživanje, definisanje, analiza, prezentacija mogućih rešenja i utvrđivanje postupka kod forenzike Android uređaja. Takođe, težišno je istraživana mogućnost korišćenja osnova programiranja i otovorenog koda u cilju forenzičke istrage.

Društveni ciljevi: Obezbeđivanje adekvatnog informisanja svih uključenih u funkcionisanje zaštite informacionih sistema o potencijalnim pretnjama po bezbednost funkcionisanja sistema kao i o mogućim rešenjima sa akcentom na zaštitu podataka i njihovu identite na komunikacionom putu, kao i navedeno pohranjeno na uređajima sa Andorid platformom.

1.5 Naučne metode

Pri izradi ovog rada korišćene su osnovne naučne metode deskripcije, indukcije, dedukcije, analize, sinteze i generalizacije.

Metoda deskripcije je korišćenja pri objašnjavanju osnovnih pojmova i sistema funkcionisanja.

U teorijskim segmentima su primenjene metode indukcije, dedukcije i analize, a u izvodjenju zaključaka metode sinteze i generalizacije.

2. UVOD

2.1 Podatak, informacija, informatika, računarstvo

Simbolički i formalizovani prikaz činjenica, nekih pojmova i instrukcija koji je pogodan za obradu bilo preko ljudi ili uz pomoć mašina predstavlja **podatak**. U osnovi, podatak predstavlja formalizovanu činjenicu kao što je reč ili slika. Podatak je poruka koja se može i ne mora iskoristiti [5].

Ukoliko postoji i najmanja verovatnoća da se poruka jednoznačno i tačno iskoristi, da predstavlja neospornu činjenicu, tada predstavlja informaciju, dok svojstva objekata i njihovih odnosa u prostoru i vremenu izražavamo podacima.

Podatak se može shvatiti kao apstraktna struktura sastavljena od:

- značenja (naziv i opis značenja određenog svojstva);
- vrednosti (mera i iznos);
- vremena.

Prema navedenom, podatak je u osnovi pojam koji opisuje i oslikava stanje nekog procesa u realnom svetu.

Skup činjenica, obrađenih i organizovanih da predstavlja neko obaveštenje je **informacija**.

Osnovni pojmovi u informatici su **informacije**, kao fenomen i **komunikacija** kao proces. Informacija je postala relevantan pojam za sve nauke koje se bave simboličkom komunikacijom u rasponu od matematike do računarske nauke, ili od logike do lingvistike, odnosno od elektronike do bibliotekarstva i dr. To je informaciji dalo interdisciplinarnu dimenziju, jer je svaka nauka pokušala i još pokušava da protumači taj kompleksan pojam. Sve ovo ukazuje da pojam informacija nije lako shvatiti niti jednostavno protumačiti.

Informacija je reč latinskog porekla "**in formare**" što izvorno znači stavljanje u određenu formu, odnosno, davanje oblika nečemu, ali je tokom vremena izgubila prvobitno značenje. Danas nema jedinstvenog pristupa fenomenu informacije, a još manje opšte prihvaćene definicije informacije.

Često se pojam podatka i informacije poistevećuju, a najbolji primer za ukazivanje na snjihovu različitost je sledeći primer, broj 11 je podatak i kao takav nema posebno značenje, međutim "Sada je 11 časova" je informacija jer smo podatku dodelili značenje. Na primeru vidimo da se informacija sastoji od **podatka** i **značenja** koje mu je dodeljeno.

Računarstvo je nauka vezana za razvoj arhitekture računarskog sistema (hardvera i softvera), npr. teoriju algoritama, teoriju programskih jezika itd.

Računarstvo se bavi proučavanjem teoretskih osnova informacije i računanja, njihovim implementacijama i primenom u računarskim sistemima. Računarstvo ima mnoga potpolja; neki naglašavaju računanje i specifične rezultate (kao što je računarska grafika), dok drugi naglašavaju svojstva računskih problema, (kao što je teorija kompleksnosti), a treći se usresređeni na izazove u ostvarenju računanja.

Na primer, teorija programskih jezika proučava pristupe u opisu računanja, dok računarsko programiranje primenjuje specifične programske jezike za rešavanje specifičnih računskih problema sa rešenjima. Dalje, interakcija čoveka i računara, se fokusira na izazove u izradi računara i činenju računara korisnim i univerzalno pristupačnim svim ljudima.

Predmet izučavanja informatike je razvoj i primena informacionih tehnologija, razvoj informacionih delatnosti i angažovanje ljudi u obavljanju tih delatnosti. Pojam informatika se sastoji od reči informacija i automatika. Prvi put se pominje u Nemačkoj 1957. godine od strane Karla Štajnbuha. Ovaj pojam pokriva istovremeno nauku o računarima (računarstvo) i nauku o informacionim sistemima.

Informatika ima za osnovu matematiku, elektroniku, fiziku i neke inženjerijske nauke.

Nastala je u 19. veku razmišljanjem tadašnjeg genija *Čarlsa Bebidža*, koji je zamislio mašinu koja bi uzimala podatke, obrađivala ih na neki način i onda obrađene podatke prikazivala.

Bebidž je to zamislio mehanički, dok su danas računari elektronski. Današnji računari imaju sličnosti sa Bebidžovom mašinom.

Primena računara je omogućila bolji život, efikasniji i efektivniji rad preduzeća, državnih organa i institucija, kao i prosperitet društva u celini, uz veliko automatizovanje svakodnevnih procesa tokom interakcije ljudi i mašina, i to:

- Elektronsko izdavaštvo podrazumeva zamenu papirnih izdanja knjiga, časopisa i drugih publikacija elektronskim izdanjima.
- Elektronske komunikacije omogućavaju gotovo trenutni prenos poruka, pisama, dokumenata, slika, audio i vizuelnih podataka među korisnicima.
- Elektronska trgovina podrazumeva razgledanje i kupovanje od kuće pomoću računara.
- Elektronsko bankarstvo omogućava izvođenje finansijskih transakcija od kuće, bez odlaska u banku.
- Primena informacionih tehnologija poboljšava život i u drugim oblastima, npr. u zdravstvu, transportu, turizmu itd.

Primena informacionih tehnologija unosi revolucionarne promene i u sistem obrazovanja. Mogućnosti široke primene multimedija omogućavaju realizovanje obrazovnog procesa na potpuno nov način. Tu je i mogućnost učenja na daljinu primenom računarskih mreža i interneta, tzv. **e-learning**, koji je sve popularniji.

2.2 Informacioni sistem

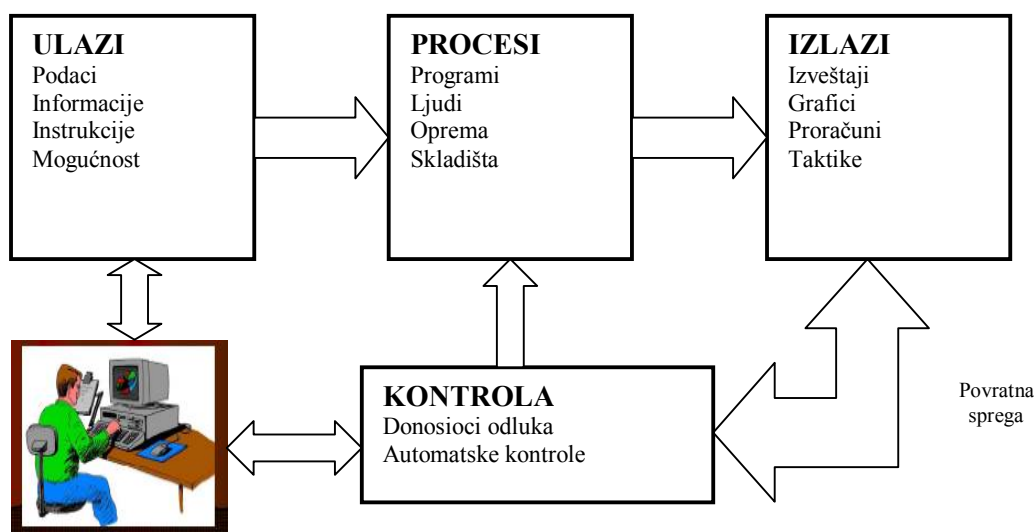
Informacioni sistem je integrisani skup komponenti za prikupljanje, snimanje, čuvanje i obradu podataka [7], odnosno predstavlja skup elemenata sa svojim međusobnim vezama u interakciji.

Da bi jedna celina bila izdvojena, odnosno da bi predstavljala sistem, ona mora imati definisanu granicu sistema koja ga odvaja od njegovog okruženja [6]. Tako definisan sistem u svojoj interakciji sa okruženjem se sastoji od: dejstva okoline na sistem i naziva se **ulaz**, i dejstva sistema na okolinu što predstavlja **izlaz** sistema.

Ukoliko posmatramo sa aspekta da osnovni element predstavlja njegovu funkciju, onda sistem predstavlja skup funkcija koje se u njemu obavljaju.

Ovako definisani informacioni sistem ima svoj osnovni cilj, a to je obrada prikupljenih podataka i informacija, radi njihove transformacije u specifičnu namenu.

Na primeru poslovnog informacionog sistema može se videti konkretna interakcija sistema sa okolinom (slika 1).



Slika 1: Interakcija informacionog sistema sa okolinom

Na slici 1. vidimo jednu organizaciju informacionog sistema, gde se podaci registruju, pripremaju, unose, organizuju i čuvaju u bazama podataka informacionog sistema. U sistemu se podaci obrađuju i obezbeđuju za dalje rešavanje poslovnih zadataka. Cilj informacionog sistema je da na ekonomičan način obradi i podatke transformiše u informaciju ili znanje.

Komponente koje čine informacioni sistem su: hardver, softver, baze podataka, telekomunikacije i ljudski resursi [7].

O hardveru je bilo reči u uvodu, a može se reći da danas skoro svaka poslovna organizacije ima u sebi računar za automatsku obradu podataka.

O softveru j takođe bilo više reči u računarstvu i njegovom istorijatu, a ovde bih napomenuo da je osnovni softver uglavnom sistemski softver, odnosno operativni sistem računara (Win P, Win7, Win 8, Linux itd.). Pored operativnog sistema u računaru se koriste i softver aplikacije za specijalizovano korišćenje.

Baze podataka su u suštini i srce svakog informacionog sistema. One predstavljaju skup međusobno povezanih podataka organizovanih na način pogodan za njihovu primenu i upotrebu.

Telekomunikacije predstavljaju u stvari mrežnu komponentu, za povezivanje više računara u mrežu bilo lokalnu (LAN), ili širu mrežu (WAN). Najpoznatija je internet mreža koja povezuje sve kontinente gde se umrežavanjem korisnicima pružaju velike i različite mogućnosti, u zavisnosti od ličnih ili poslovnih potreba.

U ljudske resurse se ubrajaju sva lica korisnici podataka iz informacionog sistema, od administratora do krajnjeg korisnika u informacionom sistemu, profesionalni informatičari ili uslužni korisnici.

2.3 Kriptografija

Od pisanja informacija postoji potreba za njihovim prikrivanjem od strane trećih, zlonamernih lica. Tada je i sama kriptografija začela svoje korene. Neki podaci o korišćenju kriptografije datiraju još iz doba Egipta a jedan od prvih velikih vojskovođa koji je koristio šifrovane poruke je Julije Cezar. Julije Cezar je koristio šifru u kojem je važno pravilo “pomeri za” u alfabetu rimskog pisma.

Primenom enigme, mašine za šifrovanje poruka na do tada još nepoznat način, koju su koristili nemci u drugom svetskom ratu stvoren je značajan pomak u kriptografiji i primeni mašina za šifrovanje. Međutim ma koliko ona tada bila revolucionarna, bila je probijena.

Pojavom računara otvaraju se nova vrata kriptografiji u pogledu razvojem brzina računara. Istovremeno sa razvojem kriptografije razvija se i mogućnost za probijanje šifri za mnogo manje vremena. Uporedo sa razvojem mogućnosti računara razvijaju se sistemi i algoritmi koji su bili znatno komplikovaniji za primenu.

Za razliku od ogromnih suma koje su se 70 godina proslog veka trosile na zaštitu i razvoj sigurnih sistema, gde su bile privilegovane samo države i bitnije institucije u državi, danas je situacija drugačija. Danas postoji puno besplatnih alata koji pružaju visok nivo kriptovanja (zaštite). U nekim državama i danas postoje ograničenja po pitanju korišćenja alata, ali sve je to uzaludno kada se danas na internetu mogu naći besplatne kriptografske metode.

Budući da se u bližoj teoriji zaštita informacionih sistema uglavnom posmatra kroz zaštitu računarskih mreža, odnosno računarskih sistema, sve je veća težnja za primenom određenih mera zaštite posebno na komunikacijskom putu od izvora do odredišta informacija.

U računarskim sistemima prenos informacija se vrši uglavnom neštićenim komunikacijskim kanalima, gde svaki napadač može da dovede do narušavanja sigurnosti sistema.

Reč kriptografija znači tajno pisanje¹. Kroz istoriju kriptografija seže od Cezara pa naovamo. Istorijski posmatrano, kriptografiji su najveći doprinos dali vojnici i diplomate. Budući da je zaštita prenosa informacija značila vojnicima zbog značaja taktike [2].

Danas se kriptografija zasniva na primeni informatičke opreme, brzih računarskih procesa, a u cilju primene složenih matematičkih metoda za kriptovanje (šifrovanje) i dekriptovanje (dešifrovanje) podataka.

Radi lakšeg shvatanja pojmovnog određivanja i suštinske razlike između termina kriptografije i kriptologije, mada se u literaturi može naći i drugo tumačenje da je kriptografija u osnovi kriptologija [2], dolazimo do sledeće definicije:

- *Kriptografija* je nauka koja se bavi svim oblicima sigurnosti transporta podataka i to: autentifikacija, digitalni potpis i razmena elektronskog novca. Kriptografija postoji i razvija se od kada postoji pisanje;
- *Kriptologija* je pak grana matematike koja se bavi praktičnom primenom metoda u kriptografiji.

Pored navedenog potrebno je napraviti, a za lakše pojmovno određenje i razliku između šifre (koja omogućava zamenu znak za znak, bit za bit) i koda (gde se jedna reč zamenjuje drugom rečju ili unapred dogovorenim simbolom. Kodovi se više ne koriste u praktičnoj primeni, ali bi svakako mogli naći svoje mesto u određenim situacijama, posebno kod primene u vojne svrhe.

Skup pravila kod imlementiranja bezbednosnih servisa naziva se šifarski sistem. Svaki šifarski sistem obuhvata transformaciju podataka, koji se nazivaju šifrovanje i dešifrovanje. Šifrovanje je postupak koji otvoreni tekst (informaciju) transformiše u šifrovane podatke (šifrat). Obrnuti postupak se naziva dešifrovanje, gde se vrši rekonstrukcija šifrata u otvoreni tekst. Vrlo bitna nezavisna vrednost koja se koristi kod šifrovanja odnosno dešifrovanja je ključ. Broj simbola predstavljaju ključ (dužina ključa) i zavisi od šifarskog sistema i predstavlja jedan od parametara sigurnosti sistema.

Kriptoanaliza se bavi razbijanjem šifri, odnosno nastoji da dođe do otvorenog teksta od šifrata, a bez poznavanja ključa šifrovanja [8]. U širem smislu kriptoanalizu možemo i posmatrati kao metodologiju koja nam ukazuje na slabostima kriptografskih elemenata. Različite tehnike kriptoanalize spadaju u napade i to uglavnom aktivne napade na informacioni sistem. Rezultat uspešne kriptoanalize je dobijanje originala bez ključa a na osnovu šifrata, čime se analizirani šifarski sistema smatra "probijenim".

Razvojem računarske tehnike, a pre svega procesora uz mogućnost obavljanja milion operacija u sekundi, dolazi do naglog razvoja kriptografije i tada se i razvijaju prvi standardi kod šifrovanja, i to DES (Data Encryption Standard). Kod ovog standarda obrađivao se blok po blok podataka i to tako da se proces šifrovanja ponavljao više puta nad istim blokom. Sa vremenom ovaj standard je postao posebno osetljiv na brute force napade. Nakon navedenog standarda razvija se AES (Advanced Encryption Standard), koji koristi 128 bitne blokove dužine ključa od 128 do 256 bita što ga čini otpornijim na napade [8].

¹ kriptografija dolazi od grčkih reči "kriptos" što znači tajna, skriven i reči "grafien" što znači pisati

Kao i kod informacionog sistema zadatak kriptografije je da tokom prenosa informacija obezbedi privatnost, odnosno poverljivost; integritet podataka; autentifikaciju i neporecivost.

Poverljivost u osnovi označava primenu tajnosti i omogućuje da je informacija dostupna samo autorizovanim korisnicima. Poverljivost se obezbeđuje od fizičke zaštite do primene matematičkih algoritama.

Integritet obezbeđuje da je prenet originalna poruka koja na prenosnom putu nije modifikovana niti izmenjena.

Autentifikacija obezbeđuje da podacima pristupaju lica kojima je poruka i namenjena odnosno da li je neko onaj za koga se i predstavlja.

Neporecivost je svojstvo koje obezbeđuje da su primaoc i predavaoc stvarno posredovali u komunikaciju i da nema mogućnosti izmene poruke tokom prenosa.

U cilju obezbeđivanja cilja kriptografije definišu se protokoli (ili algoritmi). Protokoli su pravila ponašanja entiteta u komunikaciji. U osnovi, vrši se određivanje izbora vrste algoritma koji će biti korišćen kod šifrovanja, odnosno dešifrovanja [2].

Na osnovu načina korišćenja ključa razvile su se dve vrste algoritama. Jedna je simetrična a druga asimetrična. Radi se o simetričnim i asimetričnim algoritmima kriptovanja. Razliku kod ovih algoritama se odnosi u tome da se kod simetričnih algoritama koristi isti ključ za enkripciju i dekripciju neke poruke a asimetrični algoritmi koriste različite ključeve za enkripciju i dekripciju iste.

Simetrični algoritmi imaju potrebu da se ključ čuva u tajnosti od neprijatelja. Za ove algoritme je vrlo karakteristično generisanje i distribucija ključeva, što zahteva dobro organizovane organizacione mere, tj. *politiku zaštite*.

Kod ovih sistema polazna osnova je da je ključ siguran i da isti poseduju samo strane u komunikaciji. Zbog visokotehnološkog razvoja, prvenstveno interneta, često se izvodi jedini mogući zaključak da su sigurni jedino izolovani računari van javne mreže.

Ove algoritme delimo u dve grupe i to: stream šifrovanje i blok šifrovanje. Stream se zasniva na tome da se enkripcija (šifrovanje) vrši po blokovima bit po bit, dok se blok šifrovanja enkripcija vrši po blokovima podataka tj. uzimaju se blokovi od više bitova (64, 128, 196, 256...), i oni se enkriptuju (dešifruju) kao celina. Dekripcija se vrši inverznim enkriptovanjem uz isti algoritam ali se podključevi koriste obrnutim redosledom.

Asimetrični algoritmi su algoritmi sa javnim ključem. Ono što je specifično za njih je da koriste dva ključa za enkripciju i dekripciju. Ideja je da se objavi jedan od ključeva koji je javni dok druga osoba jedino može otvoriti istu poruku sa svojim tajnim ključem.

U osnovi, simetrični algoritmi su brži i njihova implementacija na računaru se odvija brže od asimetričnih algoritama. Obično se asimetrični algoritmi koriste za enkripciju slučajno generisanog broja koji se koristi kao ključ za enkripciju originalne poruke metodama simetričnog algoritma. Ovo se još naziva i hibridna enkripcija.

2.4 Digitalni potpis

Služi nam kao potpis u stvarnom svetu i predstavlja naš potpis u istom. Svrha digitalnog potpisa je da potvrdi autentičnost sadržaja i da obezbedi identitet poruke (da poruka nije menjana na svom putu).

Osnovu čini sadržaj same poruke, gde pošiljaoc poruke primenom definisanog kriptografskog algoritma stvara digitalni zapis određene dužine, koji u potpunosti odražava sadržaj poruke.

Za digitalni potpis koriste se asimetrični algoritmi sa javnim i tajnim ključem na sledeći način. Pošiljaoc svoju poruku koju želi da pošalje šifruje svojim tajnim ključem koji je u stvari digitalni potpis. Primalac po prijemu poruke istu dešifruje javnim ključem pošiljaoca, kreira potpis i upoređuje ga sa primljenim potpisom. Ako su identični potpisi poruka je onda identična onoj koju je pošiljaoc i poslao, potvrda da je stigla identična poslata poruka.

