

UNIVERZITET SINGIDUNUM

DEPARTMAN ZA POSLEDIPLOMSKE STUDIJE

MASTER STUDIJE

MASTER RAD

FORENZIČKA ANALIZA PRENOSNIH RAČUNARA I USB MEMORIJA

Mentor:
Prof. dr Gojko Grubor

Student:
Slaviša Andrejić
Br. Indeksa 410758/2011

- Jun 2014. godine -

Spisak slika i tabela

Slika 1: USB memorija 12
Slika 2: Primer glavnog ekrana PDA sa Palm OS 6.1 15
Slika 3: IPod tuch i IPhone 5 21
Slika 4: Nivo ukupne bezbednosti u funkciji komponenti bezbednosti 24
Slika 5: Nivo ukupne bezbednosti IKTS u funkciji pretnji 25
Slika 6: Generički model sistema zaštite i međusobni odnosi komponenti 31
Slika 7: Arhitektura fleš memorijskog čipa u odnosu na MTD 43
Slika 8: Skrivanje podataka u lošim blokovima 45
Slika 9: Solid state drive (SSD) controller 45
Slika 10: Sadržaj foldera ''Projekat Studija Slucaja'' na ''računaru firme ABD'' 57
Slika 11: Interfejs programa USBDeview, sa podacima o tretiranom USB disku 58
Slika 12: Sadržaj igrajućeg USB diska, nakon privremenog oduzimanja 59
Slika 13: Rezultat skeniranja USB diska alatom Active@UNDELETE 59
Slika 14: Ključ HKLM\SYSTEM\CurrentControlSet\Enum\USB..... 61
Slika 15: Ključ HKLM\SYSTEM\ControlSet00x\Enum\USBSTOR..... 62
Slika 16: Ključ HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices..... 63
Slika 17: Prikaz događaja u Event logu, povezanog sa igrajućim USB diskom..... 63

Tabela 1: Klasifikacija informacione imovine 29

SADRŽAJ:

1. Metodologija naučnog istraživanja ..... - 7 -
1.1 Uvodne napomene i obrazloženje rada ..... - 7 -
1.2 Predmet istraživanja ..... - 9 -
1.3 Ciljevi istraživanja ..... - 10 -
1.4 Hipotetički okvir ..... - 10 -
1.5 Metode i tehnike istraživanja ..... - 10 -

2. Prenosni računari i USB memorije ..... - 12 -
2.1. USB memorije ..... - 12 -
2.1.1 Bezbednosni rizici upotrebe USB memorija ..... - 13 -
2.2 Lični digitalni asistent (Personal digital assistant) – PDA ..... - 15 -
2.2.1 Karakteristike PDA ..... - 16 -
2.2.2 PALM OS ..... - 16 -
2.2.3 Windows C ..... - 17 -
2.2.4 PDA bazirani na LINUX-u ..... - 18 -
2.2.5 Generička stanja PDA ..... - 19 -
2.2.6 ActiveSinc i HotSinc opcije ..... - 19 -
2.2.7 Bezbednosni rizici povezani sa korišćenjem PDA: ..... - 20 -
2.3 iPod i iPhone ..... - 21 -
2.3.1 Operativni sistem iPhone ..... - 22 -
2.3.2 Apple HFS i FAT32 ..... - 22 -
2.3.3 Bezbednosni rizici povezani sa korišćenjem iPod i IPhone ..... - 23 -

3. Bezbednost informacija ..... - 24 -
3.1 Definicije pojmova bezbednost i sigurnost informacija ..... - 24 -
3.2 Funkcionalna zavisnost bezbednosti i pretnji ..... - 25 -
3.3 Glavni faktori uticaja na bezbednosno stanje IKTS ..... - 26 -
3.4 Opšta definicija sistema zaštite ..... - 27 -
3.5 Osnovne funkcionalnosti sistema zaštite ..... - 28 -
3.6 Informacioni sistem kao objekat zaštite ..... - 28 -
3.7 Generički, funkcionalni model sistema zaštite ..... - 31 -
3.8 Definisanje optimalnog sistema zaštite ..... - 32 -

4. Digitalni dokazi ..... - 33 -
4.1 Faze istrage ..... - 35 -
4.2 Pravosudni aspekt digitalnih kompjuterskih dokaza ..... - 36 -
4.3 Karakteristike forenzičkih alata za kreiranje precizne kopije digitalnih dokaza - 37 -
4.4 Upravljanje digitalnim dokazima ..... - 37 -
4.5 Procedura sakupljanja posrednih kompjuterskih dokaza ..... - 38 -
4.6 Korisnici digitalnih dokaza ..... - 40 -
4.7 Priprema digitalnih dokaza za veštačenje pred sudom ..... - 40 -
4.8 Preporuke IOCE za upravljanje digitalnim dokazima ..... - 41 -

5. Digitalna forenčka analiza prenosnih računara i USB memorija ..... - 42 -
5.1 Specifičnosti fleš tehnologije od značaja za izbor forenzičkih alata i procedura - 42 -
5.1.1 FLASH TRANSLATION LAYER (FTL) ..... - 43 -
5.1.2 Kontroleri ..... - 44 -
5.1.3 Mapiranje ..... - 44 -
5.1.4 Brisanje podataka i manipulacije skrivenim zonama ..... - 44 -
5.2 Solid State Drive (SSD) ..... - 45 -
5.3 Specifičnosti mobilnih telefona od značaja na digitalnu forenzičku analizu ..... - 49 -
5.3.1 Digitalni dokazi na mobilnim telefonima ..... - 50 -
5.3.2 Potencijalni dokazni materijal na SIM kartici ..... - 51 -
5.3.3 Digitalna forenzika mobilnih telefona ..... - 52 -
5.3.4 Metode akvizicije podataka ..... - 52 -
5.3.5 Akvizicija digitalnih dokaza iz mobilnih telefona i alati za akviziciju ..... - 54 -
5.3.6 Manuelni pregled mobilnih telefona ..... - 54 -
5.3.7 Akvizicija putem konekcionih servisa ..... - 54 -
5.3.8 Direktan pristup memoriji ..... - 55 -

6. STUDIJA SLUČAJA ..... - 57 -
6.1 Identifikacija neovlašćene upotrebe USB memorija i oporavak izbrisanih podataka sa USB memorije ..... - 57 -
6.1.1 Scenario ..... - 57 -
6.1.2 Priprema USB memorije i igrajućeg službenog računara ..... - 57 -
6.1.3 Profilisanje – potpuna identifikacija USB memorije ..... - 58 -
6.1.4 Oporavak izbrisanih podataka sa USB memorije ..... - 59 -
6.1.5 Identifikacija neovlašćene upotrebe USB memorije ..... - 60 -

ZAKLJUČAK ..... - 64 -

LITERATURA ..... - 66 -

Sažetak:

Prenosni računari i USB memorije su sve zastupljeniji u procesima informatičke obrade i skladištenja podataka, kako za potrebe pravnih subjekata tako i fizičkih lica. Na to utiču njihove karakteristike (male mase i gabariti, velike brzine rada i kapacitet skladištenja podataka, multifunkcionalnost i sposobnost povezivanja sa drugim uređajima na različite načine i drugo), koje se po zakonitostima tržišne ekonomije, unapređuju gotovo svakodnevno.

Navedene karakteristike, koje su ujedno i specifičnosti prenosnih računara i USB memorija u odnosu na standardne desktop računare, nesumnjivo doprinose unapređenju privatne i službene komunikacije, olakšavanju i ubrzavanju realizacije službenih zadataka i ličnih obaveza. S druge strane utiču na povećanje bezbednosnih rizika njihove primene i planiranja adekvatnih,optimalnih sistema zaštite.

S obzirom na moguću primenu prenosnih računara i USB memorija, vrstu i količinu potencijalnih digitalnih dokaza koje mogu da sadrže, iziskuju posebne mere, postupke i alate za digitalnu forenzičku analizu i konstantnu modernizaciju tih mera, postupaka i alata.

Ključne reči: Prenosni računari, USB memorije, bezbednosni rizici, optimalni sistem zaštite, digitalni dokazi, digitalna forenzička analiza

Abstrakt:

Portable devices and USB flash drives become more and more present in informatic processes and storage of data for the legal entities as well as natural persons. Their numerous features, such as small weight and dimensions, high velocity of work and storage capacity, multi-functionality and the ability to connect to other devices in different ways, etc. are responsible for their presence in the mentioned fields. Global market competition demonds for improving of portable devices and USB flash drives characteristics almost on daily basis.