2.5 Forenzika kao nauka

Forenzika ima za cilj davanje odgovora na pitanja od interesa za pravni sistem kroz primenu više nauka u istom cilju. Isto se vrši ukoliko se radi o kriminalu ili parničnim postupkom pred organima reda. Potiče od lat. Reči "*forēnsis*", što doslovno znači „pred forumom“. U rimsko doba, "krivična prijava" se podnosila javno predstavljanjem slučaja u forumu, tako što bi optuženi za krivično delo i tužilac govorili pred forumom. Osoba sa boljim argumentima i prezentacijom bi odnela pobedu pred forumom. U današnje vreme se termin forenzika prvenstveno odnosi na forenzičku nauku [19].

Prva upotreba Forenzike pripisuje se Arhimeđu (287-212. p.n.e.) koji je imao za zadatak da utvrdi da li je kruna koja je bila napravljena za kralja Hiera II, od čistog zlata ili je zlatar dodao još neki element u nju. Prvi pisani dokument o upotrebi medicine i entomologije u forenzuičke svrhe, pripisuje se knjizi Xi Yuan Lu (period od 1186–1249) koja je objavljena 1248. U jednom od slučaja osobe ubijene sa srpom istražitelj je rešio slučaj tako što je tražio da svi koji poseduju srpove iste donesu na jedno mesto. Nako što je na životinjskom lešu pravio rane srpovima upoređivao je otiske koje ostavljaju. Nakon što je predočio dobijene dokaze ubica je priznao zločin. Pored toga, knjiga sadrži savete o tome kako da se napravi ralika između davljenja (voda u plućima) i davljenja (polomljen vrat i hrskavica) zajedno sa drugim dokazima proizišlim iz ispitivanja leša i utvrđivanja da li je smrt prouzrokovana ubistvom, samoubistvom ili je reč o nesreći [23].

U Kineskoj kulturi za otkrivanje krivca korišćenja je metoda pljuvačke. Od osumnjičenih je traženo da napune usta sa suvim pirinčem i da ga potom ispljunu ili da na kratko ližu šipke vrućeg metala. Kod oba testa usta krivca proizvode manje pljuvačke. Optuženi se smatrao krivim ako se pirinač lepi za usta u izobilju ili ako nakon lizanja vruće šipke, jezik bude teško spaljen usled nedostatka pljuvačke koja bi mu pružila zaštitu.

Evropom tokom šesnaestog veka, vojni lekari su proučavali podatke o načinu i uzroku smrti kod vojnika. Ambroise Paré, Francuski vojni hirurg, je proučavao efekte nasilne smrti na unutrašnje organe. Dva Italijanska hirurga Fortunato Fidelis i Paolo Zachia postavili su temelje moderne patologije, proučavanjem promena u strukturi tela koje su se desile kao posledice bolesti.

1836 engleski hemičar James Marsh je koristio hemijske procese pri utvrđivanju uzroka smrti kao posledice trovanja arsenom.

Policija je počela da koristi otiske prstiju kao dokazni materijal kada je Juan Vucetich u Argentini rešio slučaj ubistva korišćenjem krvavog otiska prstiju koji se nalazio na uzorku skinutog odsecanjem dela vrata na kome su se otisci nalazili. 1909 Rodolphe Archibald Reiss (1875-1929) otvara prvu školu Forenzike u Lozani (Švajcarska).

Na razvoj forenzike poseban uticaj je imao pronalazak mikroskopa posebno kod DNK analize dokaza.

U skladu sa potrebama razvijeno je više naučnih disciplina forenzike i to: računarska, forenzička arheologija, forenzička fotografija, za nas najbitnija digitalna forenzika i druge.

2.6. Digitalna forenzika

Digitalna forenzika je uzbudljiva. Polje koje će imati snažan uticaj u raznim situacijama, uključujući unutrašnje korporativne istrage, građanske parnice, krivične istrage, prikupljanje obaveštajnih podataka i pitanja vezana za nacionalnu bezbednost [18].

Mobilna forenzika verovatno najbrže raste i razvija se kao digitalna forenzička disciplina, koja nudi značajne mogućnosti i mnogo izazova. Bitan deo mobilne forenzike podrazumeva učenje i analizu podataka iz uređaja gde je važno u startu dobro poznavati kako platformu, tako i alat koji će se koristiti tokom istrage. Dobro poznavanje i razumevanje će pomoći forenzičkom istražitelju uspešnu istragu i analizu na mobilnim uređajima.

Za više od tri decenije, razne kompanije su uložile značajna sredstva u istraživanje i razvoj prenosnih računarskih uređaja u nadi da će otvoriti nova tržišta. Kao i kod tradicionalnih računara, hardverske komponente su u središtu izrade prenosnih uređaja, koji su značajno napredovali i sada pružaju malu, moćnu, mobilnu platformu za prenosne računare.

Centralna figura u razvoju Android operativnog sistema je Endi Rubin, koji je kompaniju formirao 2003. godine pod nazivom Android.inc, gde će i operativni sistem koji se nalazi u delu mobilnih uređaja biti nazvan Android.

2.6 Uređaji koji koriste Android platformu

Smart telefoni (Smartphone)

Pametni telefoni predstavljaju najpopularnije Android uređaje. Od trenutka kada se počelo sa masovnom primenom ovih uređaja oni zauzimaju značajan segment tržišta mobilnih telefona koji brzo raste. Široko je prihvaćeno da android svojim besplatnim alatima i jeftinijom izradom pretenduje da tržište iPhone uređaja prestigne i postane najpopularnija platforma smart telefona [18].

Tablet računari

Predstavljaju prenosne računare sa ekranom osetljivim na dodir. Tablet računari u sebi sadrže više komponenti koje koriste radi obavljanja svoje primarne funkcije. Obično je tastatura na tablet računaru realizovana softverski, a može se koristiti i eksterna tastatura sepcijalno dizajnirana za korišćenje na uređajima sa Andorid operativnim sistemom. Postoje tablet računari koji u sebi sadrže i SIM kartice za podršku prenosa podatka putem interneta i računari bez SIM kartice uz podršku za bežično povezivanje preko bežične WiFi veze i Bluetooth veze i konekcije sa eventualno drugim eksternim uređajima.

Netbook

Netbok je mali, lagani računar koji ima manje procesorske snage nego Laptop računar, uz mogućnost da se koristi odnosno poveže na internet i obrađuje razne vrste dokumenata i tekstualnih sadržaja. Spada u ono što se često naziva "računar u malom". Netbook računari zbog svojim malih performansi (manji displej, tastatura i skladični prostor, odnosno memorija) ekspanzijom cloud-a nalaze svoju širu primenu[21].

Google TV

Je platforma bazirana na Android operativnom sistemu, razvijena od strane Googl-a i Logitech-a. Prvi uređaji bili su zasnovani na Intel procesorima arhitekture x86, dok je druga generacija ovih uređaja bila bazirana na ARM arhitekturi procesora koji su razvijanu sa Google web pretraživačem i ugrađuje se u smart uređaju [22].

Global Positioning System (GPS)

Global Positioning System (GPS) je alat koji omogućava korisnicima pozicioniranje, navigaciju i tajming (PNT) usluga. Ovo je trenutno jedini sistema koji je u potpunosti u funkciji preko 24 globalna poziciona satelita koji se nalaze u orbiti zemlje. GPS ima široku kako komercijalnu tako i usku primenu posebno u vojne svrhe, gde se u poslednje vreme koristi za navođenje raznih vrsta oruđa [18].

Danas je najpopularnija njegova komercijalna primena kod uređaja za navigaciju koji se nalaze ili ugrađeni u automobile, kamione i druga prevozna sredstva ili kao zaseban uređaj koji pruža potpuno pouzdano pozicioniranje na zemlji.

Drugi uređaji:

Sam pristup android platforme, od njegove dostupnosti, malih troškova održavanja, dostupnosti aplikacija, dovodi do razmatranja da se u druge uređaje ugrađuje andorid sistem. Neke za koje se očekuje da budu u skorije vreme integrisani su:

1. Kuhinjski uređaji;
2. e-readers čitači;
3. Medija plejeri;
4. Mašine za fotokopiranje;
5. Kućni telefoni, audio i video ramovi za fotografije;
6. Uređaji za igranje igrice i
7. Printeri.

Kao što se vidi razvoj andorid sistema će i u narednom periodu zaokupljati pažnju forenzičara zbog njihove šire primene android uređaja (ukoliko to nije slučaj već sada).

2.7 Alati za digitalnu forenziku

Radi uspešne forenzičke istrage najbitnije je razumevanje i efikasnost u upotrebi svih alata koji su na raspolaganju u cilju njenog uspešnog sprovođenja.

Poznavanje alata za foreničku analizu je bitan segment posebno kod izbora alata koji bi bio najpogodniji za odgovarajući posao, odnosno odgovarajuću istragu.

Alati koji su multifunkcionalni, odnosno mogu da se koriste u više faza istrage su najbolji jer pružaju više informacija, od mreža do podataka koji su korišćeni na uređaju nad kome se vrši istraga.

Neki od najpoznatijih alata sa širokom primenom je EnCase sa verzijom 7.10 [25], koja je prema podacima sa sajta najnovija, do nekih alata sa otvorenim, odnosno koji su besplatni [24]. EnCase je najkorišćeniji alat jer se isti priznaje na sudu kao pouzdani alat za forenziku digitalnih uređaja.

3. ZAŠTITA INFORMACIONIH SISTEMA

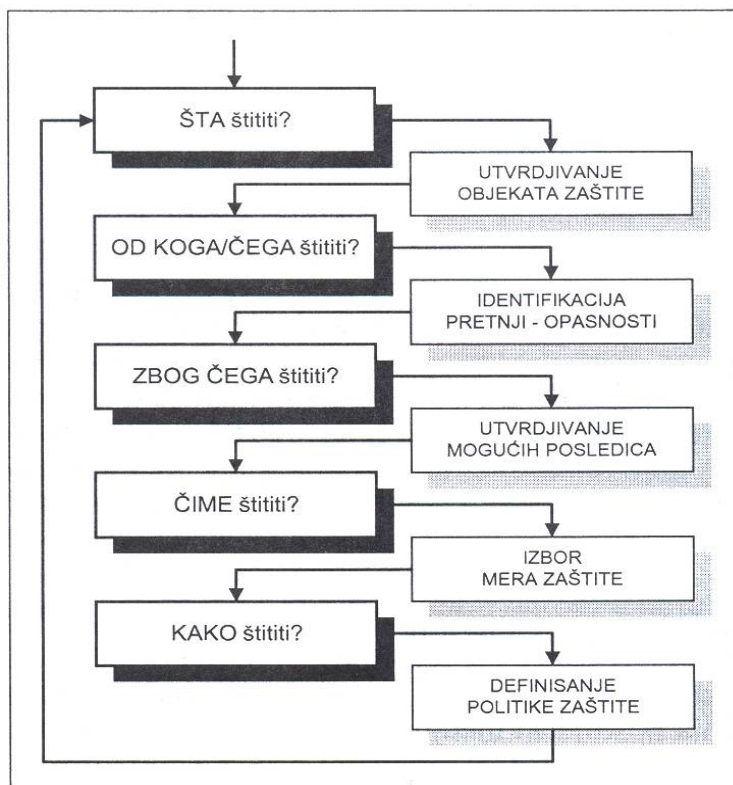
Zaštita informacionog sistema obuhvata radnje, mere i postupke u cilju zaštite podataka i informacionog sistema od nepredvidih događaja sa neželjenim posledicama [1].

U tom smeru je i sve veća potreba za onemogućavanjem svakog slučajno ili namernog narušavanja i sprečavanja funkcija računarskih sistema. Takođe, treba stvoriti i neophodne uslove za pravilno korišćenje unapred definisanih funkcija informacionih sistema. Kao osnova za nalaženje zadovoljavajućeg odgovora na pitanje zaštite informacionih sistema, polazimo od klasifikacije pretnji koje mogu ugroziti isti na: nesreće, greške i kriminal. Na bazi navedene klasifikacije data su četiri odgovora na pitanja gde se dobija delimična odgovor a njihovom sintezom i potpuniji odgovor, i to:

- Vrednost hardvera i softvera;
- Raznovrsnost funkcija računarskih sistema;
- Raznovrsnost, priroda i značaj podataka i informacija koje se u okviru računarskih sistema prikupljaju, uređuju, skladište, obrađuju, distribuiraju i arhiviraju;
- Karakteristike računarskih sistema.

Najpre je potrebno definisati cilj zaštite sistema, a to je da bilo koji sistem zaštite ima smisao samo ukoliko se nešto, od nečega i zbog nečega štiti, a da bi se isti postigao mora se na funkciju izvršavati sa nečim i na neki način. Rešenje ovako postavljenih ciljeva, odnosno pitanje je moguće uz logičke celine, a po principu "zlatnih pitanja" kriminalistike, kroz odgovarajuća "zlatna pitanja" informatičke zaštite i koja zahtevaju potpune odgovore.

Slika 2: "Zlatna pitanja"



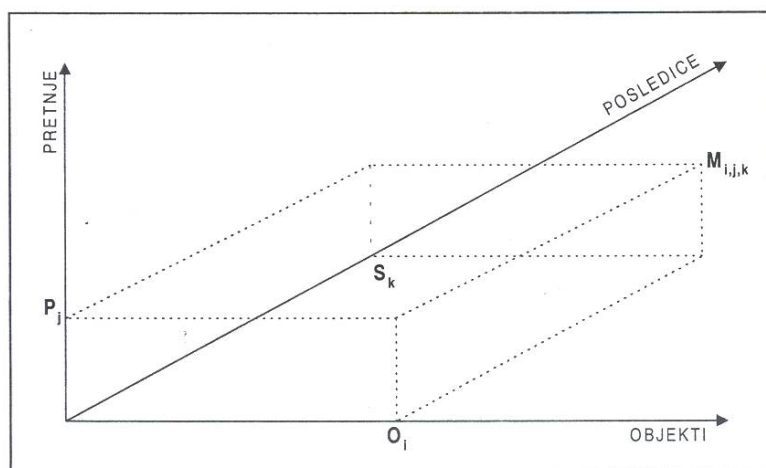
3.1 Glavni enteti problema zaštite

U oblasti informatičke zaštite, odnosno u oblasti informacionih sistema, glavni entiteti problema su: objekti, pretnje, posledica, mera i politika zaštite [1].

Radi konkretnije analize moguće je na sledeći način predstaviti problem zaštite kroz trodimenzionalnu matricu, na sledeći način.

Svaki element matrice M predstavlja skup mera koje bi trebalo primeniti u cilju sprečavanja posledice S_k , a koja može nastupiti ukoliko pretnja P_j ugrozi objekat O_i , odnosno:

$$M_z = M(O_i, P_j, S_k)$$



Slika 3. Trodimenzionalna matrica mera zaštite

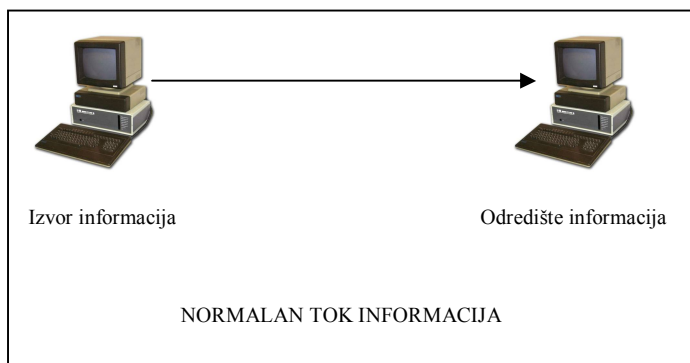
3.1.1 Objekti

Objekti, kao odgovor na pitanje “šta štititi?” je prvi korak u izvučavanju problema zaštite u računarskim, odnosno informacionim sistemima. U svakom informacionom sistemu postoji niz objekata čije je vrednosti potrebo zaštititi, i to: podatak, datoteka, baza podataka, fotografija, digitalni zapis slike i zvuka, softver, hardver itd...

3.1.2 Pretnje

Pretnje, kao odgovor na pitanje “Od koga” ili “Od čega” štititi, daje odgovor na pitanje koji sadrži rizike od objektivnih pojava kao što su vatra, voda, eksplozija itd., ali i specifične pretnje poput KEMZ-a (komprimitujućeg elektro-magnetnog zračenja). Procena mogućih gubitaka od KEMZ-a najčešće je nematerijalnog porekla a dokazivanje postojanja i procenu mogućih gubitaka, čini vrlo teškim. Među pojedinim pretnjama postoji uočena međuzavisnost koja usložava uticaj na informacioni sistem.

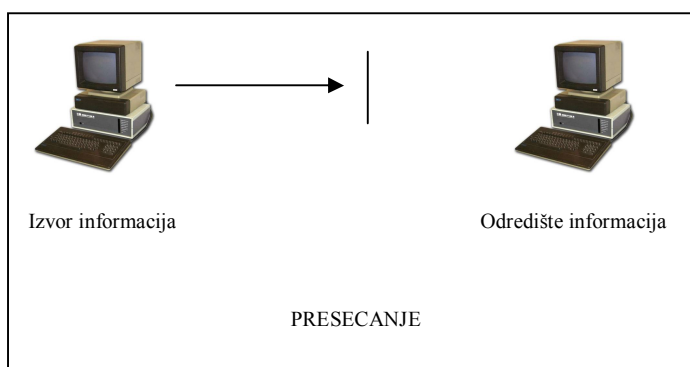
Slika 4. Normalan tok informacija



Za razliku od normalnog toka informacije u komunikacionom kanalu (slika 4), pretnje koje utiču na sam tok informacije u informacionim sistemima delimo u četiri kategorije, i to na presecanje, presretanje, izmena i fabrikovanje [4].

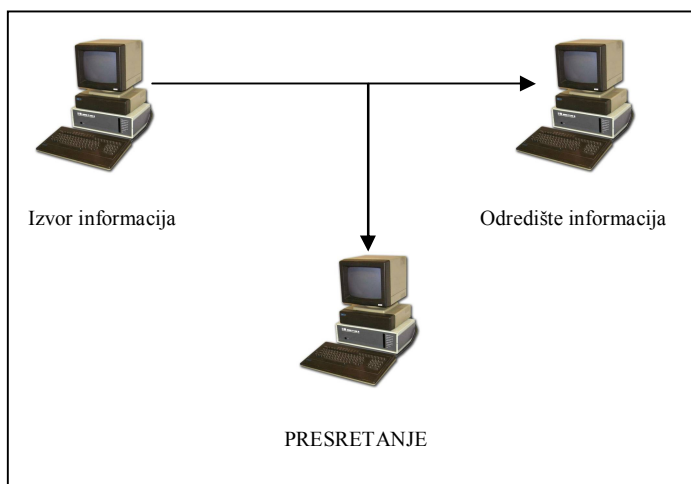
Presecanje ili prekidanje predstavlja napad na raspoloživost, a presecanjem se prekida tok u kretanju informacije, odnosno onemogućava se pružanje neke radnje ili uopšte funkcionisanje nekog sistema. Ovde se uglavnom radi o aktivnom napadu (slika 5).

Slika 5. Presecanje



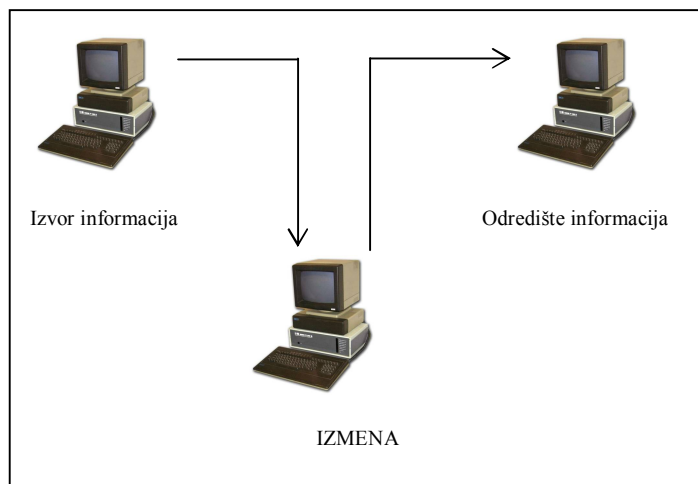
Presretanje, obuhvata napad na poverljivost i može se sprovoditi kao prisluškivanje saobraćaja, nadziranje intenziteta i uvid u samu poruku koja se prenosi i slično (slika 6). Ova vrsta napada spada u pasivne napade, teško se i otkriva jer ne menja podatke i ne utiče na unutrašnje funkcionisanje samog sistema. Ova vrsta napada može biti i pripremna faza za neki od aktivnih napada.

Slika 6. Presretanje



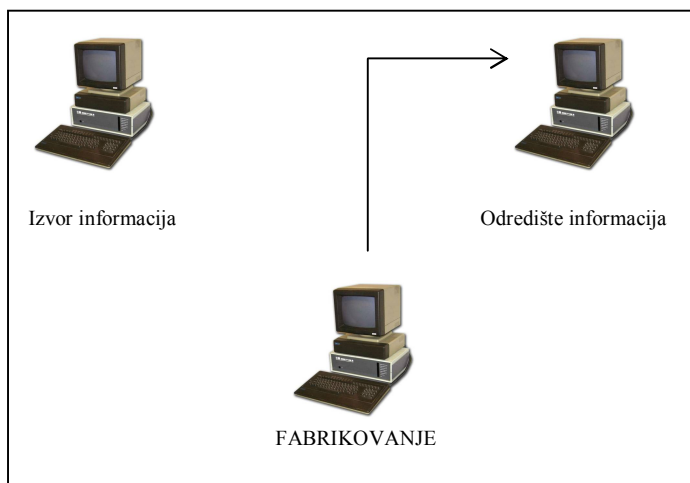
Izmena obuhvata napad na integritet sistema. Ovaj napad spada u aktivne napade a sprovodi se tako što se na prenosnom putu unutar sistema vrši izmena podataka sistema. Iako spada u aktivni napad koji vrše određene promene parametara sistema, vrlo često može biti i neprimećen izvesno vreme, a najčešće zbog složenih tehnika koje se koriste kod ove vrste napada (slika 7).

Slika 7. Izmena



Fabrikovanje predstavlja napad na autentičnost sistema. Naime, ovaj napad spada takođe u aktivne napade i to tako što generiše lažne podatke, saobraćaj ili izdaje neovlašćene komande. Za ovu vrstu napada je karakteristično lažno predstavljanje korisnika, usluga, servera ili nekog drugog sistema (slika 8).

Slika 8. Fabrikovanje



3.1.3 Posledice

Posledice kroz odgovor na pitanje “zbog čega štititi”, utvrđuju negativne posledice koje pretnje mogu da izazovu. One dovode do potpunog oštećenja, modifikacije hardvera i softvera, otkrivanje podataka, potpunog prekida rada sistema i slično. Sve navedeno dovodi do povećanja gubitaka a iste svakako treba smanjivati kroz predviđanje mogućih posledica [3] .

3.1.4 Mere

Mere kao odgovor na pitanje “Čime štititi?” gde identifikujemo sve mere koje nam stoje na raspolaganju za izgradnju celovitog i pouzdanog sistema zaštite. Mere razvrstavamo na [1]:

Normativne mere- Odnosi se na pravne, organizacione i kadrovske sa osnovnom karakteristikom a posebna bitna je pravo pristupa i korišćenja podataka koji znatno doprinose povećanju raspoloživosti sistema i njegove produktivnosti.

Fizičko-tehničke, u odnosu na sam projektovani sistem informacija pored troškova koji se znaju prilikom njihovog uspostavljanja potrebni su i troškovi održavanja istih. Ovi troškovi se mogu isplanirati u skladu sa finansijskim mogućnostima, međutim efikasnost ovih mera opada ukoliko nisu u potpunosti i na adekvatan način primenjene normativne mere (fizičko obezbeđenje IS, Faradejev kavez, krypto uređaji i slično).

Logičke mere su vrlo bitno sredstvo zaštite u informacionim sistemima. Ovim merama se pristupa krajnje odgovorno, smišljeno i racionalno, tim pre što direktno utiču na smanjenje raspoloživosti i smanjenje efikasnosti računarskog sistema.

Kriptološke mere kao vrlo značajne mere u kombinaciji sa merama od KEMZ-a omogućavaju vrlo visok i efikasan način zaštite u informacionim sistemima. Međutim i kod ovih mera efikasnost znatno opada ukoliko nisu normativne mere primenjene adekvatno.

3.1.5 Politika

Politika koja daje odgovor na pitanje “Kako štititi” što predstavlja način za utvrđivanje strategije za upravljanje rizikom, a nakon čega se pristupa procesu analize i procene rizika.

3.2 Analiza i procena rizika

Kroz analizu međuzavisnosti rizičnih događaja, uticaj na pojedine događaje ili njihove kombinacije na sistem određuju verovatnoću nastajanja rizika što obuhvata **analizu i procenu rizika**.

Analiza se vrši pomoću kvantitativne analize i kvalitativne procene.

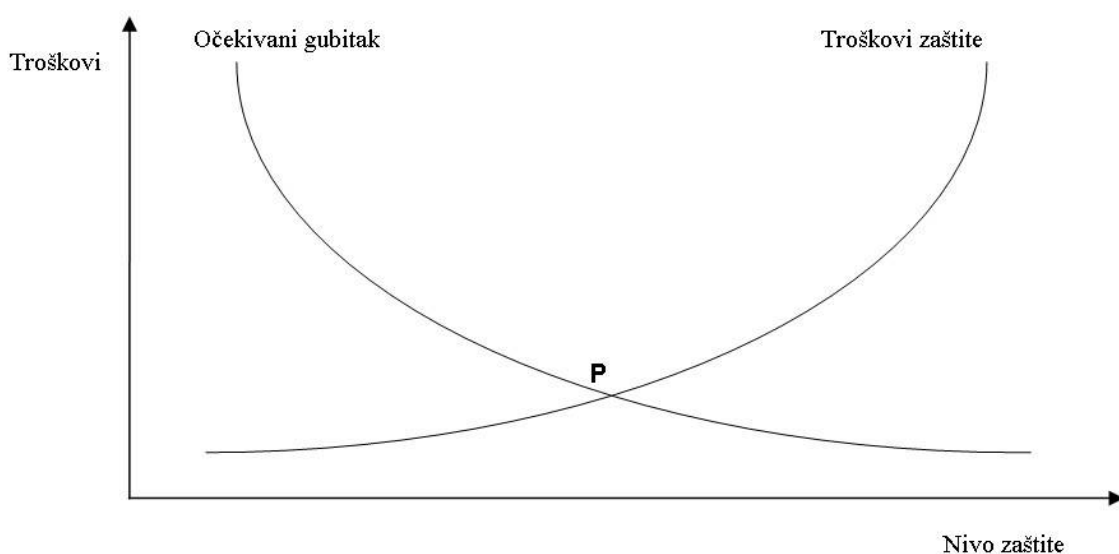
Kvantitativna analiza obuhvata analizu gde rizik predstavljamo kvantitativnim merilima, odnosno kao uticaj rizika na ciljeve određenog projekta i verovatnoće da do tih neželjenih događaja i dođe.

U odnosu na nivo rizika, koji može biti nizak, umeren ili visok vrši se verovatnoća mogućih promena u sistemu. U faktore rizika ubrajaju se: Sam rizičan događaj; Verovatnoća pojavljivanja rizičnog događaja; Obim gubitka koji može da nastane ako se rizični događaj i ostvari.

Za kompleksniju analizu rizika koriste se metode izražene kroz određene jednačine, uz određene kategorije rizika i pretnji uz korišćenje tzv. Matrice.

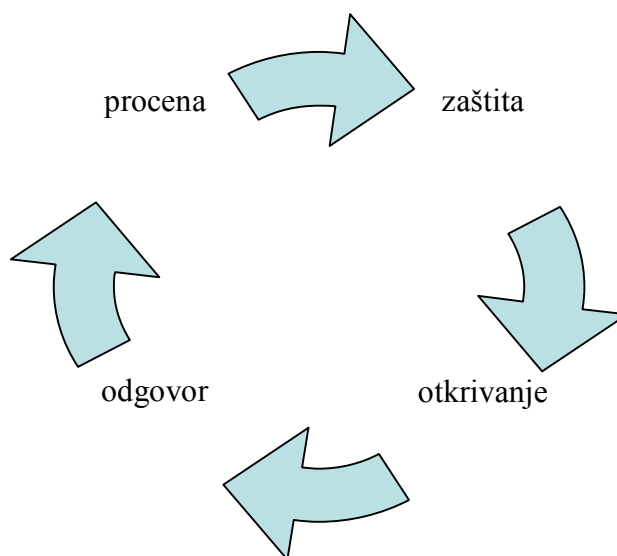
3.3 Sigurnost

U informacionom sistemu sigurnost definišemo kao proces održavanja prihvatljivog rizika i resurse za ostvarivanje navedenog procesa. Ovo u osnovi znači kompromis između ulaganja u informacioni sistem i smanjenja štete i posledice uz smanjenje mogućnosti nastanka štete. U osnovi, veće ulaganje u sigurnost nesumnjivo smanjuje izloženost sistema riziku ili same računarske mreže, što je u direktnoj vezi sa većim troškovima i utiče na smanjenje profitabilnosti vlasniku. Ovo ukazuje na neophodnu ravnotežu između ulaganja i sigurnosti što se grafikom predstavlja kao na sledećoj slici:



Slika 9. Odnos potencijalnog gubitka i troškova zaštite

Sigurnost kao proces se zasniva u četiri koraka, procena (planiranje), zaštita (sprečavanje), otkrivanje i odgovor [3].



Slika 10. Proces sigurnosti

Procena je u direktnoj vezi sa normativama, a sama greška u proceni direktno utiče na sve ostale procese.

Zaštita podrazumeva sistem podmera radi smanjenja mogućnosti ugrožavanja informacionog sistema. Ukoliko dođe do propusta u zaštiti primenjuje se sledeći korak, otkrivanje.

Otkrivanje je proces gde je bitna identifikacija napada, odnosno povrede sigurnosnih pravila na nezakonit, neovlašćen način koji je preduzet nad nekim računarskim sistemom.

Odgovor je oporavak od posledica napada. Ranije je bilo najbitnije vraćanje rezervnih kopija oštećenih podataka tokom upada, dok se u novije vreme sve više koriste pravna sredstva (podnošenje krivične prijave protiv lica koje protivpravno upada u sistem), među koje spada prethodno prikupljanje dokaza merama digitalne forenzike u cilju obezbeđivanje relevantnih podataka o samom napadu posledicama koje je ostavio na sistem.

Prilikom uspostavljanja sistema zaštite treba težiti uspostavljanju ravnoteže između veličine rizika i nivoa zaštite koji može biti standardni, srednji, viši i najviši nivo uz naravno sagledavanje troškova.

Sigurnosni ciljevi se sagledavaju kroz trojstvo sigurnosti, od engleske skraćenice koja je slična i najvećoj obaveštajnoj agenciji SAD, CIA (Confidentiality, Integrity, Availability). Ovaj sistem predstavlja tri osnovna principa informacione bezbednosti [3].

Poverljivost – cilj je sprečavanje namernog ili nenamernog neovlašćenog otkrivanja sadržaja poruka. Može se narušiti na više načina a jedan od načina je loše definisani sigurnosni protokoli i pristup mreži od strane neautoarizovanog entiteta.

Integritet – cilj je obezbediti da se podaci ne smeju menjati od strane neovlašćenih lica odnosno procesa i ovlašćena lica odnosno procesi ne smeju vršiti neovlašćenu promenu podataka.

Raspoloživost – cilj je obezbediti da procesi odnosno lica mogu pouzdano pristupiti resursima sistema, odnosno podacima. U osnovi predstavlja pretpostavku da su sistemi podignuti i da rade kao što je predviđeno.

Sigurnosna usluga u sistemu ima zadatak da poveća sigurnost samog sistema. U stvari sigurnosnu uslugu čine mehanizmi koji imaju za cilj predupređivanje napada, sanaciju štete i slično.

3.4 Metode zaštite

Pristup metodama zaštite zavisi od nekoliko podela, a sa vremenom se menjaju sa razvojem informaciono komunikacionih tehnologija. Mi ćemo se baviti sa pristupom četiri grupa metoda zaštite [3]: kriptografske metode, programske metode, organizacione i fizičke metode.

Budući da se ova podela smatra prevaziđenom i prihvaćena je podela koju je definisala organizacija (ISC)² i ima deset domena sigurnosti. Neki autori metode odbrane klasifikuju na sledeći način: šifrovanje, softverska kontrola pristupa, hardverska kontrola pristupa (pametne kartice ili bimoetrija), pravila zaštite ili zaštitne polise (promena lozinke se zahteva u sistemu) i fizičku kontrolu pristupa.

Aspekti zaštite podrazumevaju više nivoa, a definišu se u odnosu na položaj mehanizma zaštite u informacionom sistema zaštite na: zaštitu na nivou aplikacije, zaštitu na nivou operativnog sistema, zaštitu na nivou mrežne infrastrukture i proceduralna i operaciona zaštita.

Zaštita na aplikativnom nivou- predstavlja područje za razvoj sopstvenih sistema za zaštitu komunikacije iz tog razloga što nije potrebna kompatibilnost sa protokolima viših nivoa. U zavisnosti od nivoa zaštite koji nude korišćeni algoritmi, procedure i okruženje u kome se sistem primenjuje, zavisi bezbednost sopstvenog sistema zaštite [8].

Zaštita na nivou operativnog sistema – ovaj aspekt zaštite tiče se samog operativnog sistema koji je veoma složen i u veoma obiman [3].

Zaštita na nivou mrežene infrastrukture – misli se na primenu mrežnih barijera (firewall), blokiranje nepotrebnih portova itd.

Proceduralna i operaciona zaštita – obuhvata definisanje i sprovođenja pravila zaštite, detekciju napada, prediktivno reagovanje, preventivne mere i slično.

² International Information System Security Certification Consortium – nekoliko severnoameričkih profesionalnih udruženja.

4. PRIMENA KRIPTOGRAFIJE U ZAŠTITI INFORMACIONIH SISTEMA

4.1 Primena simetričnih algoritama

Najpoznatiji simetrični algoritam je DES (Data Encryption Standard), koji je razvijen od strane IBM-a 1977. godine. Njega zamenjuje AES (Advanced Encryption Standard), a kao glavni razlog njihove zamene je taj što AES koristi ključeve veće dužine. U osnovi simetrična kriptografija koristi se tajnim ključem i to istim i za enkripciju i dekripciju podataka.

Kod prenosa informacija gde koristimo jedinstveni ključ moguć je napad pod nazivom **brute-force attack**, koji podrazumeva isprobavanje svih mogućih kombinacija tajnog ključa sve dok se ne pronađe korišćena kombinacija, odnosno razbije šifra i otkrije tajni ključ koji se koristi za otključavanje svih poznatih kriptograma.

Od poznatih simetričnih algoritama izdvojio bih *Lucifer*, *DES*, *TRIPLE DES* i *2-KEY 3DES* a zatim.

4.2 Primena asimetričnih algoritama

Asimetrični šifarski sistemi nastaju kao odgovor na problem distribucije ključeva tajnih simetričnih ključeva i njihovu potrebu da obe strane u komunikaciji poseduju isti tajni ključ. U teoriji se može još naći i kriptografija sa javnim ključem ili kriptografija sa 2 ključa [2]. Koristi se za efikasnu autentifikaciju, integritet i neporecivost.

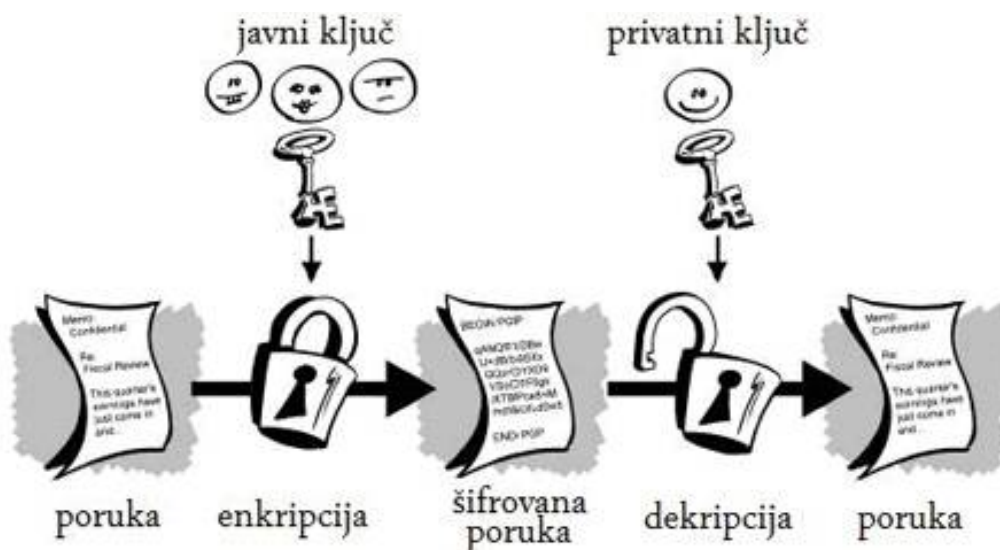
Problem distribucije tajnih ključeva kod simetričnih sistema je dosta skup proces, koji može da obezbedi samo država koja raspolaže dovoljnom količinom novca, međutim pošto distribucija simetričnih ključeva zahteva novac nije za komercijalnu, odnosno javnu upotrebu.

Sistem kriptovanja pomoću asimetričnih ključeva su 1976. godine objavili Vitfield Difi i Martin Helman, koji su, pod uticajem radova Ralfa Merkla o razdeljivanju javnih ključeva, objavili metodu usaglašavanja pomoću javnog ključa. Ova metoda razmene eksponencijalnih ključeva, koja je postala poznata pod nazivom "razmena ključeva Difi-Helman", bila je prva praktična metoda uspostavljanja sigurne veze preko nezaštićenih kanala bez unapred dogovorenog ključa. Merkllova tehnika usaglašavanja pomoću javnog ključa je postala poznata pod nazivom „Merklove zagonetke“ i objavljena je 1978. godine [11].

Pored uobičajenog kriptovanja poslatih poruka, asimetrična kriptografija se koristi i za digitalne potpise: određena poruka može biti potpisana privatnim ključem, a svi koji je prime mogu, pomoću javnog ključa, utvrditi da li je poruka poslata od prave osobe i da li je u netaknutom stanju tj. nepromenjena. Većina algoritama za asimetričnu kriptografiju je relativno zahtevna u kontekstu broja izvedenih računskih operacija u odnosu na algoritme za simetričnu kriptografiju sa naizgled sličnom pruženom sigurnošću.

Ta činjenica je vrlo važna za njihovu praktičnu upotrebu. U većini slučajeva se koriste hibridni ili mešani sistemi kriptografije da bi se dobila i brzina i sigurnost.

Slika asimetrične kriptografije ilustruje sve napred navedeno u pogledu načina korišćenja metoda javnog i tajnog ili privatnog, ključa kod prenosa poruke.



Slika 11: Šema asimetrične kriptografije³

Asimetrični algoritam (algoritam sa javnim ključem) se koristi za [2]:

- 1.- šifrovanje i dešifrovanje (poverljivost),
- 2.- digitalni potpis (autentifikacija) i
- 3.- razmenu simetričnog ključa.

4.3 RSA algoritam

RSA prvenstveno je namenjen za šifrovanje podataka, a danas se koristi i u sistemima elektronskog potpisa. RSA danas predstavlja industrijski standard u oblasti asimetrične kriptografije i zaštite podataka, a našao je svoju široku primenu u mnogim sigurnosnim protokolima i sistemima elektronskog poslovanja. Ime je dobio od početnih slova svojih tvoraca Ronald Rivesta, Leonarda Ejdlmana i Adi Šamira.

Primer razmene poruke RSA algoritmom se vrši na sledeći način [4]:

Na strani slanja poruke biraju se veoma veliki prosti brojevi p i q , gde p mora da bude različit od q .

Zatim se računa proizvod brojeva p i q , tako da dobijemo

$$n = p \times q$$

Pored navedenog na strani pošiljaoca se vrši izračunavanje nove funkcije

³ Preuzeto sa sajta Wikipedia, http://security.foi.hr/wiki/index.php/Osobna_kriptografija_-_GPG,_TrueCrypt,_SSL

$$f = (p-1) \times (q-1)$$

Nakon toga na strani pošiljaoca se bira proizvoljni broj e , tako da je

$$d \times e = 1 \bmod f$$

Na strani pošiljaoca se f i d čuvaju u tajnosti.

Šifrovanje poruke se vrši na sledeći način, odnosno na strani pošiljaoca se obavlja sledeće u cilju dobijanja šifrata:

$$C = P^e \bmod n$$

Ovako poslat šifrat na strani primaoca obavlja dešifrovanje na sledeći način;

$$P = C^d \bmod n$$

Konkretni primer primene asimetrične kriptografije RSA algoritma dat je u primeru broj 31 "RSA šifrovanje i dešifrovanje" [2].

4.4 Hibridni algoritmi

Tvorac ovog algoritma je Fil Cierman, a nastao je kao odgovor na narušavanje lične privatnosti, usled razvoja informaciono telekomunikacionih tehnologija i u nastojanju vlada i država da se sve stavi pod "kontolu". Inače, Fil Cierman je bivši agent NSA (američka agencija za nacionalnu bezbednost) [15].