These characteristics, which are also the specifics of Portable devices and USB flash drives over standard desktop PCs, undoubtedly contribute to the improvement of private and official communication, facilitating and accelerating the implementation of official duties and personal commitments. On the other hand, they increase security risks of their use and planning adequate,optimal protection system.

With regard to the possible application of Portable devices and USB flash drives, the type and quantity of potential digital evidence that may contain, they require special measures, procedures and tools for digital forensic analysis and constant modernization of the measures, procedures and tools.

Key words: Portable devices, USB flash drives, security risks, optimal protection system, digital evidence, digital forensic analysis

1. Metodologija naučnog istraživanja

1.1 Uvodne napomene i obrazloženje rada

Gotovo svakodnevna modernizacija i razvoj informacione tehnologije (**IT**) uslovili su sve masovniju upotrebu prenosnih računara (***portable devices***) i USB memorija (***USB flash drives***) u procesima informatičke obrade i skladištenja podataka, kako u privatnom – ličnom životu pojedinaca, tako i u službenoj - korporativnoj upotrebi. Na taj način unapređene su mogućnosti za poslovanje, laku i brzu razmenu informacija i usluga, ali je stvoren i ogroman prostor za razne zloupotrebe. Prenosni uređaji, s obzirom na sve veće skladišne kapacitete, mogu sadržati informacije i podatke koji po svom karakteru nisu za javnu eksploataciju, ili čijom neovlašćenom upotrebom ili obelodanjivanjem mogu nastupiti određene štetne posledice po vlasnika tih informacija.

Prenosni (**portable**) računari predstavljaju posebnu vrstu personalnih računara prilagođenu korisnicima koji imaju potrebu da računar nose sa sobom. Ovi prenosni računari, osim standardnog, imaju i baterijsko napajanje koje im omogućava višečasovni samostalni rad.

U grupu prenosnih računara spada veći broj uređaja, kao što su: laptop i notebook računari, **IPod** (*iPad*), **PDA** (*Personal Digital Assistants*), prenosni hard diskovi, mobilni telefoni (posebno kategorija takozvanih pametnih telefona (***smartphones***)). Njihove najznačajnije karakteristike ogledaju se u malim dimenzijama, samostalnosti u radu, brzini rada, velikom kapacitetu skladištenja podataka, različitim mogućnostima povezivanja i prenosa podataka. Na gotovo sve navedene uređaje, uključujući i pojedine mobilne telefone, mogu se konektovati USB memorije.

Laptop i notebook računari su prenosni računari prosečne mase do 3 kg i dimenzija približnih A4 formatu papira. Mogu da obavljaju zadatke kao i standardni PC računari. Delovi laptop računara slični su onim u standardnim PC računarima, ali su manjih dimenzija i prilagođeni za mobilne korisnike (otporni na potrese, promene temperature i imaju smanjenu potrošnju energije). Pored toga, laptop računari imaju ugrađen **LCD** (*Liquid Crystal Display*) ekran i tastaturu sa donekle drugačijim rasporedom tastera u odnosu na standardne PC računare, zbog manjih dimenzija. Na tastaturi može da se nalazi poseban taster (*pointing stick*) u obliku gumice na olovci ili poseban senzor (*touch pad*) površine nekoliko kvadratnih centimetara i osetljiv na dodir, a koji zamenjuju fukcije miša. Imajući u vidu ogromnu sličnost sa desktop računarima, laptop i notebook računari, neće biti u fokusu ovog rada.

Mobilnost i male dimenzije prenosnih računara i USB memorija, između ostalog, predstavljaju povoljnu okolnost da budu zloupotrebljeni u svrhu neovlašćenog kopiranja i skladištenja poverljivih informacija i podataka korporacije, preduzeća, ili neke druge organizacije (Vojska, Policija, Sud i dr.). S obzirom na samostalnost u radu, navedeni uređaji se mogu koristiti van kontrolisane lokacije (radne sredine), pa je povećan rizik od njihove krađe, a samim tim i neovlašćenog pristupa nasnimljenim podacima.

Osim krađom, do neovlašćenog pristupa podacima uskladištenim na ovim uređajima može se doći posredstvom bežične (Wi-Fi) i *Bluetooth* konekcije, s obzirom da većinu savremenih prenosnih uređaja ovog tipa karakteriše i mogućnost ovakvog načina povezivanja.

Kada su u pitanju informacije ili podaci koji se čuvaju ili obrađuju na pomenutim uređajima, poseban bezbednosni rizik predstavlja činjenica da pojedini zaposleni u firmama, institucijama ili ustanovama, praktikuju da fajlove sa podacima sa radnog mesta ponesu sa sobom i van radnog vremena ih obrađuju na kućnim računarima, nakon čega fajlove vraćaju na službene računare ili mrežu.

Bezbednost prenosnih računara i USB memorija može se povećati upotrebom lozinki i enkripcijom. Prilikom obrade podataka na javnim mestima treba uzeti u obzir da informacije koje se prikazuju na ekranu uređaja mogu biti vidljive neovlašćenim licima, a potrebno je izbegavati i upotrebu nezaštićenih javnih mreža. Takođe, u cilju zaštite pohranjenih informacija, prenosne računare i USB memorije treba čuvati na bezbednom mestu kada su van upotrebe.

Kada se govori o bezbednosti prenosnih računara i USB memorija, primarno se misli na bezbednost informacija (podataka) sadržanih na ovim uređajima, a sekundarno na bezbednost samih uređaja (posredna zaštita informacija).

Imajući u vidu da se nedozvoljena - kriminalna upotreba prenosnih računara i USB memorija široko rasprostanila, a da postojeće tehnike računarske forenzike nisu bile dovoljne za forenzičko ispitivanje navedenih uređaja, ranih 2000-tih godina, razvijena je relativno mlada oblast digitalne forenzike – forenzika mobilnih uređaja (***Mobile device forensics***), koja se odnosi na forenzičko ispitivanje bilo kog digitalnog uređaja koji ima internu memoriju i komunikacijske sposobnosti, uključujući PDA i GPS uređaje i tablet računare [35].

Na prenosnim računarima - mobilnim uređajima, može se čuvati velika količina podataka, dokumenata, slika, audio i video fajlova, podataka o komunikaciji korisnika uređaja (SMS i MMS poruke, evidencija poziva, liste kontakata i telefona - IMEI / ESN informacije, poruke elektronske pošte i druge komunikacije putem bežičnog pristupa internetu (GPRS, EDGE, 3G, Wi-Fi)). Multifunkcionalnost mobilnih uređaja već dostiže mogućnosti personalnih računara, ali ide i korak dalje jer integriše i uređaje kao što su fotoaparati, video kamere, snimači zvuka i uređaji za GPS navigaciju (podaci o geolociranju, uključujući i geografske oznake sadržane u metapodatacima slika).

Razvojem tehnologije izrade prenosnih računara i USB memorija, raste količina i vrsta podataka koji se mogu naći na tim uređajima. Dokazi, koji se potencijalno mogu oporaviti – povratiti sa mobilnih uređaja mogu poticati iz nekoliko različitih izvora, uključujući internu memoriju prenosnog računara, ili mobilnog telefona, SIM kartice i priključene memorijske kartice. Eksterni (spoljni) memorijski uređaji su SIM kartice, SD kartice, MMC kartice, CF kartice i Memory Stick.

Zbog konkurentnosti na tržištu, originalni proizvođači prenosnih računara i USB memorija, često menjaju oblike novih uređaja, operativni sistem, strukturu datoteka, način čuvanja podataka, usluge, periferalije, pa čak i pinske konektore i kablove. Ne samo po pitanju vrste podataka koji se mogu sačuvati, ovi uređaji iz dana u dan evoluiraju i po načinu primene.

Sa aspekta digitale forenzičke istrage za potrebe bezbednosnih službi, vođenja krivičnog postupka, ali i obezbeđivanja korporativne zaštite, napred navedene karakteristike čine prenosne računare bogatim izvorom različitih podataka i informacija, koje se ne mogu sagledati bez primene posebnih alata i procedura.

Rezultat navedenih izazova su širok spektar alata za pribavljanje digitalnih dokaza iz prenosnih računara i mobilnih uređaja. Tehnologiju i tržište fleš memorijskih čipova koji su uglavnom zastupljeni kod prenosnih uređaja, osim raznolikosti, okružuje i visok stepen poverljivosti što dodatno utiče na razvoj univerzalnih alata za njihovu digitalnu forenzičku analizu.

Postupak forenzičkog istraživanja prenosnih računara i USB memorija uglavnom obuhvata procedure koje su zastuplene i kod drugih grana digitalne forenzike, ali sadrži i neke posebne postupke. Forenzički alati pribavljaju podatke sa uređaja fizičkom ili logičkom akvizicijom koje se razlikuju po tome da li se uskladišteni podaci posmatraju po procesima u operativnom sistemu (***logical view***) ili u odnosu na memoriju u sirovom obliku, po srodnim hardverskim komponentama (***physical view***). Fizička akvizicija u odnosu na logičku pruža mogućnost ispitivanja izbrisanih fajlova i podataka (u neraspoređenoj memoriji - *unallocated memory*, ili u prostoru sistemskih datoteka - *file system space*), koji bi inače bili nedostupni [15].

U ovom radu je dat je osvrt na rad sa digitalnim dokazima i specifičnosti prenosnih računara i USB memorija kao izvora digitalnih dokaza i drugih informacija. Pored ovoga dato je i razmatranje pojedinih načina, alata i procedura prikupljanja podataka sa pomenutih uređaja sa aspekta digitalne forenzičke analize u krivičnom postupku u odnosu na forenziku desktop računara koja je već u značajnoj meri standardizovana.

1.2 Predmet istraživanja

Predmet istraživanja ovog rada je sagledavanje bezbednosnih rizika upotrebe prenosnih računara i USB memorija u odnosu na benefite i načine njihove upotrebe kako bi se ukazalo na potrebu primene adekvatnih mera i postupaka bezbednosne zaštite radi sprečavanja eventualnog nastupanja štetnih posledica po sistem.

Takođe, izradom rada, nastojalo se na ukazivanju specifičnosti prenosnih računara i USB memorija sa aspekta digitalne forenzičke analize, pri čemu su pojedini karakteristični postupci obrađeni kroz praktičan primer.

1.3 Ciljevi istraživanja

Glavni cilj rada je ukazivanje na specifičnost planiranja mera zaštite informacija i informacione imovine (informacije, hardver, softver i ljudi) usled sve zastupljenije primene prenosnih računara i USB memorija, s obzirom da mikrolokacija primene ovih mera prevazilazi okvire – posed korporacije na koju se odnose.

Poseban cilj ovog rada je da ukaže na karakteristike prenosnih računara i USB memorija koje su bitne za kvalitetnu digitalnu forenzičku analizu pomenutih uređaja i obezbeđivanje čvrstih dokaza sa stanovišta sudskog procesa.

1.4 Hipotetički okvir

Opšta hipoteza

Subjekti čije je poslovanje povezano sa skladištenjem, obradom, ili čuvanjem informacija (korporacije, firme, Vojska, Policija i dr.) sve češće se sreću sa problemima koji su posledica nepravilnog ili neovlašćenog korišćenja službenih ili privatnih prenosnih računara i USB memorija. Dijapazon ovih posledica je širok, od namerne krađe podataka ili širenja malvera, do nenamernog gubljenja uređaja sa informacijama nasnimljenim za doradu u kućnim uslovima.

Posebna hipoteza

Veliki kapacitet skladištenja i brzine obrade podataka, kao i broj funkcija koje mogu obaviti, utiču na sve masovniju upotrebu prenosnih računara i USB memorija, pri čemu je ta upotreba često i kriminalnog karaktera. S obzirom na specifičnosti koje ih karakterišu, zahtevaju dodatne veštine, znanja, ali i forenzičke alate i procedure, tj. složeniju forenzičku analizu u odnosu na, donekle standardizovanu digitalnu forenzičku analizu personalnih računara.

1.5 Metode i tehnike istraživanja i tok istraživačkog procesa

Metoda naučnog istraživanja je sistematski, kritički, kontrolisani i ponovljivi proces sticanja novih znanja, neophodnih za identifikovanje, određivanje i rešavanje naučnog problema. U ovom naučnom istraživanju primenjeni su glavni principi: *sistematičnost, kontrolisanost i kritičnost.* Primenjena su teorijska i empirijska istraživanja radi rešavanja hipotezom postavljenih problema. Istraživanje je izvršeno kroz faze *pripremne*, uglavnom teorijskog karaktera, *prikupljanja i obrade podataka*, *izvođenja eksperimentalne verifikacije, interpretacija rezultata, izvođenje zaključaka i validacija hipoteze.*

U ovom istraživačkom radu korišćene su različite metode istraživanja. Od *opšte naučnih metoda* korišćene su statistička metoda, metoda modelovanja i analitičko-deduktivna metoda. Takođe su korišćene *osnovne, opšte metode društvenih nauka*: pozitivistička metoda, metoda razumevanja, komparativna metoda, metoda idealnih tipova, metodološki funkcionalizam i strukturalizam i dijalektičke metode.

Od *posebnih naučnih metoda i tehnika* primenjene su: analitičko-sintetička metoda, metoda apstrakcije i konkretizacije, metoda generalizacije i specijalizacije, metoda klasifikacije, logičke metode indukcije i dedukcija, kao i metoda spoznaje i dijalektičkog jedinstva indukcije i dedukcije.

Od *tehnika istraživanja* u radu su primenjivane tehnike: *ocene, sređivanja, obrade podataka i zaključivanja.*

Tok istraživanja, kao prvi logični korak uključuje *prikupljanje literature* o metodologiji naučnog istraživanja i digitalnoj forenzičkoj istrazi sa težištem na forenziku fleš memorija, zatim, istraživanje desk metodom literaturnih podataka i materijala preuzetih iz raznih izvora, kroz faze otkrivanja, opisivanja i objašnjavanja određenih faza digitalne forenzičke istrage. Rad je struktuiran u određene celine i svaka od njih konkretno objašnjava glavne faze i procese digitalne forenzičke istrage prenosnih računara i USB memorija.

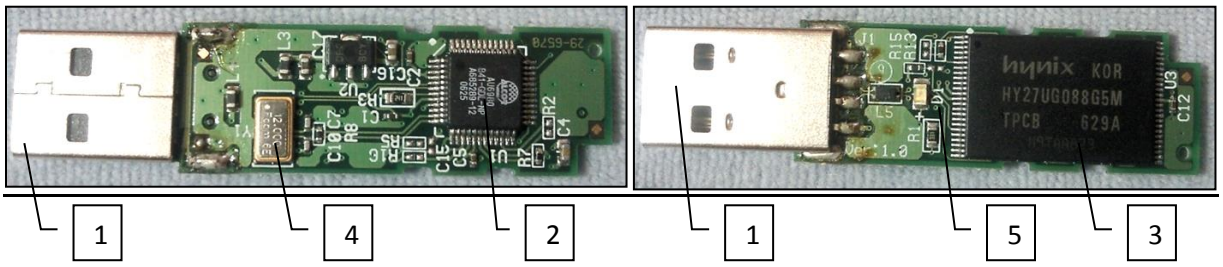
2. Prenosni računari i USB memorije

2.1. USB memorije

USB ili fleš memorija je medijum za skladištenje digitalnih podataka, baziran na fleš memoriji NAND tipa i opremljen USB priključkom preko koga može da komunicira sa računarom ili nekim drugim uređajem. Pandan je disketama, CD i DVD diskovima od kojih je jednostavniji za upotrebu. Sve masovnije su u upotrebi, a posebno tamo gde je bitno da su podaci pohranjeni na fizički što manjem mediju [30].

Fleš memorija NAND tipa ili fleš EEPROM je vrsta EEPROM (Electrically-Erasable Programmable Read-Only Memory) memorije, kod koje se bajtovi ne mogu pojedinačno brisati.

USB memorije sa računarom komuniciraju preko Universal Serial Bus (USB) porta koristeći se USB 1.1. ili 2.0 interfejsom. Podržavaju razne brzine prenosa podataka, a u slobodnoj prodaji danas se mogu naći u veličinama od 64MB do 64GB. Kao izvor energije za rad uređaja služi napajanje koje se dobija preko USB konektora, pa ne zahtevaju baterije. Koriste USB *mass storage* standard koji podržavaju najnovije verzije operativnog sistema kao što su Linux, MAC i Windows. Ovi uređaji su poznati kao i USB stikovi, USB diskovi i sl. Da bi se pristupilo podacima koji su smešteni na USB fleš drajvu korisnik mora da konektuje uređaj na USB port ili USB HUB, priključen na računar ili neki drugi uređaj [28,34].