PGP (Pretty good privacy) algoritam kombinuje neke od najboljih karakteristika obe navedene konvencionalne i kriptografiju javnog ključa, zbog čega i predstavlja hibridni kriptosistem. Kada pošiljaoc šifrjuje otvoreni tekst, on najpre kompresuje otvoreni tekst, a zbog uštede vremena modema za prenos i uštede prostora na disku za smeštanje podataka i kao najbitnije jača kriptografsku sigurnost. Kompresija smanjuje model otvorenog teksta i povećava otpornost na kriptanalizu. Mali paketi se ne pakuju već se ostavljaju u izvornom obliku [13].

Nakon toga PGP pravi privremeni ključ, odnosno slučajni broj koji se generiše pokretima miša i pritiskanjem tastera na tastaturi. Ovako definisani ključ ima jednokratnu upotrebu a koristi se za kriptovanje simetričnom kriptografijom. Zatim se šifrjuje privremeni ključ koji se pridružuje šifrovanim podacima. Dešifrovanje poruke se vrši obrnutim redosledom, gde se pomoću tajnog koda najpre dešifrjuje privremeni ključ, a onda se uz pomoć njega dešifrjuje i primljena poruka.

Slika, odnosno dijagram kako se odvija napred navedeni proces šifrovanja i dešifrovanja kod PGP hibridne kriptografije dat je u primeru, gde je potpuno grafički predstavljen na već opisani način, figure 1-4 i figure 1-5 [13].

Razlog zašto je nastala hibridna enkripcija se ogleda u brzini, jer je hibridna i do hiljadu puta brža od asimetrične, zbog čega je i izvršeno kombinovanje simetrične i asimetrične enkripcije (šifrovanja).

PGP koristi asimetričnu enkripciju i pruža i mogućnost digitalnog potpisivanja dokumenata. Kod PGP se umesto šifrovanja celog dokumenta šifruje samo kontrolni kod dokumenta. Naime, bilo kakva promena dokumenta menja i njegov kod i samim tim nam ukazuje da je na putu vršena izmena poruke.

4.5 Digitalni potpis i sertifikat

Sa konceptom potpisa smo svi upoznati. Potpisati dokument znači da je nastao ili da je odobren sa naše strane. Potpis je dokaz da dokument koji primi primalac dolazi od pošiljaoca u komunikaciji, odnosno od ispravnog entiteta (osobe ili računara). Primer kada kupac potpisuje ček, banka mora da bude sigurna da je ček izdao taj kupac i niko drugi. Drugim rečima, potpis na čeku označava njegovu verifikaciju a kada bude verifikovan predstavlja njegovu autorizaciju. [4].

Dalje se može razmatrati i razlika kod konvencionalnog i digitalnog potpisa, gde mi kod konvencionalnog na jedan način potpisujemo ček, na drugi ugovor u banci itd. Dok je digitalni potpis jedan jedinstveni i ne može biti drugačiji inače nije verifikovan i autentičan.

Na ovaj način dolazimo do definicije da je digitalni potpis postupak kojim se određeni segment bloka podataka, ili poruke koja se prenosi obeležava kriptografski potpisnikovim tajnim parametrom [14].

Digitalni potpis se formira tako što se primenom algoritma najpre određuje otisak poruke. Nakon tako određenog otiska se šifruje na strani pošiljaoca svojim privatnim ključem, uz primenu RSA algoritma. Šifrovani deo otiska predstavlja potpis poruke i pridružuje se istoj. Da bi se dokument potpisao koristi se Hash funkcija softvera⁴.

Zatim se softverski otisak transformiše u digitalni potpis uz pomoć tajnog ključa pošiljaoca. Ovako formiran digitalni potpis dodaje se poruci i on je jedinstven i za poruku i za privatni ključ koji ga je kreirao.

Verifikacija digitalnog potpisa se obavlja u tri faze: izdvajanje digitalnog potpisa iz poruke; kreira se otisak informacionog dela poruke istim postupkom kao pošiljaoc; na kraju se vrši poređenje otiska sa dobijenim otiskom iz poruke i ako je isti, verifikacija se smatra uspešnom.

Digitalni potpis ima za cilj da garantuje autentičnost, integritet i neporecivost.

Digitalni sertifikat je u konačnom elektronski dokument koji izdaje sertifikaciono telo (Certification Authority - CA). Smatra se i digitalnom ličnom kartom, jer sadrži podatke o korisniku sertifikata i podatke o izdavaocu sertifikata.

⁴ sabija proizvoljnu poruku na fiksnu veličinu, i koristi se za otkrivanje promena u poruci. U osnovi predstavlja sumu, a u kriptografiji cilj je jedan heš jedna poruka.

To je uverenje kojim se potvrđuje veza između podataka za verifikaciju elektronskog potpisa i identiteta potpisnika, koji je izdat od strane akreditovanog sertifikacionog tela [10].

Sertifikaciono telo garantuje tačnost podataka u sertifikatu tj. garantuje da javni ključ koji se nalazi u sertifikatu pripada korisniku čiji su podaci navedeni u tom istom sertifikatu i javno je dostupan na internetu, zbog toga što se u okviru sertifikata nalaze javni ključevi korisnika sertifikata, distribucijom sertifikata se distribuiraju i javni ključevi.

Digitalni sertifikat čini verzija formata sertifikata (najpoznatiji i najzastupljeniji je X.509 standard), serijski broj, identifikator algoritma, naziv i rok važnosti sertifikata, vlasnika sertifikata, polje dodatnih atributa (broj telefona, e-mail i slično), informaciju o javnom ključu vlasnika i digitalni potpis sertifikata.

4.6 Kriptoanaliza

Nasuprot kriptografiji, kriptoanaliza⁵ je nauka koja se bavi dekodiranjem ili popularno razbijanjem šifri, uopšte dolaženjem do kriptografskih protokola. Različite tehnike kriptoanalize su u stvari napadi, a iste delimo na aktivne i pasivne. Pasivnim napadom se samo *prisluškuje* poruka, dok se aktivnim napadom uključuje maskiranje, menjanje poruke ponovno slanje i DoS (Denial of Service) napade.

Skoro svi programi za enkripciju umesto brojeva kao ključa, koriste niz slova i brojeva, tj lozinku. Svi ovi algoritmi su u velikom stepenu sigurni uz postojanja mogućnosti da se lozinka otkrije ako se ne pridržavamo nekih pravila pri njenoj izradi.

Napad pri kome kriptoanalitičar koristi samo šifrat je najčešći. Do podataka za ovu vrstu kriptoanalize kriptoanalitičar može relativno lako doći, ali uspešan napad je veoma težak i zahteva veliki šifrovani uzorak poruke koja se prenosi. Kod napada gde kriptoanalitičar poseduje i nešifrovani i šifrovani podatak je druga vrsta napada. Ove dve vrste su, u stvari, napadi na sam algoritam, a u praksi se češće koriste napadi na lozinku. Takvi napadi su veoma spori i potpuno efikasni.

Evo nekoliko pravila prilikom smišljanja lozinke:

Idealno je da se za lozinku uzme niz slučajnih brojeva i slova. Pri tom bi trebalo da se koristi više od jednog niza slučajnih slova i brojeva. Ovakve lozinke izbegavamo jer su teške za pamćenje i upotrebljavaju se reči iz svakodnevnog govora. U tom slučaju potrebno je pridržavati se sledećih pravila:

- Ne koristiti reči koje se lako mogu pogoditi kao što su: godina rođenja, devojčko prezime majke (ili supruge), ime deteta, supružnika, roditelja, bliskog rođaka, kućnog ljubimca i slično;
- Potrebno je koristiti više od jedne reči.
- Najbolja lozinka može biti deo citata iz neke knjige ili neka rečenica koja nema smisao;

⁵ Potiče od grčke reči *kryptós* (skriveno) i *analýein* (razmrsiti).

5. FORENZIČKA ISTRAGA RAČUNARA

5.1 Istraga i akvizicija digitalnih podataka

Forenzička istraga kompjuterskog sistema se deli na zvaničnu i korporacijsku. Zvanična se još zove i javna dok se korporacijska naziva još i tajna digitalna forenzička istraga. Sa strane forenzike, bilo da se vrši analiza računara sa kojeg je izvršen napad, računara preko koga se posredovalo u izvršenju napada ili samog računara koji je napadnut, vrši se istraga pojedinačnog računara koji se u istrazi ispituje i naziva se ispitivani računar [16].

Suštinski, digitalni forenzičar kod istrage neophodno tesno sarađuje sa drugim licima, obično licima zaduženim za bezbednosnot računarskih mreža, koji pružaju neophodnu pomoć prilikom izvođenja digitalnih dokaza, posebno specijalisti za upravljanje kompjuterskim incidentom, a to su lica koja odlično poznaju sistem i računar koji se ispituje (IDS/IPS, firewalls itd).

Neophodni koraci pre početka istrage su sledeći:

1. prijava incidenta, odnosno krivičnog dela (bez obzira da li je pre toga vršena korporacijska analiza ili ne);
2. Razmatranje da li ima dovoljno podataka za početak digitalne istrage (lozinka računara, vlasnik računara, softver);

U osnovi, zahteva se pre početka istrage uglavnom da se iz računara izvuče sve što se može, a da se kasnije analizom obuhvati deo koji je neophodan.

Kada analitičar prihvati istragu pristupa sledećem:

1. Razmatra mogućnost angažovanja drugih lica, eksperata posebnih platformi (Linux, Unix i td.), kao i pravljenje prioriteta u radu ukoliko se u istragu uzima više računara, pravi strategiju pristupa podacima i akviziciji ciljnih računara (ukoliko se radi o fajl severu, proksi serveru i td.);
2. pravljenje imidža na forenzičkom računaru;
3. izbor forenzičkog alata;
4. koji se tip dokumenata traži na računaru, odnosno šta je cilj istrage (dokumenta, slike, ključne reči i druge informacije koje se dobijaju od zvaničnog organa istrage;
5. bekapovanje (kopiranje) originalnog imidža skinutog sa diska.

Nakon ovako prikupljenih podataka od strane analitičara i ustupljenih poznatih podataka od strane zahtevaoca istrage, pristupa se radu na istrazi konkretnog računara.

5.2 Isključivanje računara i SWAP fajl

U nijednom sistemu ne postoji zlatno pravilo kod pristupa istrazi, a jedino je pravilo je da se računar koji je oduzet u predistrazi ne uključuje. Uključeni računar obavlja brojne operacije prilikom rada i može doći do gubljenja značajnih podataka bitnih za istragu računara.

Postupanje sa računarom zavisi od platforme, odnosno operativnog sistema koji je instaliran na analiziranom računaru. Kod Windows operativnog sistema postoje tri načina, i to:

1. normalno isključivanje;
2. korisnički definisano isključivanje; i
3. nasilno isključivanje napajanja.

Svaki od načina isključivanja izaziva promene u fajlovima samog sistema, posebno swap fajlu koji je vrlo značajan u samoj akviziciji računara za razumevanje preduzetih procesa od strane korisnika računara u momenu koji je bitan za rezultat istrage. Naime, neophodno je dobro poznavanje svih koraka u radu računara kod ovog sistema a radi uspešne istrage podataka.

Swap fajlovi su kod Windows-a vrlo značajni, a radi se o privremenim fajlovima koji se koriste za brzu razmenu u sistemu, a za analitičara odnosno forenzičara predstavljaju zlatni rudnik istrage. Postoje dve vrste swap fajlova, i to privremeni koji nastaju kada se zatvara Windows i permanentni koji nastavlja da postoji kada je sistem isključen. Zbog korišćenja skupih RAM memorija i njihove adekvatne upotrebe omogućena je upotreba swap fajlova, gde se deo podataka iz RAM memorije prepisuje u swap fajlove koji se smeštaju na hard disku zbog čega i predstavljaju značajan izvor podataka za forenzičare prilikom istrage računara. Kod starijih operativnih sistema ovaj fajl se zvao WINDOWS386.SWAP, u novijim je to PAGEFILE.SYS i smešten je u rutu particije C na disku.

5.3 Korišćeni termini u forenzičkoj istrazi

Digitalni dokazi se definišu kao svaka informacija koja ima dokaznu vrednost koja je uskladištena ili prenesena u binarnoj formi. Digitalni dokaz uključuje kompjuterski dokaz, digitalni audio, digitalni video, mobilni telefon, digitalnu fax mašinu itd. Digitalni dokaz je informacija preneti u digitalnom obliku na koju se sud može osloniti [17].

Akvizicija digitalnih podataka počinje onog momenta kada su podaci neophodni za istragu prikupljeni i uskladišteni.

Objekti ili informacije podataka su podaci koji imaju potencijlanu dokazujuću vrednost. Objekti podataka se mogu pojaviti u formatima raznih vrsta, ali se ne sme menjati originalna informacija.

Fizički predmeti su predmeti u kojima mogu uskladištiti objekti podataka ili informacija i sa kojima objekti mogu biti preneseni.

Originalni digitalni dokaz su fizički predmeti i objekti podataka pridruženi tim predmetima u vreme akvizicije ili privremenog oduzimanja predmeta.

Duplikat digitalnog dokaza je precizna digitalna reprodukcija svih objekata podataka koji se sadrže u originalnom fizičkom predmetu.

Kopija digitalnog dokaza je precizna reprodukcija informacija koje su sadržane u originalnom fizičkom predmetu.

Prilikom sprovođenja istrage neophodno je održati efikasni sistem kontrole kvaliteta kod akvizicije, upravljanja i forenzičke analize dokaza. Standardna procedura ili skraćenica SOP (Standard Operation Procedure) je uputstvo za kontrolu kvaliteta celokupnog postupka istrage, akvizicije i upravljanja forenzičkom analizom digitalnih dokaza. SOP mora da obuhvati beleženje svih aktivnosti istraga kao i eventualno korišćenje drugih prihvaćenih procedura, opreme i materijala.

Strukturno, SOP sadrži: naslov, namenu, opremu, opis procedure, kalibraciju, kalkulaciju, ograničenja, sigurnost i reference. U osnovi SOP je vrlo značajan za agencije koje se bave forenzičkom istragom posebno kod ispunjavanja standarda i kriterijuma.

5.4 Standardizovana procedura

Standardizovana procedura privremenog oduzimanja računara kao dokaznog materijala, kod digitalne istrage zbog značaja potencijalnih izvora podataka i njihove osetljivosti određena je procedura koja se sastoji u sledećem [2]:

1. Pretraga mesta krivičnog dela kompjuterskog kriminala;
2. Integritet digitalnih podataka;
3. Izveštaj o procesuiranju i strukturi osumnjičenog HD;
4. Identifikacija ispitivanog materijala;
5. Uspostavljanje lanca čuvanja digitalnih dokaza;
6. Uslovi čuvanja digitalnih dokaza;
7. Procedura procesuiranja dokaza sa HD; i
8. Identifikaciono označavanje ostalih medija za skladištenje (osim HD);

Pored navedenog, neophodno je tokom istrage kompjuterskog kriminala obezbediti kopije dokaza za potrebe tužioca, advokata odbrane i drugih potražioca tokom vođenja istrage.

Osnovnom procedurom digitalne forenzike, poznate pod nazivom Daubert Gudlines, uslovi za prihvatljivost digitalnih dokaza pred sudom su sledeći:

1. Moguće je izvođenje dokaza po zahtevu suda;
2. poznat je stepen grešaka koje unosi sama procedura i može se dokazati;
3. Objavljen u vrhunsom višestruko recenziranom naučnom časopisu i da se prihvata u relevantnim naučnim krugovima.

Najveći stepen razumevanja je zahtev da je za primenjeni alat poznata greška koja se unosi tako da bi se na zahtev suda isti mogao dokazati. Do danas je nekoliko alata podvrgnuto ovoj proceduri a poznatiji su EnCase, FTK i drugi.

Pored navedenog vrlo je bitno i izneti da je u formi razvoja informaciono telekomuniacione opreme i uređaja, neophodno posedovati pouzdane i standardizovane, od suda prihvaćene forenzičke alate. Stim uvezi, danas se zbog zahtev za višestruko testiranje i objavljivanje rezultata testa sa stepenom greške koju alat unosi, koristi forenzički alat sa zatvorenim kodom (EnCase 4.0). Međutim, sa druge strane forenzički alati sa otvorenim kodom od strane proizvođača imaju uvek objavljenu svoju proceduru i stepen greške koji unos navedeni alati.

5.5 Lica koja se bave upravljanjem kompjuterskim incidentom

Sa aspekta efektne zaštite računarskih sistema, odnosno informacionih sistema u globalnom smislu, neophodno je definisati tim za upravljanje bezbednosnim kompjuterskim incidentom, koji uključuje lica sa sledećim profilima ili specijalistima za sledeće oblasti:

1. Menadžer zaštite informacija;
2. Administrator računarske mreže;
3. Specijalista za upravljanje i kontrolu bezbednosnog rizika;
4. Kontrolor sistema kvaliteta;
5. Predstavnici eventualnih drugih timova;
6. Digitalni forenzičar;
7. Pravnik; i
8. Menadžer za ljudske resurse.

U svakom slučaju ovakav tim bi bio idelan tim, ali bi nam sada predstojalo debelo ubeđivanje menadžmenta firme za stvarnom potrebnom svih profila odnosno specijalnosti zaposlenih u firmi.

Istragu kompjuterskog kriminala koju bi sadržali timovi gore navedenog sastava je jedini način za efikasan ishod istrage. Ovakav pristup uključenja što većeg broja ljudi neophodnih specijalnosti za svaki konkretan slučaj je jedini način koji omogućava valjanu istragu i način da se prikupe, sačuvaju, analiziraju i valjano predstave dokazi o izvršenom kompjuterskom kriminalu. Uspešan rad ovih timova se obezbeđuje samo odgovorajćem specijalističkom obukom članova tima.

6. DIGITALNA FORENZIKA ANDORID UREĐAJA

6.1 Karakteristike android uređaja

Nekoliko karakteristika su zajedničke na većini Android uređaja, i to:

Prvo, Android je projektovan od samog početka da bude na mreži, bez obzira da li koristi mobilne mreže kao što je globalni sistem za mobilne komunikacije i Kodeksa Division Multiple Access (GSM⁶ / CDMA⁷) ili bežične mreže (Wi-Fi). Bez obzira na mesto, sposobnost da bude na mreži je osnovna odlika bilo kojeg Android uređaja. Mnogi od uređaja su zaista smart i na taj način podržavaju telefoniranje, prijem i slanje tekstualnih poruka, kao i drugih usluga kada se nalaze na mobilnoj mreži. Interakcija na uređaju se obično obavlja preko ekrana osjetljivog na dodir, ali mnogi uređaji takođe omogućavaju korišćenje tastera, koji podržavaju interakciju korisnika [18].

Druga osnovna karakteristika Android uređaja je sposobnost da preuzmete i instalirate aplikacije (Apps) iz Android Market-a. Ovo je osnovna karakteristika za mnoge korisnike jer im omogućava da prošire funkcionalnost uređaja. Ove aplikacije su bogat izvor informacija za forenzičara.

Osnovna karakteristika Androida je mogućnost korisnicima da sačuvaju svoje podatke na uređajima. Uglavnom Android uređaji dolaze sa nekim od uređaja za skladištenje, (NAND flash) interne memorije kao i spoljašnje SD kartice koja je prenosiva i čuva veće količine podataka. SD kartice su obično formatirane sa FAT32.

Google Strategija

Android je očigledno moćna platforma mobilnih uređaj koja košta ogromna sredstva a Google Android ga je dao za džabe?

Odgovor leži u nastojanju Googl-a da organizuje svetske informacije što ga čini univerzalno dostupnim i korisnim. Mobilni telefoni su najpopularniji uređaji u svetu, a Google veruje da činjenjem dostupnim aplikacija sa svoje App Store, deo njihove misije je realizovan. Kada je više ljudi online, više ljudi koriste pretragu, što u konačnom dovodi do prihoda jer je Googl-u primarni izvor posedovanje i nuđenje informacija.

Android je najviše kritikovan OS jer njegovo tržište nije uređeno, a direktna je posledica kako Google čini dostupnima javnosti i Android proizvođačima u otvorenom kodu svoj OS. Ovo je u suprotnosti sa drugim uređajima, kao što je iPhone gde Apple ima potpunu kontrolu nad hardverom i OS i značajan uticaj preko treće strane na aplikacije.

Koncept Android uređaja je dostupnost svima koji žele da imaju stalno dostupan internet i da im stalno budu dostupni servisi koje pružaju ovi uređaji.

⁶ Globalni Sistem za Mobilnu komunikaciju, je međunarodni standard za mobilne mreže

⁷ Daje podršku za više korisnika nego GSM mreža

Dakle, stvaranjem Android mobilnog operativnog sistema koji zadovoljava zahteve potrošača, kao i potrebe proizvođača, Google ima odličnu distribuciju platforme za njihovo pretraživanje i oglašavanje u cilju povećanja svojih prihoda.