1. - USB priključak
2. - Upravljački uređaj
3. - Memorijski čip
4. - Kvarcni oscilator
5. - LED lampica

Slika 1: USB memorija

USB memorije se sastoje od male štampane elektronske ploče smeštene u plastično ili metalno kućište, a USB konektor je obično zaštićen odvojivim poklopcem. Najčešće se koriste za transver podataka sa jednog računara na drugi, preduzimanje ili obavljanje zadataka administratora sistema, transvera aplikacija, čuvanje muzike (filmova, fotografija, i sličnih podataka), kao i za podizanje operativnog sistema.

Osim navedenih, najčešćih načina upotrebe, USB memorije mogu biti i zloupotrebljene za smanjivanje broja dokaznih materijala na računaru. Naime, počin1ac izvesnog krivičnog dela koji je svestan svoje krivice, pokušaće da se zaštiti od mogućeg forenzičkog tratmana, tako što neće dopustiti da unutrašnji mediji računara dođu u dodir sa osetljivim informacijama, pri čemu u ovu svrhu može koristiti USB memorije, prenosne hard diskove, virtualne diskove, virtualne operativne sisteme i butabilne operativne sisteme [7].

2.1.1 Bezbednosni rizici upotrebe USB memorija

Najveći rizici po bezbednost informacionog sistema usled korišćenja USB memorija ogledaju se u takozvanom curenju podataka, za šta su USB memorije pogodne zbog svoje male veličine i sveprisutnosti. Posebna vrsta rizika pri upotrebi USB memorija predstavlja to što su pogodne za širenje malicioznih programa [28].

Veliki kapacitet USB memorija, uz male gabarite i niske cene, utiče na njihovu masovnu upotrebu za skladištenje podataka, što bez adekvatnih operativnih i logičkih kontrola može predstavljati ozbiljnu pretnju poverljivosti, integritetu i dostupnosti informacija. Kada je u pitanju bezbednost informacionih sistema treba uzeti u obzir da je sa radnih stanica bez nadzora, USB memorije teško fizički pratiti, jer mogu da se ponesu u rančevima, torbicama, džepovima pantalona i jakni i slično.

Otkrivanje i ustanovljavanje korporativnih podataka, na ličnim – privatnim USB memorijama je veliki izazov za korporacije – organizacije iz više razloga, pa mnoga preduzeća imaju strogu politiku zaštite svojih sistema kada su u pitanju USB diskovi, pri čemu ih neke od kompanija zabranjuju, kako bi se smanjio bezbednosni rizik. Sa druge strane, pojedine organizacije i nisu svesne rizika koji ovi uređaji predstavljaju po sigurnost sistema [28, 29].

Prema istraživanju kompanije SanDisk, iz 2008.godine, krajnji korisnici najčešće kopiraju sledeće korporativne podatke [28]:

podatke o potrošačima /korisnicima usluga (25%),
podatke o finansijama (17%), poslovne planove (15%),
podatke o zaposlenima (13%),
podatke o planovima u oblasti marketinga (13%),
intelektualna svojina (6%),
izvorne kodove (6%).

Po nastanku računarskih virusa i malicioznog softvera, osnovno sredstvo prenosa infekcija bile su diskete. Umesto disketa, USB memorije se danas najčešće koriste za transver podataka (sa jednog na drugi računar), pa su samim time i najčešći oblik širenja infekcije malicioznim kodom. Kada zlonamerni siftver dospe na USB memoriju, ona kasnije može inficirati uređaje na koje se nakon toga priključuje. Prema istraživanju kompanije Microsoft iz 2011.godine, od ukupnog broja infekcija Windows operativnog sistema, 26% se odnosi na zloupotrebu funkcije Autorun kod USB memorija.

Windows fajl **Autorun.inf** sadrži informacije o programima koji treba da se pokrenu automatski kada se prenosnom mediju (najčešće USB memoriji i sličnim uređajima) pristupi sa Windows platforme. Podrazumevana postavka Autorun u verzijama Windowsa, pre Windowsa 7, automatski pokreće program naveden u autorun.inf fajlu, kada se pristupa raznim vrstama prenosnih medija. Mnoge vrste malicioznog softvera se samostalno kopiraju na prenosni medij, ali to nije primarni mehanizam distribucije, jer autori malvera često ugrađuju i dodatne tehnike infekcija.

2.2 Lični digitalni asistent (Personal digital assistant) – PDA

Lični digitalni asistent **(*Personal digital assistant*) - PDA** je mobilni uređaj koji je poznat i kao ručni računar. To je mali, laki uređaj koji se koristi za obradu i skladištenje podataka, sa mogućnošću korišćenja privatnih i poslovnih aplikacija. U današnje vreme ogromna većina PDA su ujedno i takozvani smart telefoni jer omugućavaju i uslugu komunikacije. Originalno je bio dizajniran kao lični organajzer, ali je do sada razvijen kao svestran višenamenski digitalni uređaj. Najveći broj PDA ima malu tastaturu, a mnogi novi uređaji umesto toga imaju tastaturu osetljivu na dodir, od tečnog kristala sa mogućnošću prepoznavanja rukopisa. U svrhu razmene podataka, PDA može da se sinhromizuje sa desktop ili laptop računarom. Sinhronizacijom se zanavljaju podaci na oba sistema tako da se najnovije izmene i dodaci reflektuju na njihove deljive baze podataka. Na taj način se sprečava gubljenje podataka u slučaju gubljenja, krađe ili kvara na PDA. Sinhronizacija se obično obavlja korišćenjem softvera za sinhronizaciju koji se distribuira uz PDA [2, 32].

Uobičajne funkcije PDA su: *Zabeleške, Kalkulator, Sat, Kalendar, Imenik, e – mail i internet pristup, video i audio snimanje, ugrađeni IC, BT; wi – fi, radio i muzički plejer, igrice i GPS.* S obzirom na postojeće funkcije, na PDA mogu da se memorišu sledeće vrste informacija:

- *Poslovne i lične zabeleške*
- *Službeni i privatni kontakti*
- *Dokumenti*
- *Lozinke*
- *Elektronska pošta (e-mail)*
- *Podaci iz banaka – finansijski podaci*
- *Informacije o firmi*
- *Slike i video*



Slika 2. Primer glavnog ekrana PDA sa Palm OS 6.1

2.2.1 Karakteristike PDA

Najveći broj PDA sastoji se iz mikroprocesora, ROM i RAM memorije, korisničkog interfejsa, tastera i ekrana od tečnog kristala koji je ponekad osetljiv na dodir. Operativni sistem PDA je smešten u ROM memoriji koja između ostalog može biti fleš (flash) tipa (može da se briše i reprogamira). Aplikacije i podaci koji su trenutno u upotrebi čuvaju se u *volatile* RAM, kako bi im procesor brzo pristupio. Potrebno im je stalno napajanje energijom. Greške ili pražnjenje baterije mogu prouzrokovati gubitak informacija. Noviji PDA imaju *sistem level* mikroprocesore kod kojih je smanjen broj neophodnih čipova i povećan kapacitet memorije. PDA sadrže čitače kartica kao što su SD – card, a mnogi imaju mogućnost IC, BT i wi-fi povezivanja. Mogu imati ugrađen PALM OS, Windows ili Linux operativni sistem [2,33].

2.2.2 PALM OS

PALM OS je operativni sistem koji je ranije korišćen na uređajima sa 16 i 32 -bitnim procesorima, baziranim na Motorolinoj „dragon bal MC 68328“ familiji mikroprocesora. Novi uređaji koriste ARM arhitekturu baziranu na „strong arm“ i „ X scale“ familiji mikroprocesora. Na ovakvim PDA uređajima, operativni sistem i aplikacije smešteni su u ROM memoriji, a korisnički podaci i druge aplikacije su smeštene u RAM memoriji. U ROM – u ima i nekoliko dodatnih usluga koje se koriste za *back up* podataka iz PIM-a (*personal informacion menagement).* Ovaj sistemski softver organizuje ROM i RAM na istom memorijskom modulu poznatijem kao kartica. PDA uređaj može da radi i bez kartice. Kod PALM OS, ukupna raspoloživa RAM podeljena je na dva dela*: dinamička RAM i smeštajna RAM. Dinamička RAM* je analogna RAM memoriji na desktop kompjuterima i koristi se kao prostor za privremeni smeštaj podataka. *Smeštajna RAM* memorija predstavlja hard disk kod desktop računara. Oba tipa RAM – a zadržavaju svoj sadržaj kada je uređaj isključen. Memorija kod PALM OS organizovana je po evidencijama. Ove evidencije grupisane su u baze podataka, u fajlu koji je u Palm file formatu (PFF). Ovi fajlovi mogu biti neki od sledećih tipova:

1. **Palm data base** – evidencija u kojoj se smeštaju korisnički podaci kao što su lista kontakata i podaci aplikacije.
2. **Palm Resource** – sadrži kodove aplikacije i objekte korisničkog interfejsa.
3. **Palm Query aplikacija** – gde se smeštaju sadržaji sa interneta.

Kod PALM OS, sve aplikacije dele istu dinamičku RAM, tako da mogu da koriste podatke jedna od druge. Novi uređaji sa PALM OS, koriste dva moda za poboljšanje funkcionalnosti nazvane „Palm Universal conector system“- (PUCS) i „Palm Expansion card slot“- (PECS).

PUCS pomaže uređaju da interaguje sa GPS prijemnicima, wi – fi modemima i drugim perifernim uređajima koji koriste USB. PECS prihvata multimedia kartice, MMCs i Secure digital kartice (SD).

Palm OS struktuiran je u sledećim slojevima:

- Aplikacije
- Operativni sistem
- Softverske aplikacije
- Drajveri hardvera.

Softver API pomaže u izvršavanju softverskih aplikacija pod različitim strukturama hardvera. Firme koje razvijaju softver, lako mogu da premoste API i pristupe procesoru diretno dajući više kontrola preko procesora.

Ponekad, ova mogućnost povećava bezbednosne rizike zbog malicioznih aplikacija. Palm OS ne brani pristup kodovima i podacima tako da svako može da pristupi i promeni ih. Palm OS obezbeđuje nekoliko ugrađenih (*built in*) bezbednosnih karakteristika. Na taj način se omogućava zaključavanja uređaja kada je isključen, uz zahtevanje lozinke za nastavak rada ili ponovnog uključivanja.

2.2.3 Windows C

Windows C je operativni sistem za prenosne uređaje koji je razvila kompanija *Microsoft*. Ovaj operativni sistem podržava multitasking i multiheaded okruženja. Najpre je promenio ime u Pocket PC, zatim u Windows mobile. Windows C radi na drugačijim procesorima od PALM OS-a, uglavnom na uređajima koji imaju X-scale, ARM ili SHx procesore. Kod ovog operativnog sistema, PIM i drugi korisnički podaci skladište se na RAM memoriji, a operativni sistem i druge aplikacije za podršku smeštene su na ROM. RAM memorija kod uređaja sa Windows C je podeljena na dva dela, od kojih je jedna za smeštaj objekata, a druga programska memorija. Deo memorije za smeštaj objekata koristi se kao stalni virtualni RAM disk, a podaci se zadržavaju preko pozadinskog napajanja, čak i ako je glavno napajanje isključeno. Windows C podržava jedan ili više slotova za kartice kao što su Compact Flash (CF) ili Secure Digital (SD). Najveći broj Poket PC uređaja koristi litijum – jonske baterije. Da bi se izbegao gubitak podataka treba češće puniti baterije.

Windows C je organizovan je po sledećim nivoima:

- Aplikacije
- Operativni sistem
- OM (original equipment manufacturer)
- Hardver.

OM nivo ili OM sloj egzistira između nivoa operativnog sistema ili nivoa hardvera. OM nivo sadrži OM adaption layer (OAL) drajvere i konfiguracione fajlove. Ovaj sloj upravlja funkcijama kao što su sistem start up, rukovanje prekidima, upravljanje napajanjem, profiling, tajmer i sat. U sloju operativnog sistema prisutni su Windows C

kernel i drajveri uređaja. Ovi drajveri uređaja omogućavaju da kernel prepozna uređaj i uspostavi komunikaciju između softvera i hardvera. Drajveri su monolitni ili slojeviti. Monolitni drajveri primenjuju svoj interfejs kao jednu akciju direktno na uređaju koji kontrolišu, dok slojeviti drajveri dele svoju primenu u jedan viši i jedan niži sloj. Viši sloj prikazuje interfejs drajvera, a niži sloj reaguje sa hardverom.

Ovaj operativni sistem takođe sadrži grafičke, Windows i invent subsisteme (GVES) i omogućuje interfejs između korisnika aplikacije i operativnog sistema. GVES objedinjuje GDI (*graphic device interface*), Windows menadžer i menadžer događaja. Sastoji se od dve komponente:

1. – **korisnička komponenta**, koja rukuje porukama, događajima, unosom sa tastature i miša i
2. – **GDI**, koja crta grafiku, tekst i slike.

Objekti u Windows C skladište se u tri tipa stalne memorije i to u fajl sistemu, registrima i Property data bases. Windows C sistem skladišti fajlove i na ROM i na RAM memoriji. Fajlovi uskladišteni na RAM imaju ista imena kao i oni na ROM. Aktuelni RAM fajlovi su senke ROM fajlova. Korisnici koji žele da pristupe shadowed fajlu mogu samo da pristupe RAM verziji. Kada korisnik obriše RAM fajl ROM fajl je dostupan.

Property data bases su svojevrsna skladišta u kojima podaci mogu biti uskladišteni, pretraživani i povraćeni. Windows C registar, skladišti sve informacije o podešavanjima koje se odnose na aplikacije, drajvere, konfiguraciju sistema i korisničke podatke. Ovi registri čuvaju se u RAM memoriji. Windows C podražava sledeće tipove memorije:

1. RAM
2. Expansion RAM
3. ROM
4. Stalna memorija.

2.2.4 PDA bazirani na LINUX-u

LINUX obezbeđuje multitasking, multihreading 32 bit operativni sistem za PDA i ima sledeću arhitekturu:

- Upravljanje memorije
- Kreiranje procesa thread
- Mehanizmi komunikacije između procesa
- Rukovanje prekidima
- Execute-in-place (XIP) ROM fajl sistemi
- RAM fajl sistemi
- Flesh menadžment
- TCP/IP umrežavanje

LINUX kernel se sastoji od modularnih komponenti i subsitema koji obuhvataju drajvere uređaja, protokole, shedjuler, menadžer memorije, virtualni fajl sistem i alokator resursa. LINUX kernel koristi se preko programskog interfejsa. Procesuiranje počinje

kada se preko interfejsa načini zahtev hardveru. Ima bezbednosne karakteristike kao što su identifikacija i autenfikacija korisnika, kontrola pristupa, tehnike za enkripciju. PPTP (Point-to-Point Tunelinng Protocol), internet protokol securiti (IPSec) i secure shell (SSH). Bez obzira na ove bezbednosne karakteristike PDA bazirani na LINUX-u, ranjivi su na napade autentifikacije.

2.2.5 Generička stanja PDA

Za razliku od desktop kompjutera, koji imaju dva stanja, (u radu ili ugašen), PDA uređaji mogu biti u različitim stanjima:

1. **Nastcent state** – stanje uređaja koje je primljeno od proizvođača. U ovom stanju uređaj ne sadrži nikakve korisničke podatke, već samo fabrička podešavanja. Uređaj se vraća u nastcent stanje, nakon takozvanog hard reseta ili oticanja baterija.
2. **Active state** – u ovom stanju uređaj je uključen i izvršava različite zadatke. Uređaj je prilagođen od strane korisnika i sadrži korisničke podatke. Uređaj se može vratiti u aktivno stanje preduzimanjem operacija takozvanog soft reseta.
3. **Quiescent state** – ovo je stanje mirovanja uređaja gde se baterija koristi samo za održavanje korisničkih podataka i aktivnosti u pozadini. Uređaj se može vratiti u Quiescent state, pritiskom dugmeta za startovanje.
4. **Semi Aktive state** – ovo stanje je između aktivnog i Quiescent state. Uređaj najčešće prelazi u ovo stanje preko tajmera koji se aktivira kada je uređaj neko vreme neaktivan. U ovom stanju štedi se baterija gašenjem monitora i sličnih prigodnih akcija. Iz ovog stanja u aktivno prelazi se dodirom ekrana, pritiskom tastera, soft resetovanjem.