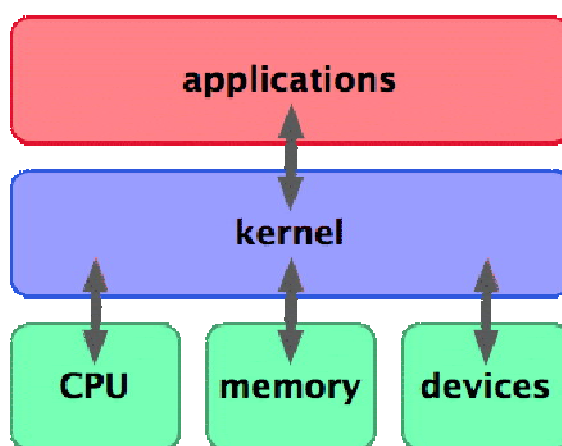
6.2 Hardver android uređaja

Android je dizajniran tako da bude kompatibilan sa mnogim uređajima, a to mu upravo omogućuje kernel⁸. Kernel se danas toliko razvio da podržava, odnosno da je kompatibilan sa mnogim uređajima koji podržavaju android operativni sistem.

CPU (Central Processing Unit) je izraz poznat forenzičarima kao srce samog uređaja, pa je tako i njegova uloga kod android uređaja ista. Naime, CPU je odgovoran za izvršavanje operativnog sistema (OS), aplikacija, kao i koordinacija i kontrola drugih komponenti, kao što je mreža, smeštaj podataka, displej i drugi uređaji integrisani u androidu.

Od samog početka, većina (ako ne i svi) Android uređaji koriste ARM procesore⁹ kao svoj CPU, koji je dovoljno snažan da podrži mobilnu platformu a dizajniran da troši vrlo malo energije zbog duže autonomije rada, odnosno zbog ograničenih kapaciteta baterije.

Neki od proizvođača kao što su Intel su u androide ugrađivali Atom procesore. Paralelno Google je ugrađivao android u svoje Google Tv uređaje, koji su izrađivani na Android platformi. Tu su još i Andorid-x86, Android na kome je korišćena Intelova x86 arhitektura.



Slika 12: Prikaz blok šeme Android uređaja sa kernelom, preuzeto sa sajta <https://commons.wikimedia.org/wiki/File:Kernel.png>.

⁸ Softver koji upravlja hardverom, resursima CPU, pristupanju i čitanju memorije i drugo

⁹ Arhitektura ovih procesora zahteva manje procesora pa samim tim i manje energije za njihov rad

Modem/radio

Modem / radio je hardversko-softverski sistem koji omogućava Android uređaju povezivanje na mobilnu mrežu kao i istovremenu glasovnu i komunikaciju prenosa podataka.

Memorija (Random-Access Memory and NAND Flash)

U Android uređajima imamo dve vrste memorije i to RAM (Random – access memory) i NAND memoriju.

RAM koristi sistem za potrebe pozivanja i izvršenja samih funkcija uređaja.

NAND memorija ne menja svoj sadržaj kada se uređaj isključi i na ovu memoriju je smešten deo bootladera-a¹⁰ [20], operativni sistem i podaci korisnika. Ona predstavlja vrlo bitnu komponentu kod forenzike i predstavlja isto što i forenzika sličnih diskova na laptop, desktop ili server računarima.

Sa strane hardverske perspektive, mobilni uređaji imaju svoje ograničenje memorije u pogledu samog kapaciteta uređaja. Često, ove dve memorije su realizovane kao jedan multičip nazvan MCP (multichip package). Kod forenzike ove vrste memorije treba znati da se one nalaze na pomenutom čipu i uglavnom su tako realizovane.

Global Positioning System (GPS)

Predstavlja revoluciju u primeni i omogućuje pozicioniranje ne samog uređaja već i mogućnost korišćenja pozicioniranja od strane svih ostalih aplikacija koje su instalirane odnosno pokrenute na android uređaju.

Wireless (i Bluetooth)

Pored mogućnosti da se prenos podataka vrši mobilnom mrežom (2G, 3G ili sada 4G), većina uređaja omogućava Wi-Fi konekciju kao konekciju za brzi prenos podataka (danas i preko 10 MB), kao i bluetooth za konekciju sa eksternim uređajima kao što su slušalice, tastature, printeri i drugi spoljni uređaji.

Eksterna memorija (Secure Digital Card)

Većina android uređaja prilikom kupovine ima i svoju SD karticu. Kao i NAND flash, i SD kartica omogućava smeštaj podataka bez aktivnog napajanja. Dobra strana ove memorije je što se prilikom zamene uređaja korisnik prebacivanjem svoje stare SD kartice prebacuje sadržaj u novi telefon bez problema i tehničkih dodatnih radnji.

Ekran Android uređaja

¹⁰ U osnovi je kod koji se koristi za zaključavanje Android uređaja, odnosno da bi proizvođači obezbedili da se koristi njihov firmware gde su određeni parametri sistema zaključavali, kao što je to slučaj kod uređaja Samsung, dok HTC ima otvoreni kod. On služi za pronalaženje kernela i sadrži podatke na kom su delu memorije sadržani potrebni podaci za rad Android uređaja.

Najvažnija ulazna komponenta Android uređaja je svakako displej. Najvažniji je zbog činjenice da se preko njega vrši upravljanje, odnosno korišćenje samog uređaja. Iz tog razloga na početku razvoja uređaja bili su displeji manje rezolucije dok se danas koriste displeji visoke rezolucije sa revolucionarnom AMOLED tehnologijom, koja je vrlo dobro prihvaćena od strane korisnika Android uređaja.

Kamera

Kamera na telefonu je inicijalno razvijena za fotografisanje, ali je i na ovom polju u zadnje vreme postignuti veliki rezultati u pitanju rezolucije koja se koristi za fotografije i video zapise koje kamere u današnjim uređajima vrše.

U nekim uređajima su ugrađene čak i dve kamere, jedna koja se koristi za video pozive (bilo inicijalno od strane uređaja ili korišćenjem novijih programa Skype, Viber i slično), od kojih je jedna boljeg i jedna lošije rezolucije (kvaliteta).

Ono što je svakako interesantno što je integrisano kod kamere je da može da vrši i prepoznavanje bar kodova, pa je samim tim primena android uređaja našla svoju širu primenu (magacini, naručivanje robe, praćenje zaliha u magacinu i slično).

Baterija

Predstavlja bitan segment svakog Android uređaja. Naime, onoliko koliko traje autonomija vaše baterije toliko će vam biti i dostupan uređaj, a posebno ukoliko se uzme u obzir činjenica da se uglavnom radi o smart telefonima, danas se često baterija puni svakodnevno zbog velikog broja aplikacija koje koriste resurse Android uređaja i koji se napajaju iz baterije telefona. Delimično se ovaj problem rešava na taj način što se iz App Stora, Google Play-a instaliraju aplikacije za štednju baterije.

Ono što je za forenzučku analizu Android uređaja bitno je da su uglavnom iza baterija smeštene SD kartice koje se koriste što treba imati na umu prilikom istrage.

USB konekcija (Universal Serial Bus)

Povezivanjem USB-om omogućuje se sledeće funkcije:

- 1.- Punjenje, gde se preko USB kabla vrši samo punjenje baterije Android uređaja;
- 2.- Disk interfejs, SD Card i drugim memorijama se pristupa preko ovog interfejsa;
- 3.- Namenjen za deljenje internet veze, odnosno za korišćenje uređaja kao modema za pristup internetu drugom uređaju a da to nije bežična veza.
- 4.- Za omogućavanje korišćenja naprednih funkcija kao što je ADB (Android Debug Bridge)¹¹.

Ugrađeni žiroskop

U samom Android uređaju ugrađen je žiroskop koji daje mogućnost da se prilikom okretanja uređaja okreće i korisničko okruženje, tipično koristi se za korišćenje displeja landscape ili portrait.

¹¹ Omogućavanje upravljanje uređajem preko USB kabla, posebno značajno i za forenzičare koji se bave prikupljanjem digitalnih dokaza sa uređaja.

Mikrofon na uređaju

Konačno, smart telefon ili tablet uređaji neće biti zanimljivi korisniku ukoliko nema mogućnost da reprodukuje zvuk. Neki uređaji imaju i više mikrofona, čak i do tri da bi se preko aplikacija koje imaju u sebi poboljšao kvalitet zvuka.

6.3 Procesi tokom startovanja Android uređaja

Kao i ostali računari Android uređaji takođe imaju standardizovan proces startovanja (boot) tokom koga se učitava firmware, OS i korisnički podaci u memoriju uređaja prilikom procesa startovanja. Vrlo bitna činjenica za forenzičara je da iako je proces pokretanja standardizovan, firmware¹² i ROM varira od proizvođača do proizvođača uređaja.

U osnovi kod svih Android uređaja definisana su 7 procesa prilikom startovanja, i to:

1.- Uključivanje uređaja, gde se uključuje čip kodom uređaja- kod iz ROM-a se upoređuje sa kodom iz CPU i vrši se inicijalizacija pokretanja hardvera i lokacija podataka iz memorije za startovanje. ROM kod je specifičan za svaku CPU koja se koriste u konkretnom analiziranom uređaju. Ovaj proces je sličan procesu startovanja kod računara;

2.- Unos boot sekvence- Ima dve faze i to IPL (Initial program load) i druga faza SPL (Second program loader). IPL je odgovoran za ubacivanje podataka u RAM početnih parametara za startovanje Android uređaja, u cilju uspostavljanja početnih servisa na uređaju. Nakon što je pripremljen RAM na ovaj način IPL kopira SPL u RAM. SPL zatim pored što je odgovoran za startovanje OS, zadužen je i za omogućavanje pristupa drugim operacijama startovanja (fastboot¹³, recovery i drugim procesima za startovanje uređaja). SPL generalno zavisi od samog proizvođača, a u osnovi njegova funkcija je pokretanje hardverskih komponenti, sat, konzola, displej, tastatura, modema, virtuelna memorija, i drugo.

Na kraju SPL smešta Linux kernel i kopira u RAM, unosi parametre pokretanja, i na kraju kreće izvršavanje kernel programa;

3.- Linux kernel;

Kernel je srž operativnog sistema, u stvari softver koji upravlja hardverom i programskim resursima.

Nakon podšavanja početnih parametara, radi potpunog razumevanja procesa smatraćemo da sada Kernel u potpunosti kontoliše uređaj. Nakon podešavanja parametara, podaci se čitaju iz NAND memorije, i omogućuju pristup sistemu i korisniku.

4.- Inicijalni procesi u uređaju;

¹² Softver koji je obično ide uz hardver odnosno koji se nalazi u njegovoj ROM memoriji

¹³ Je dijagnostički protokol za povezivanje uređaje preko USB protokola gde je omogućena modifikacija sistemskih elemenata pomoću navedene USB konekcije

Nakon što kernel preuzme uređaj pristupa se startovanju servisa na android uređaju. Kao primer koliko je kompleksno pokretanje uređaja navodi se primer preko 650 linija progama kod HTC na Androidu 2.2.

Ovde bi svakako trebalo naglasiti činjenicu bitnu za forenzičare da se kod internet pretraživača kada se završi boot proces uređaja, privremena memorija (Cache) premešta sa particije smeštene na NAND fleš memoriji u privremeni RAM disk (tmpfs) smešten u at/app-cache.

5.- Zygote i Dalvik;

Zygote je virtuelna mašina koja omogućuje virtuelno okruženje za Java izvršavanje progama. Bez njega ne bi bilo pokretanja nekih funkcija Android uređaja. Zygote može naknadno da pokreću drugo virtuelno okruženje nazvano Dalvik.

6.- Proces koji se odvija u sistemskom serveru;

Nakon pokretanja Java okruženja preko Zygote virtuelne mašine smatra se da je podignut i počeo sa radom sistem server, koji omogućuje telefoniju, mrežu i ostale osnovne funkcije uređaja.

7.- Kraj pokretanja (boot –ovanja);

Nakon ispunjavanja svih prethodnih funkcija, sistema šalje poruku da je “ACTION_BOOT_COMPLETED” i da je uređaj startovan nakon čega može da počne njegova interakcija sa korisnikom.

Navedeni procesi su objašnjeni radi lakšeg shvatanja procesa na Android uređajima, posebno u slučaju potrebe digitalne forenzičke istrage uređaja koje pokreće Android operativni sistem.

6.4 Android fajl sistem i struktura podataka

Za forenzičare je najbitnije kako analizirati podatke koji se dobiju istragom. Zbog složenosti skladištenja podataka i korišćenja od strane samog OS u Android uređaju, nema literature koja bi mogla u potpunosti da da odgovore na pitanja forenzičara [18].

Android uređaji u svoje memorije skladište veliki broj podataka, i to uglavnom kombinaciju ličnih podataka korisnika i podataka za rad samog uređaja, gde su aplikacije (programi) primarni izvor podataka i dele se na:

- Aplikacije koje su dobijene uz Android uređaj;
- Aplikacije koje su instalirane od strane samog proizvođača;
- Opciono Google/Android aplikacije sa Play store; i
- Aplikacije instalirane od strane korisnika, uglavnom sa Android Market-a.

Suštinski, podaci koji do kojih se može doći forenzičkom analizom android uređaja (smartphone-a, tableta-a i drugih uređaja), mogu se prikupiti sledeći podaci:

- Tekst poruke (SMS, MMS)
- Kontakti

- Pozivani brojevi
- E-mail poruke (Gmail, Yahoo)
- Podaci za četovanja (Viber, Instant Messenger)
- GPS koordinate
- Fotografije, video snimke
- Istoriju web pretraživanja
- Istoriju pretraživanja u internet pretraživačima
- Uputstva za vožnju
- Facebook, Twiter i druge socijalne mreže
- Podatke i dokumenta smeštena na samom uređaju
- Muziku
- Aktivnosti iz podsetnika i kalendara
- Informacije o tekućim računima
- Istorija kupovine
- Razmena fajlova

Podaci koji koriste aplikacije na Android uređajima se smeštaju na dve lokacije, internu i eksternu memoriju, što zahteva dobro poznavanje strukture podataka kod istrage. Nakon instalacije aplikacije, ukoliko su smeštene na eksternoj memoriji (SD Card) mogu se smeštati bilo gde, međutim to nije slučaj ukoliko se aplikacija instalira u memoriji samog uređaja.

Kod android uređaja podaci se smeštaju u unapred određenim folderima (direktorijumima) pa tako za pretraživače, kod default browsera se smešta u paketu čije je ime `com.android.browser` a fajlovi su smešteni u `/data/data/com.android.browser`.

Podaci se smeštaju na više načina i to na NAND fleš, SD kartici ili na mreži, što se može objasniti kao:

- 1.- Deljeni resursi
- 2.- Interna memorija
- 3.- Eksterna memorija
- 4.- SQLite
- 5.- Mreža

Kao značajnu činjenicu za forenzičku istragu, smatram bitnim u kojoj se memoriji Android uređaja mogu naći koji podaci. Već smo pomenuli da Android uređaji imaju RAM i NAND fleš memoriju i u svaku od njih se smeštaju određeni podaci. Da bi forenzičar znao u koju da traži određeni podatak koji je cilj forenzičke istrage u literaturi se mogu naći sledeći podaci, to:

RAM sadrži veoma značajne podatke koje koriste aplikacije da bi vršile obradu podataka, kao što su:

1. Lozinke
2. Ključevi za razmenu podataka
3. Korisnička imena
4. Podaci aplikacija
5. Podaci iz procesa sistema i servisa

Kod NAND fleš memorije najveća prednost je što se na nju smeštaju podaci a ista ne mora biti napajana. Male dimenzije i jeftina izrada su još jedna od prednosti skladištenja podataka posebno za uređaje kao što su smartphone aparati i tableti.

Kao i većina Linux sistema, postoji nekoliko sistema datoteka u upotrebi na Android uređajima, koji se koriste da se pokrene i upravlja sistemom. Kod forenzičke istrage primarni fokus je na particije gde se čuvaju korisnički podaci, posebno EXT, FAT32, and YAFFS2 file systems.

7. ADB I FORENZIČKI ALATI

U osnovi, Android uređaji ne mogu da se vežu na kompjuter bez interakcije sa istim. U forenzici Android uređaja neophodno je sa što manje uticaja računara na sam uređaj a da se izvrše sva potrebna snimanja podataka potrebnih za istragu [18].

7.1 Android Debug Brige (ADB)

Radi unificiranog pristupa izradi image-a ili slike uređaja na kome se vrši forenzička analiza, bez korišćenja aplikacija koje su dostupne u otvorenom kodu, koristićemo ADB [27].

ADB je u osnovi spona između android uređaja i računara preko koga se vrši analiza. ADB dolazi uz kompletan Android SDK koji se mora skinuti u celosti bez obzira što nam treba samo ADB. SDK sadrži potrebne alate za razvoj aplikacija na Android uređajima. Nakon instalacije SDK, pokretanja SDK menadžera, vrši se izbor potrebnih alata za instalaciju, koji zavisi od tipa Android OS na uređaju do alata za komandne linije i vrlo bitnog google driver-a.

Da bi ovako instalirani ADB mogao da se koristi neophodno je izvršiti dodatna podešavanja na Android uređaju i na samom računaru, i to:

1.- Na Android uređaju opcije za razvoj, odnosno opcije za programera su sakrivene, a da bi iste bile aktivirane neophodno je sedam puta pritisnuti na Broj verzije (Build number) u Podešavanjima uređaja. Kada se ove opcije otključaju dolazimo do opcija za programera, gde je bitno da je mod "Režim otklanjanja grešaka" uključen, da bismo mogli da komande koje unosimo u Comanderu računara izvršavali u uređaju.

2.- Na računaru u naprednim opcijama potrebno je uneti put do alata u ADB modu, tamo gde su instalirani na računaru (Computer – Properties - Advanced system settings - Enviroment Variables - "PATH" – uneti sačuvanu putanju sa C particije, koja sadrži SDK-platform-tools i tools). Nakon toga se vrši ponovno pokretanje računara. Ovako pokrenut računar sada treba da instalira driver za uređaj. Instaliranje se vrši automatski ili ručno preko alata koje sadrži SDK menadžer, USB driver u zavisnosti od arhitekture OS koji koristite.

Da bi ste proverili da li ste pravilno instalirali ADB potrebno je da pokrenete Comander. Nakon pokretanja istog ukucati ADB Devices. Ukoliko se dobije lista uređaja ispod komandne linije onda je izvršena priprema radne stanice za korišćenje u forenzičke svrhe korišćenjem nekih komandi u Linux-u.

Napred navedeno se koristi za rad i Windows okruženju, dok bi znatno jednostavnije bilo da radna stanica poseduje VMWARE sa instaliranim UBUNTU operativnim sistemom pod LINUX-om. Ovako pripremljena radna stanica omogućava vam snimanje kompletne slike uređaja bez dodatnih podešavanja, a sve zbog problema koji ima Linux i ograničenje na FAT fajl sistemu od 4 GB, dok je slika koja se dobija istragom veća od 7 GB, jer su i memorije uređaja na kojima se vrši danas analizo preko 8 GB. Na Andorid uređaju se instaliraju i apliakcije SuperSu i Busybox sa android marketa [33].

Komande koje se koriste prilikom izrade image-a fajla u ADB, za analizu i akviziciju su sledeće:

Komanda	Sintaksa	Značenje
ADB	ADB -d	Izdavanje naredbe uređaju koji je povezan preko USB porta
Shell	ADB Shell	Izdavanje naredbe uređaju direktno preko računara
Forward	Forward <i>local, remote</i>	Komunikacija preko portova, ulaz i izlaz
nc	nc -l	Portovi za ulaz i izlaz
dd	dd if=/ <i>...</i>	Određivanje fajlova za kopiranje, kreiranje slike

7.2 Forenzički alati

FTK Imager

Forenzički besplatni alat za izradu slike (image fajla), za potrebe forenzike je FTK Imager. Koristi se kako za izradu image fajla, tako i za analizu u forenzičke svrhe. Navedeni program pravi savršene kopije (forenzičke slike) kompjutera, bez izmena na originalnom dokazu [29]. Treba napomenuti da je obavezno korišćenje i alata za blokiranje pisanja preko USB porta koji mogu da se nađu besplatno.