2.2.6 ActiveSinc i HotSinc opcije

Da bi se zaštitili mobilni uređaji i podaci potrebno je shvatiti načine na koji se uređaji međusobno povezuju. Desktop sinhronizacija mobilnih uređaja podrazumeva pristup bez povezivanja. ActiveSinc vrši sinhronizaciju PDA uređaja baziranih na Windows-u, sa desktop računarima. Korisnik može izabrati da ActivSince zaštiti lozinkom. HotSinc je proces sinhronizacije elemenata između PDA sa Palm OS i PC računara. Sinhronizuje korisnički Microsoft out look inbox, listu kontakata, kalendar, kao i zadatke i zabeleške.

ActiveSinc napadi: ActiveSinc dozvoljava neograničen broj pokušaja pristupa pogrešnom lozinkom. Napadač može pokušati da dobije aktivSinc lozinku korišćenjem pasford sniffinga ili brutalnog/rečničkog napada. Kada korisnik snimi lozinku na desktop kompijuter napadač će lako doći do nje samim pristupom računaru.

Ovo omogućava napadaču da instalira maliciozne programe na PDA, kao što je keylogger koji će beležiti sve aktivnosti rađene na PDA.

HotSinc napadi: Palm uređaji su ranjivi na HotSinc napade. Korišćenjem HotSinc opcije razni virusi, Trojanci i drugi *spayware* mogu biti preneseni na PDA. Za vreme HotSinc procesa Palm operativni sistem otvara TCP portove 14237 i 14238 kao i UDP port 14237. Napadač može ostvariti vezu sa ovim portovima i pristupiti privatnim informacijama ili poslati maliciozni kod.

2.2.7 Bezbednosni rizici povezani sa korišćenjem PDA:

- Krađa uređaja – jedan od najvećih bezbedosnih problema kod korišćenja PDA uređaja
- Krađa lozinke, pri čemu se ovaj rizik može smanjiti korišćenjem dužih bezbednih lozinki koje sadrže alfa numeričke karaktere i simbole, kako bi bile teže za crack – ovanje.
- Napadi virusa
- Korupcija podataka
- Ranjivost aplikacija (postoji određeni rizik i u programskim jezicima kao što je Java i u radnim okruženjima kao što je Active X koje najčešće koriste PDA Web pregledači)
- Ranjivost preko bežične mreže, kao prevencija ovoga je obezbeđivanje podataka na uređaju u takozvanom stand alone modu (mod u kome uređaj nije povezan na bežičnu mrežu). PDA koji koriste bežične servise i bežične portove takođe su ranjivi bežičnim napadima. Kao zaštita od bežičnih napada preporučuje se instaliranje WPN klijenta i enkripcija konekcije.

2.3 iPod i iPhone

iPOD je prenosni media plejer, koji pruža veliki kapacitet za smeštaj podataka, audio, video i drugih formata (MP3, M4A/AAC, AIFF, Audible audio book, kao i Apple Losles audio formate). Klasični iPod uređaji koriste hard diskove za smeštaj podataka, a novije verzije kao što su iPod Nano, iPod Shuffle i iPod Touch, koriste fleš memoriju. Muzički i video fajlovi na iPod-u organizuju se iTunes programom sa PC ili Mac računarom. iPod Touch poseduje Wi – Fi i *multitouch* interfejs. Koristi *iPhone OS* kao svoj operativni sistem [2,31].



Slika 3: iPod touch i IPhone 5

iPhone je multimedijalni uređaj sa mogućnošću internet povezivanja, sa ekranom osetljivim na dodir, preko koga se odvija interakcija korisnika sa uređajem uključujući i virtualnu tastaturu za unos teksta. iPhone uključuje sledeće standardne mogućnosti:

- Telefon
- E-mail
- Safari web pretraživač
- Media pleyer
- SMS poruke
- Mape sa GPS uređajem
- iTunes prodavnicu
- prodavnicu aplikacija
- kalendar
- Youtube
- kamera
- stocks, vremensku prognozu i zabeleške
- kalkulator.

2.3.1 Operativni sistem iPhone

Ovaj operativni sistem koji je razvijen iz MAC OS X koriste iPhone i iPod Touch. Koristi manje od 300mb ukupne memorije uređaja. iPhone OS sadrži četri apstraktna nivoa [2]:

1. **Jezgro OS** - obezbeđuje kernel okruženje, drajvere i osnovni interfejs operativnog sistema.
2. **Nivo centralnih servisa** - pruža fundamentalne servise za aplikacije kao što su Addres Book, Core Location, CFNetwork, Security i SQLite.
3. **Nivo media** - omogućava rad grafičkih i mediskih tehnologija kao što su Core Audio, OpenAL i video tehnologije.
4. **Cocoa Touch nivo** - omogućava korisnicima korišćenje grafičkih i drugih aplikacija.

iPhone prilagođava particije diska kako bi mogao da upravlja uskladištenim podacima. Sastoji se od Nand fleš memorije standardno podeljeno na dve particije:

1. ***Root*** (korena) **particija** veličine 300mb – sastoji se od operativnog sistema i svih instaliranih aplikacija. To je read-only particija i ne menja originalno fabričko stanje.
2. **Korisnička particija** predstavlja svu preostalu memoriju i sadrži sve korisničke podatke. Nazvana je i privatna.

2.3.2 Apple HFS i FAT32

iPODI formatirani na MAC računarima koriste Apple HFS plus fajl sistem, dok uređaji formatirani na Windowsu koriste FAT32 sistem. iPODI koriste različite formate fajlova za smeštanje različitih podataka. Koriste standardni wCard fajl format za smeštaj informacija o kontaktima. Ovaj format zamena je za električnu biznis kartu. wCard sadrži lične podatke kao što su ime i adresa i lako mogu biti dodati (*attached*) uz e – mail [2].

2.3.3 Bezbednosni rizici povezani sa korišćenjem iPod i IPhone

Veliki kapacitet memorije, mala veličina i velika brzina transvera podataka čini iPOD korisnim za napadače u informatičkim krađama. Popularnost iPOD i njihov imidž (nevinog, sveprisutnog, neupadljivog mediaplejera) učinili su ih popularnim i kod kriminalaca. iPod-i mogu biti hakovani ili prilagođeni korišćenjem različitih tehnika.

Ovi uređaji mogu biti konfigurisani da rade kao eksterni hard diskovi ili da izvršavaju određene skripte. Kriminalci ih koriste za :

- Širenje virusa i Trojanaca
- Smeštaj i distribuiranje ilegalnih slika i videa
- Čuvanje zapisa o kriminalnim aktima kao što su datum i vreme
- Za distribuiranje kontakt podataka među kriminalcima.

Osim nabrojanih osobina karakterističnih za iPod, iPhone obuhvata i mogućnost internet povezivanja, sve osobine standardnog mobilnog telefona, pa se u ovom smislu za kriminalne aktivnosti koristi i u sledeće svrhe:

- krađa korisničkih podataka kao što su brojevi telefona, *e-mail* adrese i SMS poruke
- povezivanje iPhone-a na drugi sistem (uređaj ili računar) radi krađe njegovih podataka
- slanje pretećih i uznemiravajućih SMS i MMS poruka
- manipulisanje SIM karticom
- kloniranje SIM kartice
- otključavanje iPhone-a sa mreže
- slanje SPAM poruka.

3. Bezbednost informacija

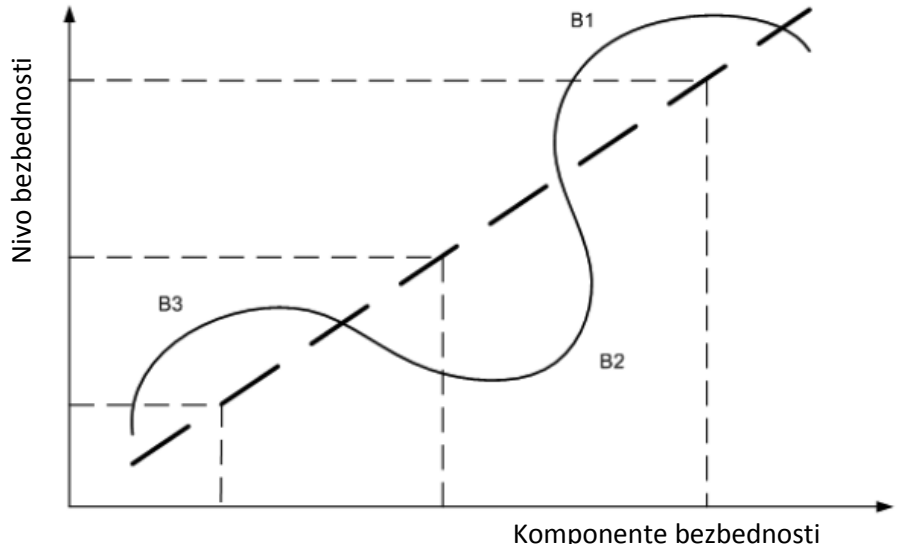
3.1 Definicije pojmova bezbednost i sigurnost informacija

Bezbednost informacija ili informaciona bezbednost su termini pod kojima se primarno podrazumeva bezbednost informacija i podataka u IKTS, a sekundarno bezbednost objekata računarskog sistema i računarske mreže, čime se posredno štite informacije i informaciona imovina (informacije, hardver, softver i ljudi). Bezbednost informacija obezbeđuje se sistemom zaštite. Optimalni sistem zaštitne informacija znači rentabilan i adekvatan sistem zaštite za konkretno poslovno okrženje, profile rizika i ukupne troškove zaštite.