Napred navedeno o FTK Imager-u u osnovi govori o mogućnostima korišćenja programa koje su sledeće:

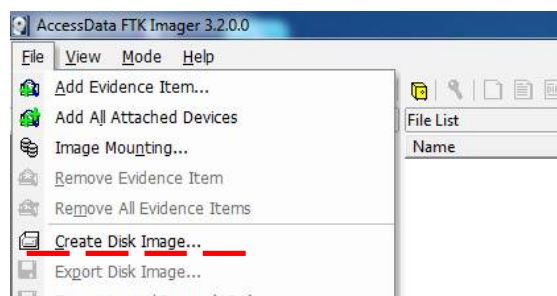
- 1.- Izrađuje forenzičke slike hard diskova, flopi disketa, Zip disketa, CD-a, DVD-a, kompletnih direktorijuma, ili konkretno pojedinih fajlova.
- 2.- Pravi izveštaj fajlova i foldera na lokalnom disku, mreži, disketi itd.
- 3.- Pravi izveštaj sadržaja forenzičke slike smeštene na lokalnom računaru ili mreži
- 4.- Iz forenzičke slike vrši oporavak fajlova, posebno obrisanih
- 5.- Iz korpe za otpatke vrši oporavak fajlova (Recycle Byn) koji nisu prebrisani
- 6.- Kreira hash funkciju analizirane memorije

Da bi se izbeglo gubljenje image fajla, odnosno dokaza, FTK pravi bit-po-bit duplikat fajla. Forenzička slika je identična originalu, što omogućava da se originalni mediji koji se analizira smesti na sigurnom dok se vrši analiza slike.

Pored instalacije na računaru na kome se planira vršenje akvizicije podataka, FTK Imager se može instalirati i na drugim prenosnim uređajima. Vrlo se jednostavno ovi programi pokreću u Windows OS kao program (FTK Imager.exe).

Naredbe koje se koriste kod izrade image u programu FTK Imager su:

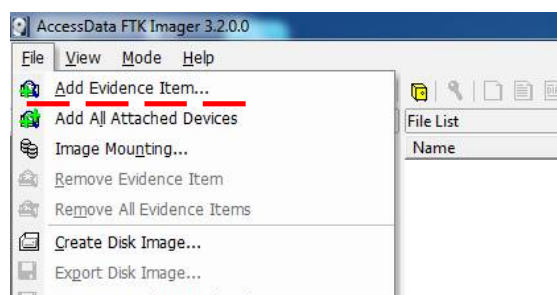
File – Create Disk Image



Slika 13: Interfejs FTK Imager

Nakon kreiranja slike analiziranog medija, moguće je izvršiti analizu image fajla, izdavanjem, ili odabirom sledeće naredbe:

File-Add Evidence Item



Slika 14: Interfejs FTK Imager

Pored navedenih, FTK Imager sadrži veoma moćan alat a to je “capture RAM”, gde trenutno vrši snimanje kompletnog sadržaja RAM memorije uređaja, što je kod nekih istraga neophodno, posebno u slučaju da se na licu mesta nalazi uključen uređaj, a odnosi se na snimanje memorije računara na kome se najpre vrši nasnimavanje programa.

Autopsy 3.1.3.

Autopsy je besplatni softverski alat za analizu sa izvršenog snimanja slike uređaja, odnosno memorije nad kojom se vrši forenzička analiza. Autopsy je moćno oružje u ruci forenzičara zbog svoje pouzdanosti i jednostavnosti u korišćenju i dobro organizovanog interfejsa samog programa, kao i moda za Android uređaje [30].



Slika 15: Interfejs Welcome prozora Autopsy programa

Za pokretanje slučaja, potrebno je izabrati u Welcome prozoru “Create New Case”. Ova komanda pokreće dalji izbor i unos podataka o slučaju vođenim putem, gde se unose, podaci o slučaju, podaci o forenzičaru, odnosno licu koje vodi istragu. Nakon unosa navedenih podataka, automatski prozor nudi mogućnosti za unos podataka radi analize, i to:

- Za sliku diska
- Za lokalni disk
- Za logičke fajlove

Ovde treba napomenuti da se proces analize može ubrzati u izboru prilikom odabira slučaja, gde se ne tretiraju prazni prostori na disku.

Automatska analiza slike fajla obuhvata sledeće aktivnosti:

- “Ingest Modules” praćenje procesa analize
- Nedavne Aktivnosti
- Baza Hash funkcije
- Identifikacija fajlova po tipu
- Komprimovani fajlovi
- Modul za ekstrakciju slika
- Pretraga rezultata po ključnoj reči
- Modul za mail
- Izborni za nepoznate fajlove
- Provera da li se isti E01 fajlovi
- Modul za Android uređaje
- Za fajlove koji su prethodno odabrani kao bitni za istragu

Nakon odabira vrste modula koji nas interesuje, u odnosu na podešavanja sa naše strane, može se vršiti i dodatna analiza po npr. ključnoj reči.

Dok traje proces unosa slike u aplikaciju u donjem desnom uglu je prikazan proces analiziranja istog.

Delovi Autopsy interfejsa su sledeći:

- Direktorijum (Tree Viewer)
- Rezultati (Result Viewer)
- Sadržaj (Content Viewer)
- Status (Status Area)

Prikaz direktorijuma sa leve strane interfejsa sadrži podatke ulaznog modula, odnosno analize unete slike analiziranog uređaja. Direktorijum sadrži nekoliko glavnih i više poddirektorijuma:

- Izvor podataka koji nam prikazuje hijerahiju sistema fajlova sa slike analiziranog uređaja. Svaki podata, fajl i direktorijum je prikazan kao na disku, odnosno memoriji.
- Pregledi gde su nam prikazani fajlovi prema tipu podataka
- Rezultati gde se mogu videti svi podaci vezani u analizu slike, čak iako su više puta prikazivani
- Izveštaji gde se prikazuju svi izveštaji unete slike i zadatih parametara sa naše strane (ukoliko smo ih unosili)

Ostali izveštaji se mogu koristiti u skladu sa individualnim ciljem i odlukom forenzičara koji vrši analizu slučaja.

8. TABLET RAČUNARI KARAKTERISTIKE

S obzirom na činjenicu da sami tablet računari imaju vrlo različite karakteristike u ovom radu će konkretnije biti reči o uređaju koji će biti korišćen u studiji slučaja. Naime, radi se o Lenovo A3500-FL, bez podrške za SIM karticu. Njegove mogućnosti, odnosno tehničke specifikacije su sledeće [31]:

Model Tablet računara	Model: Lenovo A3500-FL Version: WLAN	
Operativni sistem	Android v4.2 Jelly Bean Dozvoljen i dostupan Android KitKat 4.4	
Dispplej	7" HD (1280 x 800) IPS	
Kamera	Prednja: 2 MP Fixed-focus	
Senzori	G-Sensor (Accelerometer) Vibration	
Kernel	Verzija jezgra 3.4.67	
Hardver	Procesor	MTK 8121(WiFi) 1.3GHz Quad Core
	Zvuk	1x Zvučnik / 3.5mm slušalice
	Memorija	RAM: 1GB, ROM: 8GB Podrška do 32GB
	Battery	Tip: 3450 mAh Li-Po, fixed Standby: Up to two weeks Vreme korišćenja: Do 8 sati
	Radio	FM Receiver
	WLAN	Wi-Fi 802.11 b/g/n
	Bluetooth	Bluetooth® 4.0

Iz karakteristika uređaja možemo da zaključimo da sam uređaj poseduje dovoljnu količinu memorije za smeštaj raznih podataka. Pored velike unutrašnje memorije uređaj podržava i memorijske SD kartice do 32 GB pod FAT fajl sistemom.

S obzirom da računar ne poseduje GSM podršku, uglavnom je namenjen za poslovnu upotrebu u preduzećima koja imaju WiFi podršku ili za korišćenje za ličnu upotrebu. Takođe, pored navedenog, može da se koristi i WiFi Thetering za povezivanje na mrežu.

Od svih parametara uređaja među bitnijim se svakako nalazi i podatak o samom jezgru Tablet uređaja koji pokreće isti.

Vrlo je značajan podatak, posebno ukoliko se neko sa programerske strane bavi povećanjem preformansi sistema, posebno kod overclock-a, a za predmetni Tablet podaci se nalaze na sajtu xda-developers [30].

Vrlo ineteresantan podatak u pogledu pokušaja popularizacije tablet uređaja i njihovu integraciju sa pametnim telefonima je uređaj koji je nazvan PHABLET [34]. Navedeni uređaj je sa nešto većim displejom nego li pametan telefon a manji displejom od Tablet uređaja. Isti nude sve karakteristike pametnih telefona.

9. NIVOI BEZBEDNOSTI ANDROID UREĐAJA I PREDLOZI ZA POBOLJŠANJE

Na jednom mestu prikupljena i izvršena podela osetljivih informacija koje se nalaze u aplikacijama koje koriste Android uređaji kao lista aplikacija koje sadrže poverljive informacije o vlasniku uređaja, se dele na sledeći način:

1.- Aplikacija ne sadrži osetljive informacije- na primer kalkulator u uređaju ne sadrži nikakve osetljive, odnosno poverljive informacije o korisniku.

2.- Nema poverljivih podataka ali sadrži meta data podatke- na primer, aplikacija vremenske prognoze na android uređaju ne sadrži poverljive informacije ali sadrži podatke o GPS položaju uređaja, što se može dovesti u vezu sa korisnikom uređaja.

3.- Sadrži podatke ali nisu osetljive, odnosno poverljive prirode- Primer informacija na socijalnim mrežama, kao što je na primer Twiter.

4.- Sadrži podatke poverljive prirode – mnoge aplikacije spadaju u ovu kategoriju koja sadrži poverljive podatke, a to su one koje u sebi sadrže puni e-mail, SMS i MMS poruke, govornu poštu, fajlove logovanja i drugo.

5.- Vrlo osetljivi podaci- u ovu vrstu spadaju aplikacije koje sadrže finansijske informacije, informacije o zdravlju, aplikacija za čuvanje lozinki i druge aplikacije koje ukoliko otkriju informacije o korisniku dovode do kompromitacije njegove bezbednosti.

Na osnovu do sada iznetog tokom istraživanja Android uređaja dolazi se do nekoliko predloga radi povećanja bezbednosti uređaja [18], i to:

1.- Uvek se konektujte na poudanu mrežu, kućna mreža, mreža prijatelja. Ovo vam omogućava da osetljive podatke koje prenosite bilo preko WiFi, bilo preko GSM mreže provajdera, nije maliciozna i ne koristi se od strane napadača da kompromituje vaše osetljive podatke.

2.- Uvek koristi lozinku (password). Takođe, potrebno je koristiti i PIN kod za mrežu, gde se koriste numerički kodovi .

3.-Nikada ne pratite linkove koje dobijate u SMS porukama kao i linkove u e-mail porukama, posebno linkove koji imaju skraćeni oblik tipa g2ng.

4-Prilikom korišćenja web browser-a koristiti drugi a ne njegov osnovni pretraživač koji ste dobili prilikom kupovine Android uređaja, jer se podaci koji se skladište u memoriju telefona tačno određeni i lako je do njih doći.

5.-Prilikom instalacija aplikacija sa Androi marketa, odnosno sa Google Play-a obavezno pratiti koje dozvole traži aplikacija prilikom instalacije. Ukoliko vam bude bilo šta sumnjivo takvu aplikaciju ne instalirati, već prekinuti instalaciju. Ilustracije radi, ukoliko vam aplikacija za sat traži pristup SMS porukama, onda to svakako ukazuje da nešto nije u redu.

Ono što je svakako neophodno je svakodnevna edukacija lica korisnika uređaja sa Android platformom, jer se navedena lista iz dana u dan povećava, kako u pogledu razvoja platformi za bezbednost tako i po pitanju aplikacija koje se postavljaju u google prodavnicu.

10. STUDIJA SLUČAJA

U sklopu pripreme izvršeno je slanje jednog mail-a sa nepoznate e-mail adrese za vlasnika Tablet računara koje u sebi sadrži ponudu i attachment, odnosno prilog. Pored navedenog došlo je i do gubljenja svih podataka sa SD kartice tablet računara, gde je izvršeno formatiranje iste.

Vlasnik uređaja je u sklopu korporacijske istrage, stručnjaku za forenziku izneo sledeće:

- Vlasnik tablet uređaja je vlasnik privatne firme za distribuciju ogreva za jug Srbije.
- Na tablet uređaju je instaliran sadržaj bitan za funkcionisanje preduzeća, posebno deo trenutne ponude firmi i podaci o zaposlenima.
- Prilikom pokušaja da na tabletu pogleda nasnimljene sadržaje dogodilo se da je kompletan sadržaj SD kartice prazan. Nakon što je ustanovio da mu je sadržaj kartice nestao, izvadio je micro SD karticu iz uređaja i pokušao da na svom računaru proverii sadržaj iste i ustanovljava isto, da nema prethodno nasnimljenih podataka. Karticu nije vraćao u uređaj.
- Fajlovi koji se traže su formata pdf.
- Vlasnik je takođe izneo da je istoga dana dobio mail sa njemu nepoznate mail-adrese (koja u sebi sadrži ime jelsijevic), ali da nije pridavao veliki značaj jer se radilo o nekoj ponudi koja mu nije bila inetersantna.
- Budući da se radi o preduzeću vlasnik je pred forenzičara postavio zadatak istrage da li je i u kojoj meri bio izložen eventualnom napadu sa mreže i oporavak izgubljenih podataka bitnih za firmu.
- O samom uređaju je izneo da na njemu od kada je u njegovom vlasništvu nije pridavan veliki značaj bezbednosti, da koristi mail-adrese za komunikaciju na njemu i da nikada nije unosio bilo kakvu lozinku i zaštitu na njemu. Pored navedenog, izneo je da povremeno isti računar koriste i njegova deca.

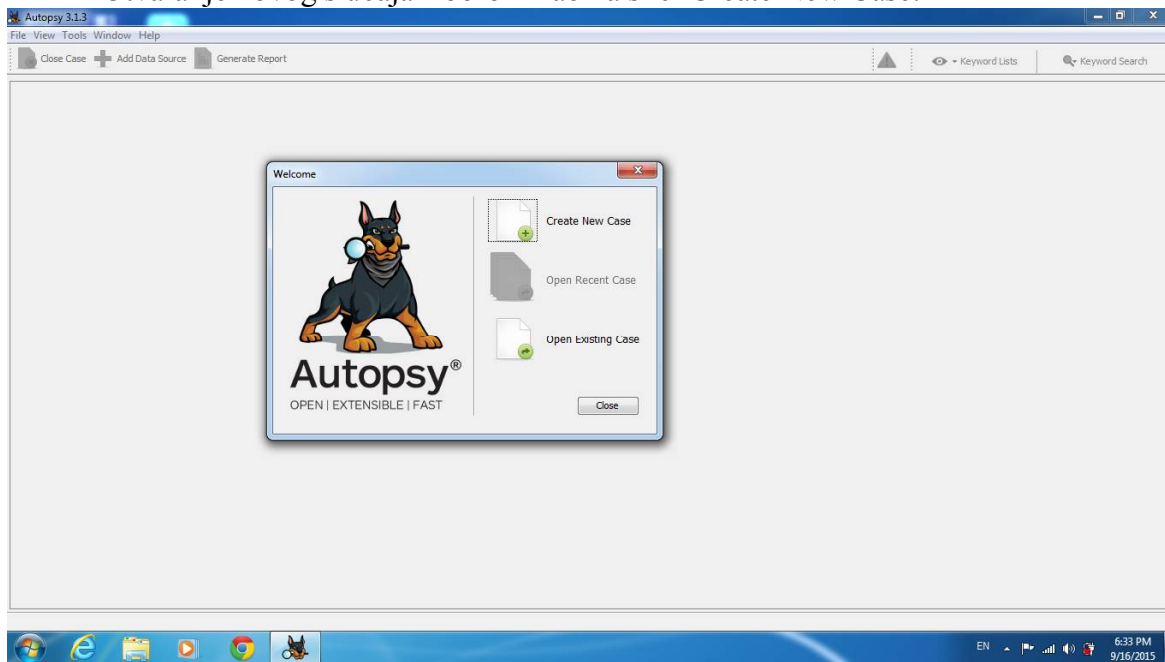
S obzirom na navedeni slučaj stručnjak za forenziku je napravio sledeću strategiju za obavljanje istrage:

- Za izradu slike micro SD kartice koristiće FTK Imager.
- Za anlizu i oporavak fajlova koristiće Autopsy 3.1.3.
- Za izradu slike kompletnog uređaja koristiće ADB bridge u VMWARE i Linuxu
- Za analizu podataka sa tablet uređaja koristiće Autopsy 3.1.3.
- Priprema izrađenih slika uređaja za slučaj potreba istrage u krivične svrhe u skladu sa rezultatima istrage.
- Vraćanje uređaja vlasniku tableta sa izveštajem i kompetnim podacima.

Pristupanjem analizi SD kartice, forenzičar u prva dva koraka vrši blokiranje pisanja na SD kartici i izradi slike pristupa na već opisani način korišćenjem Softwer Write Block-a i FTK Imagera.

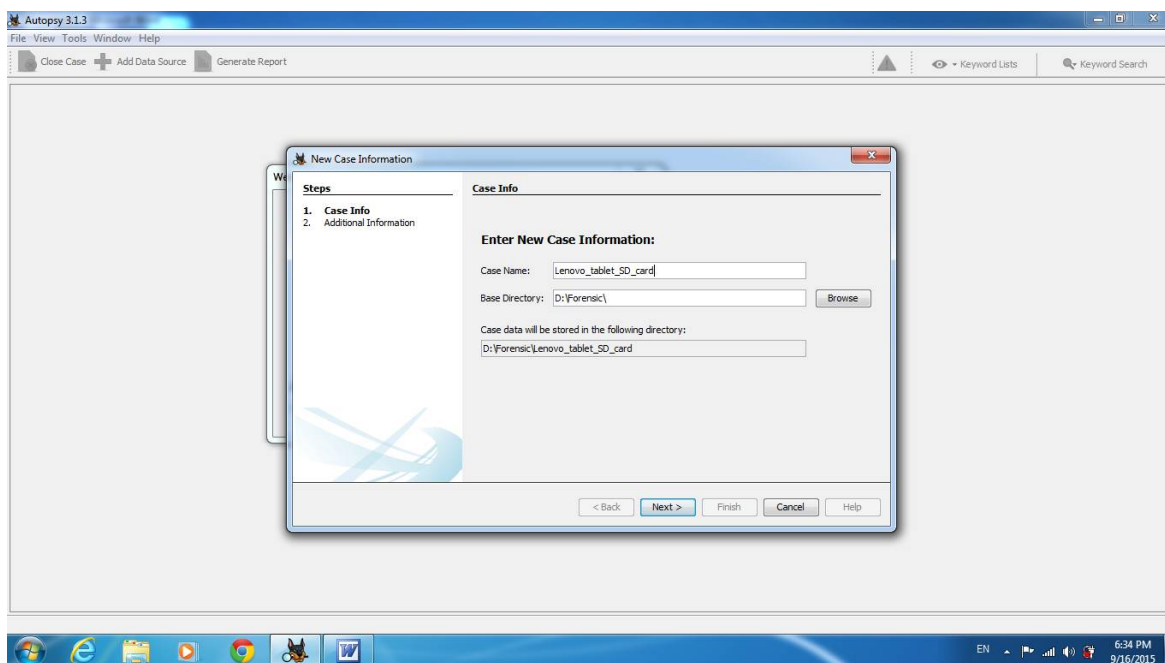
Nakon što je izradio sliku SD kartice, prelazi na analizu iste u programu Autopsy na sledeći način, korak po korak:

Otvaranje novog slučaja izborom kao na slici Create New Case:



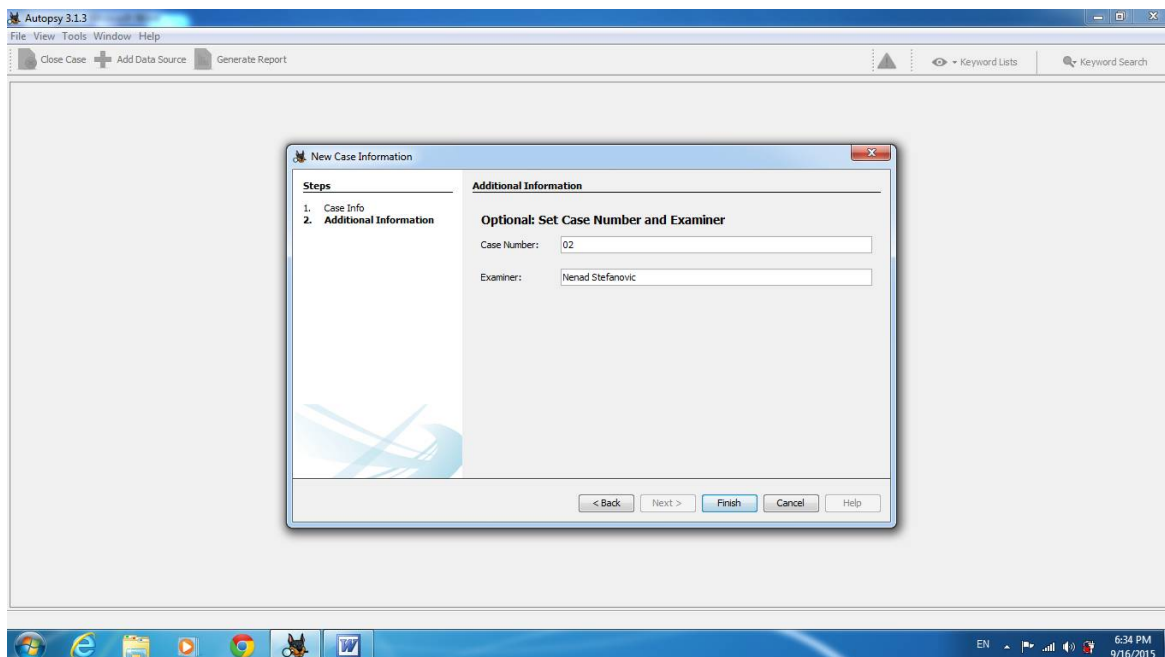
Slika 16: Početni prozor nakon pokretanja Autopsy programa (Welcome)

Zatim u izboru informacija o istrazi unosi ime koje daje slučaju i unosi direktorijum u kome će biti smešteni rezultati istrage, po preporuci na D disku:



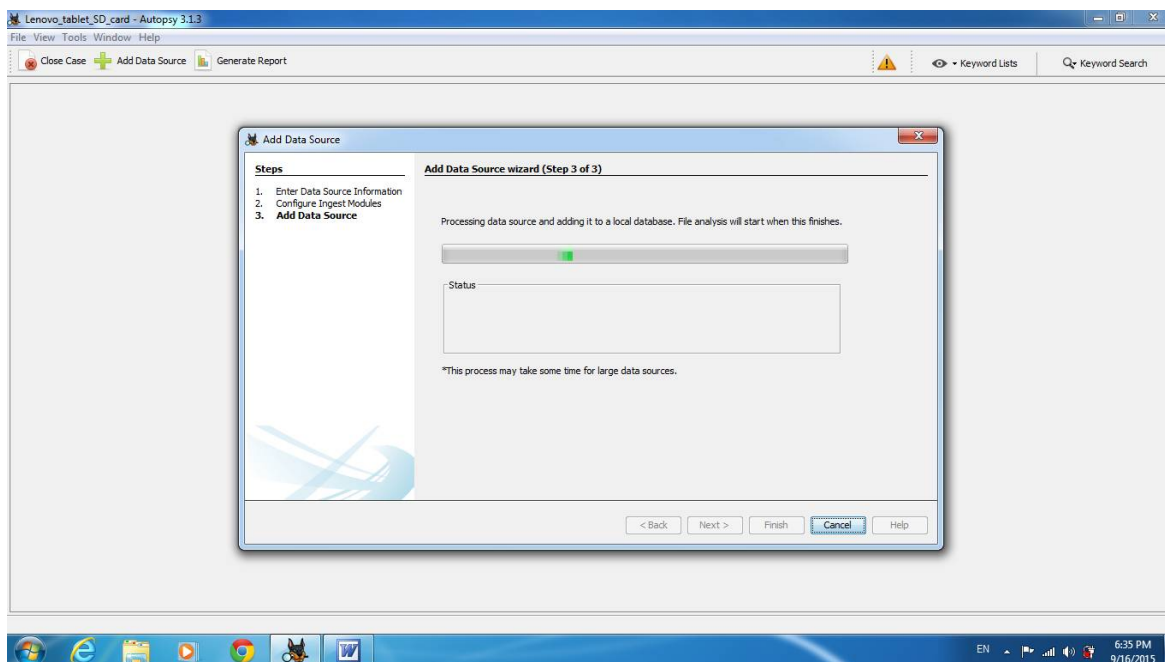
Slika 16: Unos informacija o slučaju

U sledećem koraku se unosi broj slučaja kao i forenzičar koji je vršio istragu odnosno analizu.



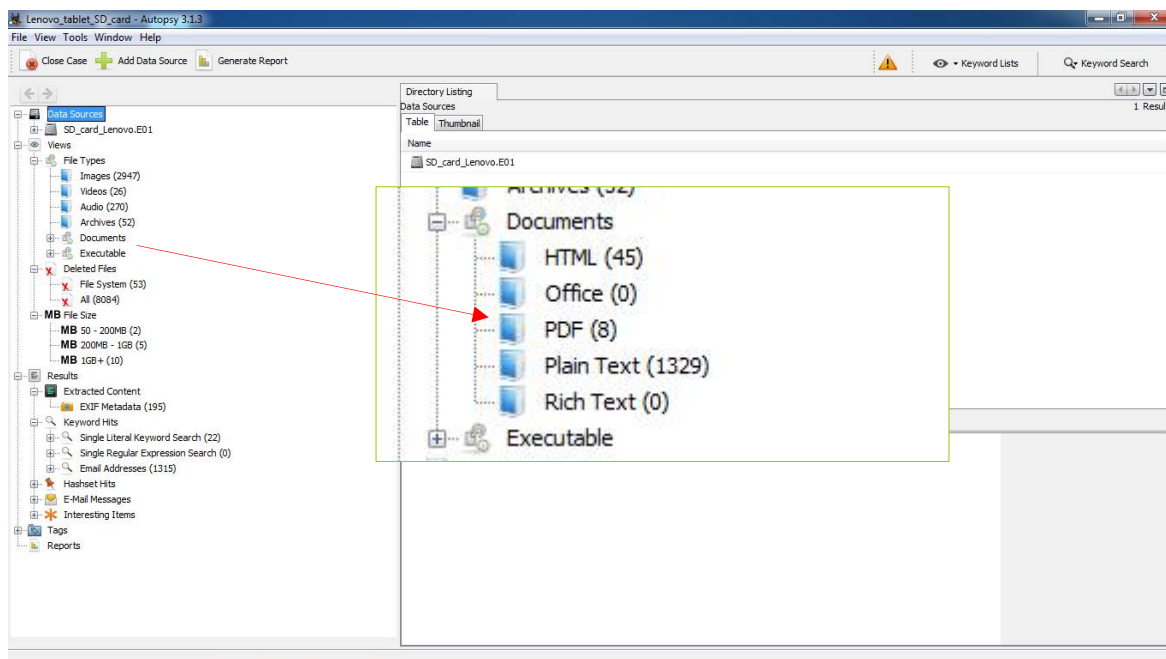
Slika 17: Unos informacija o slučaju

Nakon ovako unetih podataka prelazi na izbor slike za analizu. U ovom slučaju slika se nalazi na računaru gde je i bio izbor prilikom izrade u FTK imager-u. Nakon toga kreće analiza unetih podataka sa slike koja izgleda kao na sledećoj slici.



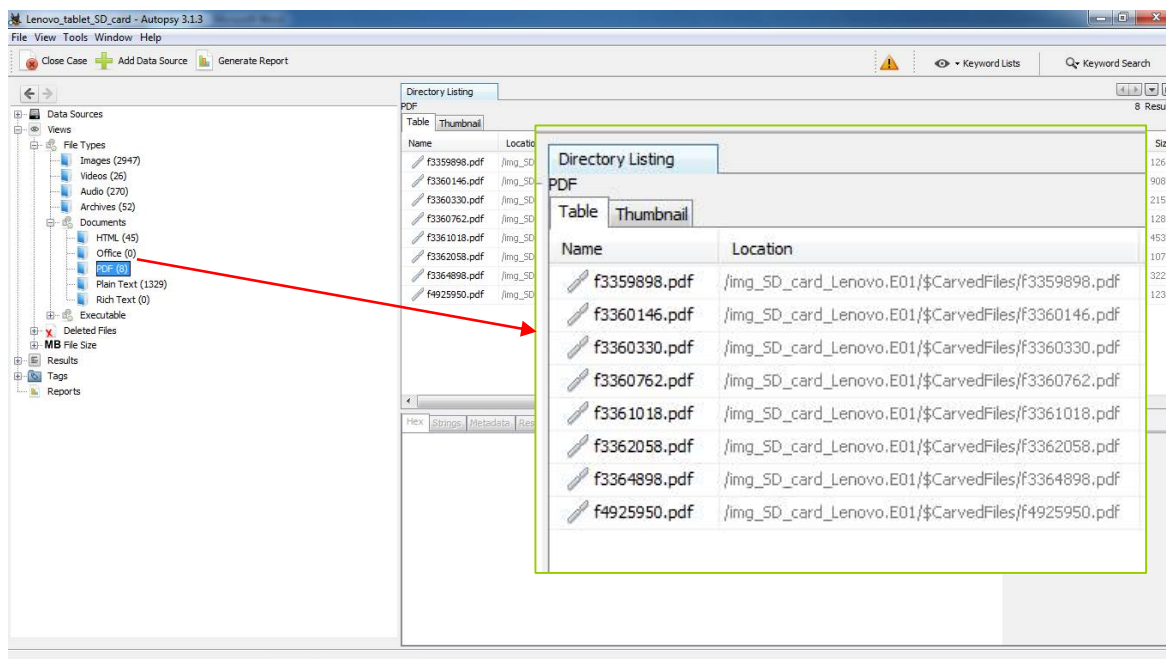
Slika 18: Proces analize (Digest mode)

Nakon izvršenog tzv. “Digest moda”, odnosno analize slike SD kartice, prelazimo na pregled sadržaja iste, po direktoijumu.



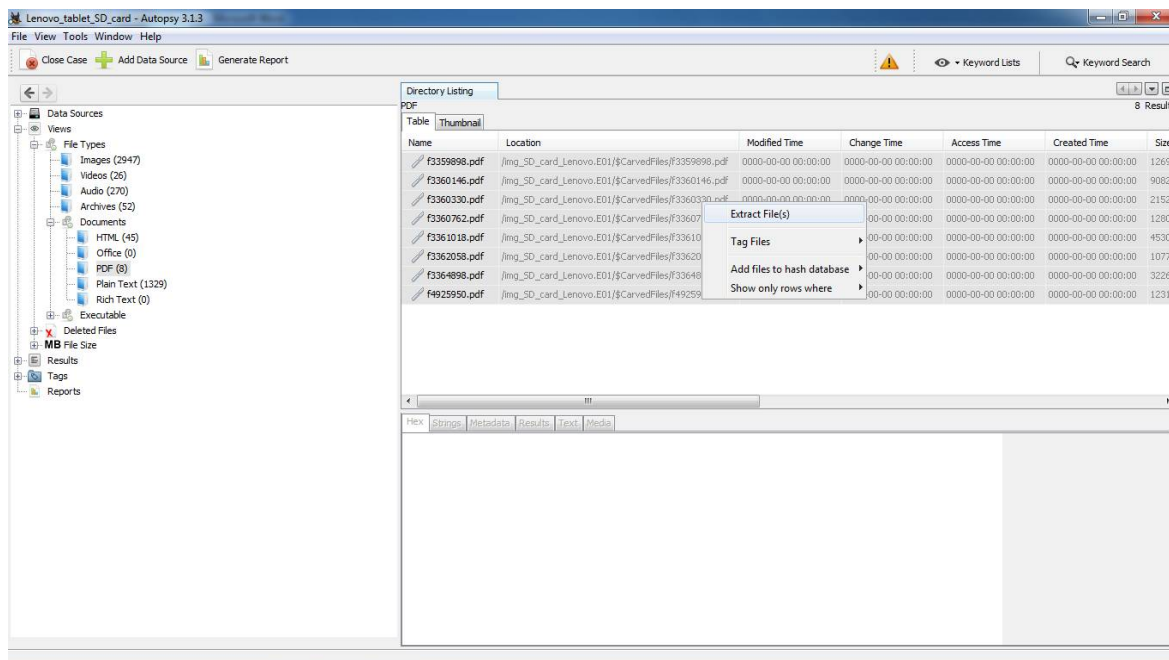
Slika 19: Pretraga analiziranog slučaja po tipu dokumenta

U prvoj fazi strage, po zahtevu vlasnika vršimo oporavak izgubljenih fajlova. Za nas najbitnije deo je iz direktorijum File Types, gde biramo Documents i naše ciljane fajlove a to su fajlovi tipa *.pdf, kojih ima 8 na SD kartici.



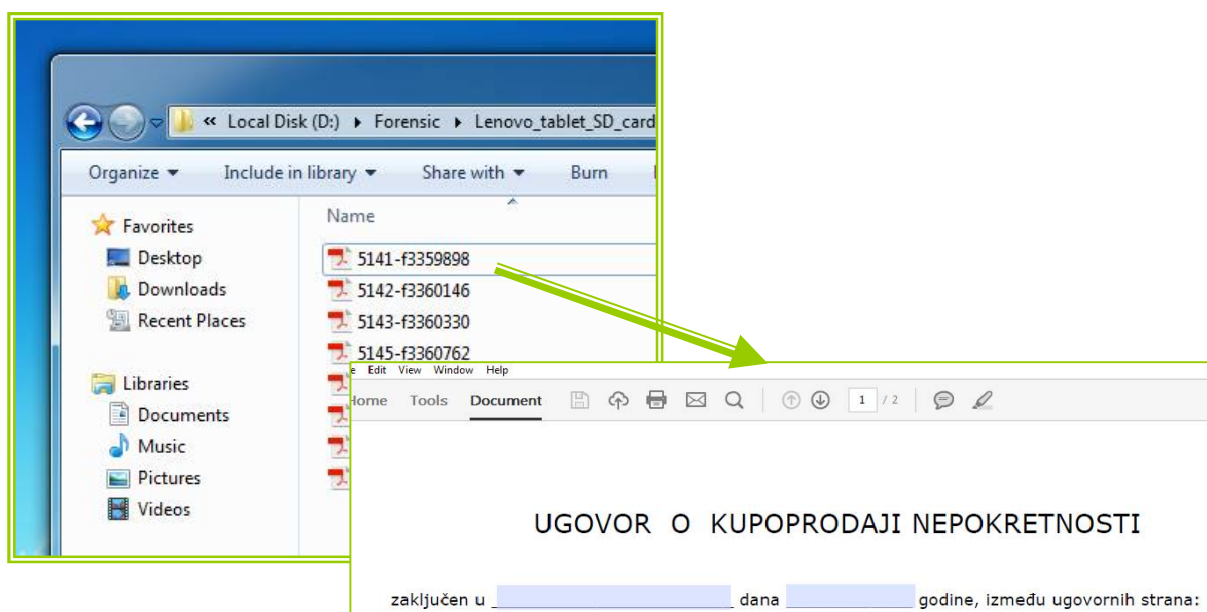
Slika 20: Pretraga analiziranog slučaja po tipu dokumenta – prikaz za pdf dokumenta

Povraćaj podataka se vrši na način tako da se izvrši izbor svih fajlova koje želimo da oporavimo selekcijom svih odjednom (Ctrl+A) ili jedan po jedan dokument ponaosob. Nakon izbora desnim klikom na komandu Extract File, vrši se oporavak fajlova u folderu Extract, u izveštaju navedene istrage.



Slika 21: Oporavljanje dokumenata

Oporavljene fajlove nalazimo u folderu u putanji koju smo sami izabrali prilikom procesa oporavka, i kopiranjem iste dostavljamo vlasniku tableta u skladu sa njegovim zahtevom.



Slika 22: Provera da li se radi o traženim dokumentima

Na osnovu imena fajlova koje smo našli kao pdf fajlove dolazimo do zaključka da je na SD kartici sadržaj izbrisan formatiranjem iste. Sada nam predstoji postupak ustanovljavanja da li je eventualno bilo narušavanja bezbednosti uređaja sa interneta, budući da vlasnik iznosi da je predmetnog dana dobio ponudu na mail sa njemu nepoznate adrese.

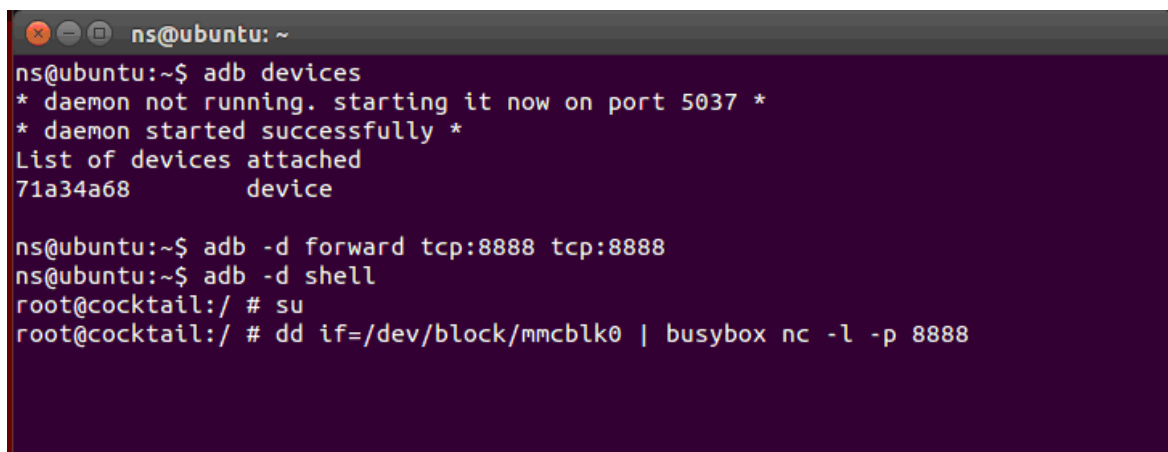
Kreiranje fajla slika (image.dd) na uređaju, dok je uključen tzv. “live image“.

Na početku se vrši provera da li uređaj ima pristup programerskim funkcijama, a ukoliko nema, potrebno je omogućiti režim popravke grešaka preko USB moda (USB debug mode). Nakon toga, vršimo nasnimavanje aplikacija Busybox i SuperSu sa Android Play marketa, ili instaliranjem direktno u ADB modu.

Nakon što je na prethodni način izvršena priprema Tablet uređaja, prelazi na povezivanje sa PC računarom preko USB, gde se uglavnom automatski vrši instalacija uređaja i driver-a. Nakon priključenja potrebno je izvršiti odobrenje i administratorske privilegije tzv. Root-ovanjem. Rootovanje izvršiti preko aplikacija dostupnih na internetu, a za ispitivani uređaj Lenovo A35000-FL, jedini način otključavanja je preko aplikacije IROOT¹⁴, jer preko SuperSu aplikacije nije bilo moguće dozvoliti administratorske privilegije.

Nakon “otključavanja” možemo preći na startovanje, pokreće radnu stanicu preko VMWARE-a i Ubuntu-a. Tokom povezivanja pratiti svaki korak i u slučaju potrebe odobravati pristup aplikacija kompjuteru, što je slučaj prilikom vezivanja na Ubuntu. Da bi počeo proces rada prelazi na rad u Terminalu.

U terminalnom prozoru redom se unose komande za kreiranje slike na način i redosledom kako je dato na sledećoj slici:



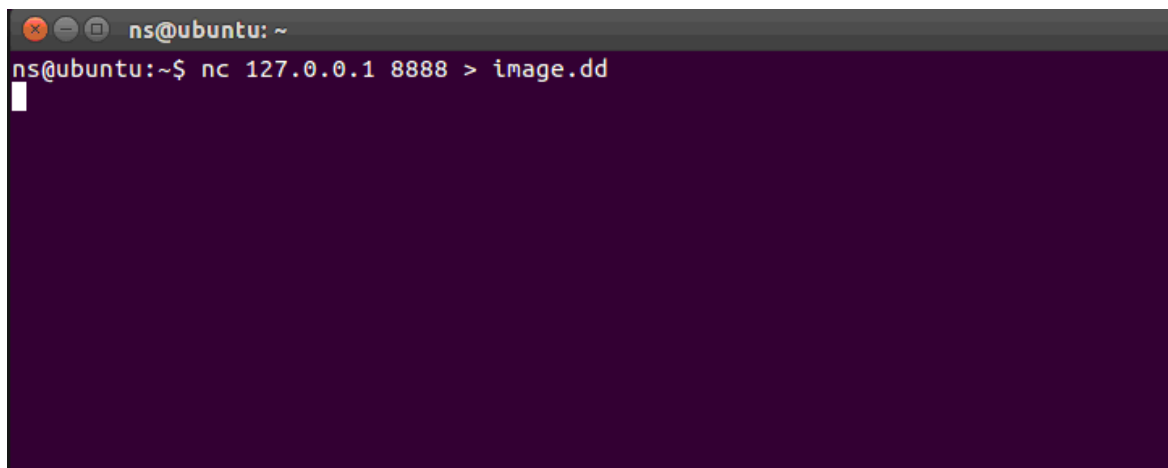
```
ns@ubuntu: ~
ns@ubuntu:~$ adb devices
* daemon not running. starting it now on port 5037 *
* daemon started successfully *
List of devices attached
71a34a68      device

ns@ubuntu:~$ adb -d forward tcp:8888 tcp:8888
ns@ubuntu:~$ adb -d shell
root@cocktail:/ # su
root@cocktail:/ # dd if=/dev/block/mmcblk0 | busybox nc -l -p 8888
```

Slika 23: Unos komandi za kopiranje- kreiranje slike

Nakon unetih naredbi za snimanje preko netcat-a, porta za čitanje i pisanje preko mreže na računaru, što ostvaruje busybox-om, otvara novi Terminalni prozor I unosi sledeću naredbu koja je data na slici koja sledi.