U zavisnosti od nivoa apstrakcije, u praksi zaštite postoje brojne definicije bezbednosti informacije, pa na nivou države to predstavlja stanje zaštićenosti nacionalnih interesa u informacionoj sferi, određenih skupom ličnih poslovnih i državnih interesa.

Bezbednost IKTS je objektivna mera stanja rizika ili stanja bezbednog neometanog funkcionisanja sistema, u odnosu na samog sebe i svoje okruženje. Sistem je bezbedan onoliko koliko je zaštićen od uticaja faktora rizika. Sigurnost je sinonim za bezbednost, a u semantičkom smislu predstavlja subjektivnu meru poverenja ili osećaja sigurnosti da je sistem bezbedan.

Bezbednost IKTS, u realnom okruženju, karakterišu razni sociološko-kulturološki i tehnološki faktori koje treba uzeti u obzir pri oceni nivoa bezbednosnog stanja IKTS. U opštem slučaju, ukupna bezbednost nekog složenog sistema obuhvata skup komponenti bezbednosti (B1,B2...Bn):



Slika 4. Nivo ukupne bezbednosti u funkciji komponenti bezbednosti [3]

Nivo ukupne bezbednosti sistema – Bu, raste sa porastom nivoa bezbednosti sistema njenih relativno nezavisnih bezbednosnih komponenti. Uobičajeno, bezbednost računarskih sistema (RS) mreza (RM), ili IKTS poistovećuje se sa bezbednošću informacija kao najvrednije imovine organizacije. Razlika između ovih pojma je u pristupu i metodologiji i zaštite.

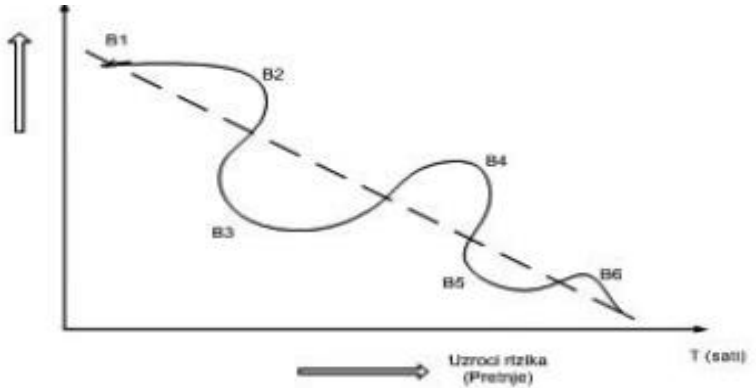
U objektno orjentisanom pristupu, bezbednost informacija se odnosi na zaštitu poverljivosti, integriteta i raspoloživosti – CIA (Confidensiality, Integrity, Avialability) informacija, bez obzira na formu, u kojoj se informacija nalazi. Bezbednost RS/RM/IKTS odnosi se na zaštitu CIA informacija koje se skladište, obrađuju ili prenose u RS/RM.

Bezbednost informacija nije konačan prozvod, već je proces kojim se omogućava kontinuirano poslovanje, smanjuje potencijalna šteta i unapređuje ukupno poslovanje. U tom smislu, bezbednost informacija se može definisati kao odsustvo rizika po poverljivost, integritet i raspoloživost informacija, odnosno kao zaštićenost informacija od neovlašćenog pristupa, upotrebe, otkrivanja, izmene ili uništenja informacija.

Bezbednost informacija se, u praksi, najćešće manifestuje kroz bezbedan rad, bez otkaza RS, RM i interneta, malicioznih programa i prisluškivanja; bezbednu komunikaciju, kupovinu i plaćanje preko interneta sa zaštitom privatnosti. Prema tome, bezbednost informacija je ciklično ponovljiv proces, stalnog održavanja zaštićenosti informacija koji se planira, implementira, izvršava, održava i poboljšava, kroz uspostavljen sistem za upravljanje zaštitom informacija – ISMS (Information Security Management system).

3.2 Funkcionalna zavisnost bezbednosti i pretnji

Bezbednost IKTS zavisi od konkretnog situacionog problema realnog okruženja. U tom okruženju, izvršioci napada i uzroci nastanka faktora rizika su agenti potencijlnih pretnji, a verovatnoća da će agent pretnje iskoristiti ranjivost sistema i prouzrokovati negativne posledice po sistem (kao i organizaciju u celini), predstavlja procenjenu meru uticaja pretnje na informacionu imovinu, odnosno rizik, koji je ujedno i osnovna kategorija analize bezbednosti IKTS.



Slika 5: Nivo ukupne bezbednosti IKTS u funkciji pretnji [3]

U realnim uslovima sa porastom nivoa pretnji, povećavaju se i rizici, a nivo ukupne bezbednosti IKTS nelinearno opada, zbog stepena neodređenosti uticaja faktora rizika.

3.3 Glavni faktori uticaja na bezbednosno stanje IKTS

Na bezbednost IKTS utiču brojni faktori, kao što su funkcionalni zahtevi poslovnog sistema (e-poslovanje, cloud computing – CC), organizaciona struktura (promena prava pristupa usled kardovskih promena), tehnološki razvoj, politika zaštite, svest o potrebi zaštite (implementacija tehnologije zaštite, bez procene rizika), komleksnost i skalabilnost sistema, poverljivost i privatnost. Zaseban bezbednosni rizik proističe iz same prirode korisnika (zaposlenih na IKTS), posebno u domenu donošenja odluka. Otežavajući faktor, sa aspekta procene rizika i planiranja zaštite IKTS, predstavlja potreba da se sistem zaštiti od nečega što se još uvek ne dešava [3].

Najznačajniji resurs svake organizacije, ujedno i kritični objekat zaštite, predstavljaju kvalitetne i integrisane informacije, potrebne za odlučivanje. Na kvalitet informacija utiče niz atributa (tačnost, blagovremenost, aktuelnost, pouzdanost, integritet, objektivost, tajnost, rasoloživost i druge), čiji je pojedinačni značaj za različite poslovne sisteme promenljiv.

Ukupan kvalitet poslovnih IKTS ilustruje se trouglom stabilnosti: hardver, softver i bezbednost. Presudan uticaj na način zaštite informacija ima činjnica da je vrednost informacije funkcija vremena, pa otuda i potreba za razvojem realnih metoda za procenu rizika, u skladu sa vremenskim okvirima i dinamikom savremenog e-poslovanja. Shodno navedenom, informacije koje obezbeđuju komparativnu prednost za duži period štite se jakim mehanizmima zaštite (npr. kriptološkim).

Na praksu zaštite IKTS najviše utiču: kompleksnost, skalabilnost, poverljivost i privatnost. Kompleksnost iziskuje duboko razumevanje principa funkcionisanja IKTS, kako bi se imlementirao konherentan sistem zaštite. Zahtev za skalabilnošću (nadogradivosti) proporcionalan je rastu kompleksnosti, distibuiranosti i umrežavanja IKTS, što pak zahteva analizu modularnosti i mogućnosti integracije. Poverljivost i privatnost su ključni zahtevi koji dramatično rastu sa povećanjem broja umreženih aplikacija, primene IKTS i servisa.

Najkompleksnija oblast zaštite savremenih IKTS u internet okruženju su modeli autentifikacije (verifikacije identiteta), kao jedini mehanizmi kojima se istovremeno prevazilaze problemi uzajamnog poverenja i zaštite privatnosti korisnika. Potreba za zaštitom privatnosti i poverljivosti ličnih podataka raste uporedo sa lakoćom sa kojom se elektronske informacije mogu skladištiti, prenositi menjati i distribuirati [3,27].