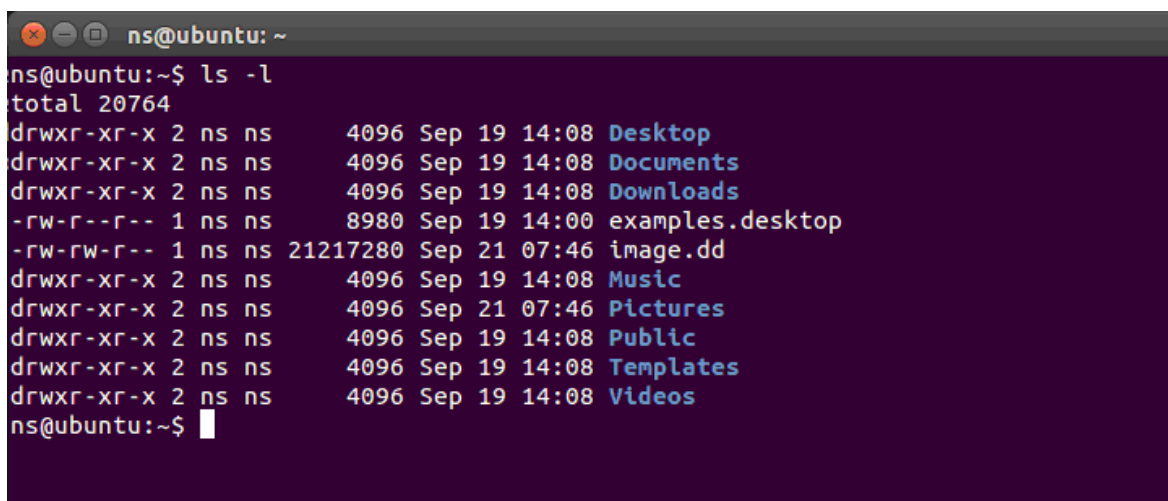
¹⁴ Preuzeto sa sajta <http://www.mgyun.com/en/getvroot>.



```
ns@ubuntu: ~  
ns@ubuntu:~$ nc 127.0.0.1 8888 > image.dd
```

Slika 24: Unos komandi za kopiranje- kreiranje slike uz čuvanje podataka na računaru

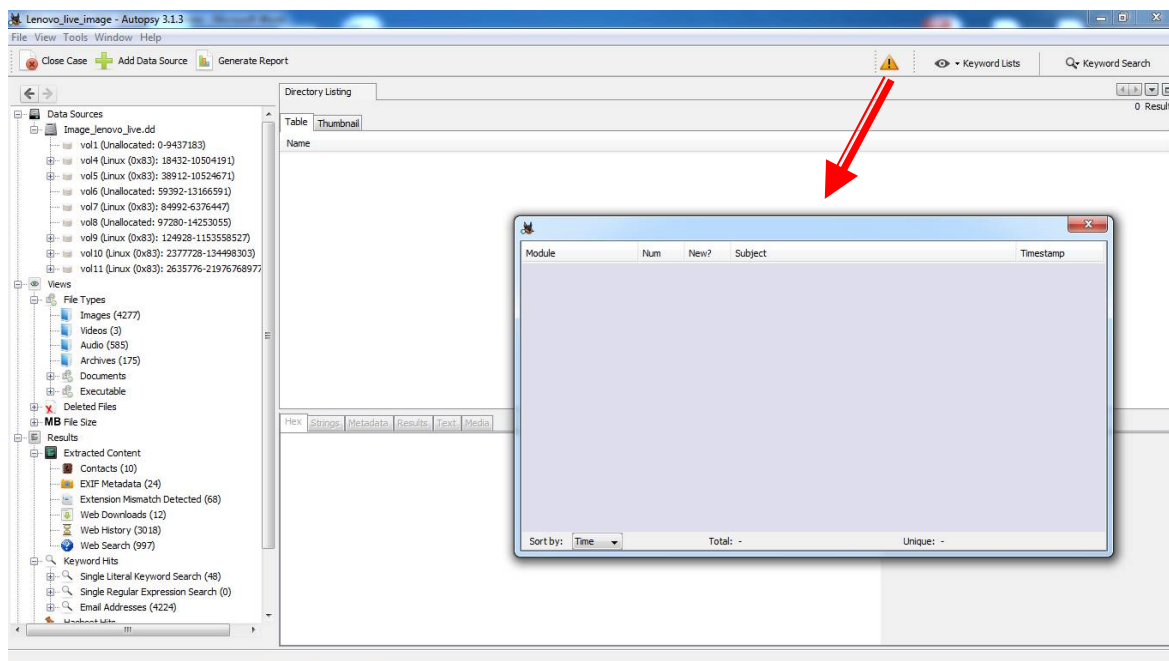
Budući da process snimanja traje duže, čak i nekoliko sati praćenje snimanja image.dd fajla je moguće davanjem naredbe kao na sledećoj slici.



```
ns@ubuntu: ~  
ns@ubuntu:~$ ls -l  
total 20764  
drwxr-xr-x 2 ns ns      4096 Sep 19 14:08 Desktop  
drwxr-xr-x 2 ns ns      4096 Sep 19 14:08 Documents  
drwxr-xr-x 2 ns ns      4096 Sep 19 14:08 Downloads  
-rw-r--r-- 1 ns ns      8980 Sep 19 14:00 examples.desktop  
-rw-rw-r-- 1 ns ns 21217280 Sep 21 07:46 image.dd  
drwxr-xr-x 2 ns ns      4096 Sep 19 14:08 Music  
drwxr-xr-x 2 ns ns      4096 Sep 21 07:46 Pictures  
drwxr-xr-x 2 ns ns      4096 Sep 19 14:08 Public  
drwxr-xr-x 2 ns ns      4096 Sep 19 14:08 Templates  
drwxr-xr-x 2 ns ns      4096 Sep 19 14:08 Videos  
ns@ubuntu:~$
```

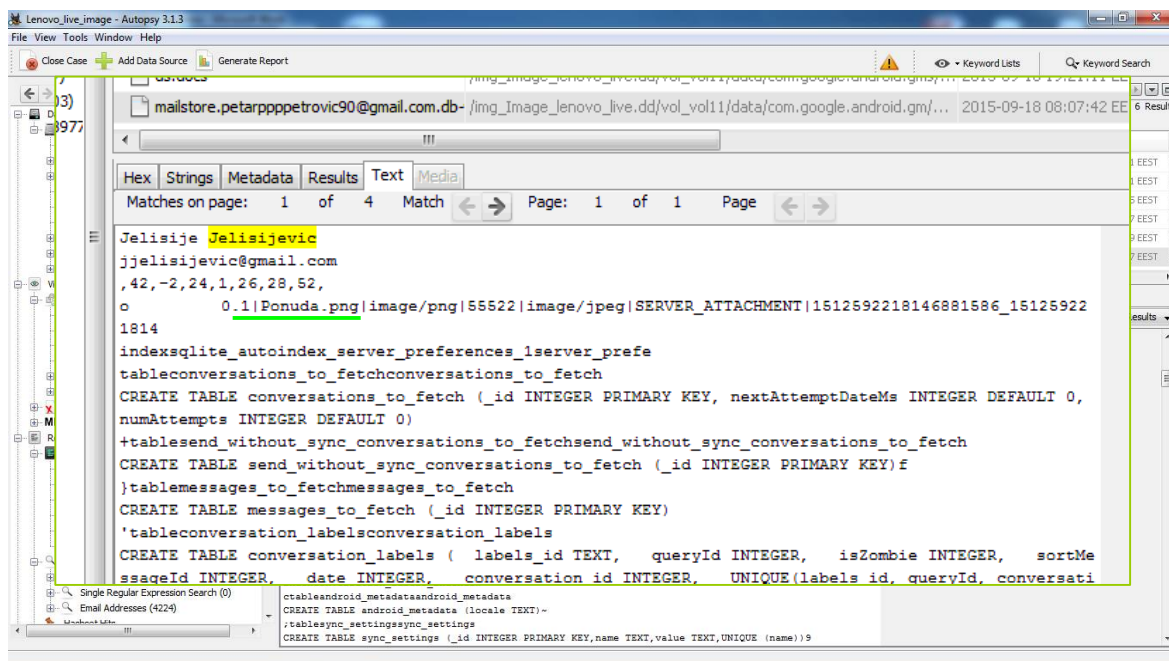
Slika 25: Praćenje procesa snimanja

Ovako kreirani fajl image.dd, unosi se na prethodno opisani način u program Autopsy 3.1.3. u modul analiza image. Analiza ovako unete slike može da zbog veličine fajla i u odnosu na jačinu računara potraje i više sati, pa treba biti strpljiv.



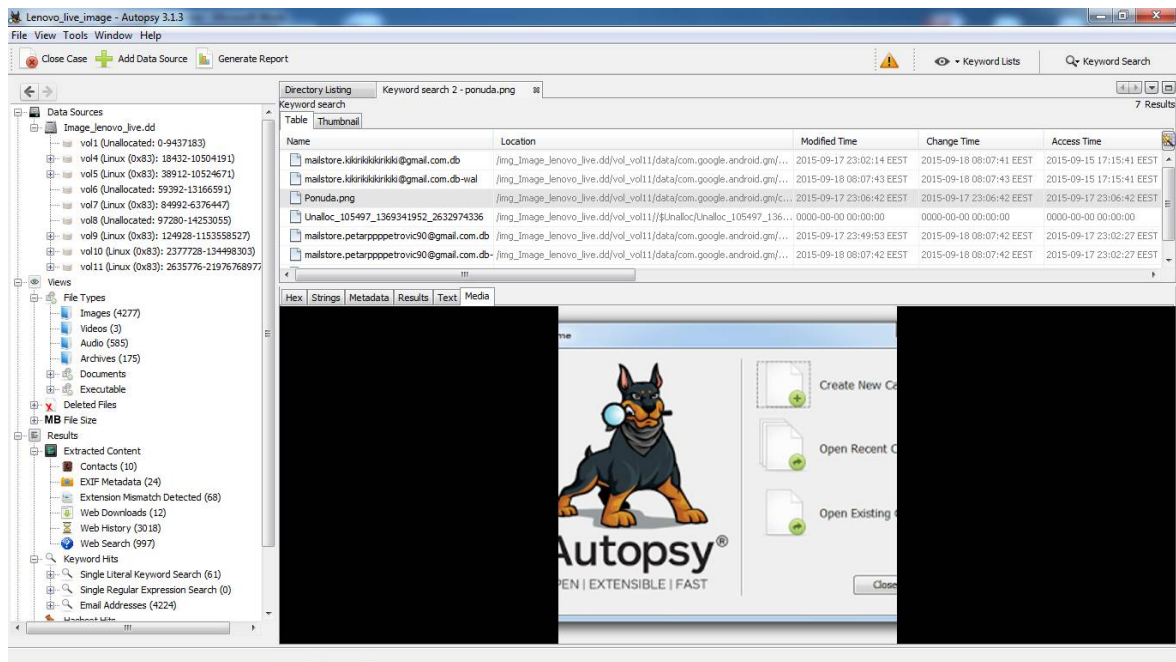
Slika 26: Interfejs za analizu žive slike Tablet računara

Vrlo bitno je da se nakon izvršene analize obavezno izvrši provera grešaka ili upozorenja na osnovu čega forenzičar usmerava svoj dalji rad (u ovom modulu se analizom ukazuje na postojanje virusa, hash funkcije i slično).



Slika 27: Pretraga po ključnoj reči

Na napred navedenoj slici je prikazana analiza I rezultati pretrage po ključnoj reči za mail koji je primljen, a pregledom ustanovljeno da nije imao u sebi izvršne naredbe.



Slika 28: Prikaz fajla u prilogu mail-a

U svakom slučaju je izvršna i pretraga priloga navedenog mail-a gde je ustanovljeno da se nalazi slika sadržaja koji je i dat u ponudi (korišćenje besplatnog alata).

Zaključak: Na osnovu izvršenih analiza sadržaja SD kartice i tablet računara ustanovljeno je da nije bilo malicioznih upada u računar, a da je formatiranje izvršeno zbog slabih nivoa zaštite računara, budući da je dostupan i porodici vlasnika računara i da je formatiranje izvršeno od strane lica iz njegovog okruženja.

11. ZAKLJUČAK

Poznavanje problema zaštite informacionih sistema kroz objekte zaštite, pretnje, posledice, mere i rizike su preduslov za uspešnu organizaciju sigurnosti samog informacionog sistema od strane lica koja se bave ovom problematikom.

Uglavnom se do sada na svim većim konvencijama povodom sigurnosti na internet mreži kao najveći problem izdvaja čovek kao korisnik, koji je nedovoljno upućen u mogućnostima korišćenja servisa sigurnosti, neophodna je kvalitetnija edukacija korisnika informacionih sistema a kroz organizacione mere (primer da svaki zaposleni ima položen ECDL i slično) i edukacija u osnovama sigurnosti, a što ovaj rad sadrži u sebi.

Pored navedenog, cilj ovog rada je bio da ukaže na obavezu zaštite podataka koji se prenose putem računarske mreže i prikaže osnovne mehanizme za njihovu zaštitu. Ovim radom su dati samo okviri kriptografije, korišćenje i sigurnost primenjenih algoritama bez konkretnih primera matematičkih operacija. Kao nauka koja se razvija brzo, sa razvojem računara, za očekivati je i njenu nadogradnju i implementaciju u sigurnosnim merama savremenih informacionih sistema.

Digitalna forenzika sa razvojem informatičke opreme u današnje vreme postaje sve popularnija i cenjenija, posebno kada se uzme u obzir činjenica da uvek postoji nastojanje treće strane da dođe do ličnih i ključnih podataka za funkcionisanje velikih korporacija danas. Digitalna forenzika kao multidisciplinarna nauka zahteva vrlo usko poznavanje funkcionisanja delova sistema za koje se vodi istraga, bilo da se radi o računaru, mobilnom telefonu ili tablet uređaju, a sa ciljem ustanovljavanja da li je i u kojoj meri narušen sistem kao i da u konačnom da predloge za unapređenje sistema bezbednosti i zaštite kako ličnih, korporacijskih tako i sistemskih podataka.

S obzirom na kompleksnost procesa koji se dešavaju kod prenosnih mobilnih uređaja na Android platformi tokom njihovog rada, u ovom radu su težišno iznete početne osnove za dalje izučavanje sa akcentom na hardver uređaja uz neophodnu softversku podršku koja pokreće uređaj. Poznavanje hardvera i softvera Android uređaja je težišno vrlo bitan postupak za akviziciju i digitalnu istragu posebno u delu smeštanja i čuvanja podataka u odnosu na primenjenu vrstu memorije. Na ovaj način se od strane forenzičara pristupa pravilnom postavljanju cilja i izboru najboljeg alata za forenzičku istragu u skladu sa postavljenim ciljem.

Sve većim nastojanjem da se u trgovinama uvedu tablet uređaji kao ulazni uređaji sistema, u školama kao zamena za knjige u nastavnom procesu, kod privatnih lica kao pouzdan uređaj sa velikom autonomijom koji pružaju komfor u svakodnevnom životu (čitanje, odnosno praćenje elektronskih medija, korišćenje aplikacija za razmenu mail poruka itd.) svakako pred nas postavlja zadatak na praćenju razvoja tablet uređaja u cilju sprovođenja uspešne forenzičke istrage istih u slučaju potrebe, bilo za potrebe javne ili tajne istrage.

Studija slučaja je pokazala da Android sistem omogućava zbog svog otvorenog koda korišćenje programerskih privilegija za izradu slike, uz određena ograničenja Linux-a.

U skladu sa postavljenim ciljem istraživanja je ukazano i na nedovoljnu edukaciju korisnika uređaja na Android platformi, što može da dovede do kompromitacije ličnih i poverljivih podataka koji se nalaze na njima.

Sveća veća težnja da se popularizuju tablet uređaji kroz razne vidove reklama i ponuda, uvođenje istih u proces edukacije, kroz nisku cenu za ovako velike mogućnosti, utiče na njihovu sve brojniju primenu i naravno sve veću težnju za izučavanje od strane lica koja će se baviti njihovim forenzičkim izučavanjem a ovaj rad je svakako ponudio jedan novi pristup.

Literatura

- [1] Goran Jović i drugi, “**Zaštita informacionih sistema**“, Naučni rad Tehnički fakultet Bor i Tehnološki fakultet Leskovac.
- [2] Prof. Dr Mladen Veinović i drugi, “**Kriptologija I**“, 2013.godine, Univerzitet Singidunum.
- [3] D. Pleskonić i drugi, “**Sigurnost računarskih sistema i mreža**“, izdanje 2007. godine, Mikroknjiga.
- [4] Behrouz A. Forouzan, “**Data Communications and Networking**“, Fourth Edition.
- [5] “**Uvod u računarstvo i informatiku**“, <https://racunarstvoiigimkg.files.wordpress.com/2013/09/uvod-u-racunarstvo.pdf>.
- [6] Prezentacija i predavanje “**Informacioni sistemi**“, <http://www.gimpi.ni.ac.rs/>.
- [7] Iz vikipedije “**Informacioni sistemi**“, <https://sr.wikipedia.org/sr/Informacioni-sistem>.
- [8] Prof. Dr Mladen Veinović i dr. Aleksandar Jevremović, “**Računarske mreže**“, 2013.godine, Univerzitet Singidunum.
- [9] Definicija DES i AES standrada kriptovanja, <http://searchsecurity.techtarget.com/definition/Data-Encryption-Standard>
- [10] Sertifikaciono telo MUP-a Republike Srbije, “**Digitalni potpis**“, <http://ca.mup.gov.rs/digitalni-potpis.html>
- [11] Visoka tehnička škola Kragujevac, odsek informatika, “**Bezbednost informacionih sistema**“, mr. Srđan Antanasijević, dipl.ing.informatike.
- [12] Dejan Đorđević, major, “**Digitalni potpis I digitalni sertifikat**“, Telfor 2007, http://2007.telfor.rs/files/radovi/01_15.pdf.
- [13] Hibridna kriptografija, **PGP algoritam**, <http://www.pgpi.org/doc/pgpintro/>.
- [14] Dejan Đorđević, major, “Digitalni potpis i digitalni sertifikat”, 15. Telekomunikacioni forum TELFOR 2007, http://2007.telfor.rs/files/radovi/01_15.pdf
- [15] Sinkovski Stevan, dipl.ing. i mr. Lučić Branislav, “**Informaciona bezbednost i kriptografija**“, Singipedia.
- [16] Milan Milosavljević, Gojko Grubor, “**Digitalna forenzika računarskog sistema**“, Univerzitet Singidunum 2009.godine.
- [17] Milan Milosavljević, Gojko Grubor, “**Istraga kompjuterskog kriminala**“, Univerzitet Singidunum 2009.godine.
- [18] Andrew Hoog, “**Android Forensics**“, Syngress 2011.godine.
- [19] <https://sr.wikipedia.org/sr/Forenzika>
- [20] <http://www.androidcentral.com/what-is-android-bootloader>
- [21] <http://whatis.techtarget.com/definition/netbook>

- [22] https://en.wikipedia.org/wiki/Google_TV
- [23] <https://maki80yu.wordpress.com/category/forenzika/>
- [24] <http://www.gfi.com/blog/top-20-free-digital-forensic-investigation-tools-for-sysadmins/>
- [25] <https://www.guidancesoftware.com/products/Pages/encase-forensic/overview.aspx>
- [26] <http://support.lenovo.com/us/en/products/tablets/a-series/a7-40-tablet>
- [27] <http://developer.android.com/sdk/index.html>
- [28] <http://developer.android.com/tools/help/adb.html>
- [29] <http://accessdata.com/product-download/digital-forensics/forensic-toolkit-ftk-version-5.5>
- [30] <http://sleuthkit.org/autopsy/docs/user-docs/3.1/>
- [31] <http://support.lenovo.com/us/en/products/tablets/a-series/a7-40-tablet>
- [32] <http://forum.xda-developers.com/showthread.php?t=2499423>
- [33] <http://freeandroidforensics.blogspot.rs/2014/08/live-imaging-android-device.html>
- [34] <http://shop.lenovo.com/sa/en/smartphones/s-series/s930/>