Pristup problemu zaštite privatnosti ličnih podataka u elektronskom okruženju razlikuje se od zemlje do zemlje i predstavlja balans između prava zaštite privatnosti pojednica (grupe ili organizacije) i potrebe države da ima pristup svim informacijama i podacima, usled porasta terorizma i računarskog kriminala.

Generalno bezbednost realnog IKTS zavisi od sledećih faktora:

1. šta sistem treba da radi (specifikacija/politika)
2. kako to radi (implementacija kroz mehanizme i zaštita)
3. da li stvarno to radi (tačnost i garantovana bezbednost)
4. može li sistem preživeti sofisticirane napadače (ljudska priroda).

Stanje bezbednosti IKTS u nebezbednom okruženju, u praksi se održava na prihvatljivom nivou rizika sa implementiranim upravljačkim (U), organizacionim (O) i tehničkim (T) kontrolama zaštite.

3.4 Opšta definicija sistema zaštite

Zahtevana bezbednost informacija i IKTS, ostvaruje se sistemom zaštite. U objektno orjentisanom pristupu, sistem zaštite predstavlja organizovan i koherentan skup U, O i T kontola zaštite, kao i njihovih veza i ograničenja, primenjenih na IKTS sa ciljem zaštite raspoloživosti, poverljivosti i integriteta procesiranih, uskladištenih i prenošenih podataka i informacija.

Najbolji rezultati analize i razvoja sistema zaštite postižu se primenom metodologije sistema inženjerijske analize, objektno - orijentisanog modelovanja (OOM) i procesnim pristupom, čija je glavna prednost smanjivanje kompleksnosti.

Prva faza u razvoju sistema zaštite je da se, na bazi procene rizika, definiše model IKTS i odrede objekti koje treba štititi, pri čemu je racionalno da se sistem zaštite razvija za životni ciklus IKTS. Pravilna procena rizika i izbor kontrola zaštite su glavni ciljevi u pristupu zaštite informacija, kako bi se taj rizik sveo na prihvatljiv nivo.

Procena rizika je specifična za svaku organizaciju, pa primena standarda najbolje prakse zaštite (NIST SP 53 A, B, C; IS_ v.4.0; IS_/IEC 27000 serija, IS_/IEC 21827 (SSE CMM) itd.) nije uvek adekvatna jer se ne uzimaju u obzir različiti profili rizika. To praktično znači da optimalni sistem zaštite informacija nije uvek i najviši nivo zaštite, koji se podrazumeva standardom najbolje prakse zaštite, već je to rentabilan, ekonomski i funkcionalno opravdan sistem zaštite za konkretno poslovno okruženje, profil rizika i ukupne troškove zaštite.

Konkretan IKTS je bezbedan, ako je adekvatno zaštićen. To znači da je bezbednost IKTS (Bis) bezbednosna funkcija sistema zaštite (Sz), čiji je domen skup atributa vektora zaštite *((intenzitet zaštite* (dužina vektora)–**Isz,** *kvalitet zaštite* (pravac vektora) – **Ksz** i *sveobuhvatnost (višeslojnost i raznovrsnost) kontrola zaštite* (smer vektora zaštite) – **Ssz)** [3]**:**

$$Bis = f(Sz) = f(Isz \ \mathbf{U} \ Ksz \ \mathbf{U} \ Ssz).$$

Atributi vektora zaštite su u konjuktivnoj vezi, pa sledi da će IKTS biti bolje zaštićen, ako je veća unija atributa, odnosno što je sistem zaštite koherentniji.

3.5 Osnovne funkcionalnosti sistema zaštite

Osnovne funkcionalnosti sistema zaštite izvršavaju se kroz servise, mehanizme, kontrole i funkcije zaštite, ili bezbednosne funkcije. Funkcije zaštite se izvršavaju mehanizmima i protokolima zaštite, koji u logičkom smislu predstavljaju način realizacije servisa zaštite.

Servis zaštite je proces ili neprekidna, ponovljiva aktivnost, izvršena funkcijama mehanizama i protokola zaštite. Korisnike ne zanima kako su servisi zaštite implementirani, već da li mogu da izvrše željenu akciju. Na primer: zaštita tajnosti informacija u komunikacionom kanalu je servis zaštite u IKTS, a algoritamska kriptografska transformacija sadržaja informacija je mehanizam za realizaciju tog servisa zaštite.

Mehanizmi i protokoli zaštite su individualni algoritmi, hardversko-softverski moduli ili metodi za izvršavanje bezbednosnih funkcija. Neki mehanizmi zaštite su za jedan, a neki za više različitih servisa (npr. kriptografski mehanizmi). Za realizaciju mehanizma zaštite, potrebno je obezbediti određene kontrolne strukture, koje mogu biti upravljačke, operativne i tehničkke, a uobičajeno se nazivaju kontrole zaštite.

Kontrola zaštite IKTS je konačna klasifikacija mehanizama zaštite i interfejs između mehanizma i čoveka. Kontrola zaštite može biti tehnička povratna sprega (npr. alarmni signal generisan na izlazu IDPS), bezbednosna funkcija arhitekture sistema zaštite, organizaciono – operativna mera (npr. barijere za fizički pristup) i upravljačko–administrativna mera (npr. primenjen standard). Termin kontrola zaštite, takođe, implicira suštinsku potrebu neprekidnog nadzora i kontrolisanja sistema zaštite i uspešno zamenjuje tradicionalne termine: administrativnih, organizacionih i hardversko softverskih mera i metoda zaštite [3].

3.6 Informacioni sistem kao objekat zaštite

Osnovno strukturno obeležje savremenih IKTS je teritorijalna distribucija RM u intenzivnoj komunikaciji sa RS, kao osnovnom tehničkom komponentom. Smanjenje kompleksnosti postiže se uvođenjem grana objekata:

- informacione imovine: poverljivost (C), integritet (I) i raspoloživost (A), ili CIA (čime se struktuiraju objekti koje treba štititi , tj. bezbednosni ciljevi i
- mera i sredstava zaštite: proceduralne (U,O) i tehničke (T) kontrole zaštite, čime se struktuiraju alati za zaštitu.

U objektno orijentisanom pristupu zaštita informacija podrazumeva zaštitu informacione imovine: čiste, fizičke i humane (Tabela 1) [3]:

Tabela 1: Klasifikacija informacione imovine [3]

Čista informaciona imovina	
Digitalni podaci i informacije	personalne, finansijske, zakonske, istraživanje i razvoj, strateške i komercijalne, e-pošte, *voice*-mail, baze podataka, lični i deljeni folder, bekap mediji – trake/CD/DVD i digitalna arhiva, šifarski ključevi, lozinke
Opipljiva informaciona imovina	personalna, finansijska, zakonska, istraživanje i razvoj, strateške i komercijalne, poštanske pošiljke, faksovi, mikrofiš i drugi bekap/arhivni materijali, ključevi skladišta medija, žurnala, magacina, knjiga
Neopipljiva inf. imovina	znanje, poslovni odnosi, trgovačke tajne, licence, patenti, iskustva, brend, reputacija, poverenje, konkurentnost, etika, produktivnost
Aplikativni program	razvijeni u korporaciji/kastomizovani sistemi, klijentski program (uključujući deljene i za krajnje korisnike), komercijalno raspoloživi softver, ERP sistemi, MIS (managament IS), baze podataka, uslužni programi/alati, aplikacije za e-poslovanje, *midleware*
Sistemski program	za servere, desktop računare, mainframe računare, mrežne uređaje, priručne i ugrađene računare (uključujući bios rom i druge *firmware*
Fizička informaciona imovina	
Infrastruktura za podršku IKTS	zgrada u kojoj su smešteni: IKTS, centar za obradu podataka, serverske/računarske sobe, kancelarije, kabina za umrežavanje LAN mreže, kabineti za držanje fascikli dokumenata, sobe i sefovi za čuvanje EM i optičkih diskova, uređaji za identifikaciju i autentifikaciju medija/ kontrolu pristupa (kartični sistemi za pristup, tokeni, smart kartice itd.) i drugi uređaji za tehničku zaštitu (CCTV, protivprovalni sistemi itd.)
Kontrole okruženja IKTS	protivpožarni alarmi/sistemi za gašenje požara/protivpožarni aparati, jedinice za neprekidno napajanje (UPSS), mrežno napajanje, mrežni transformatori/ filteri/atenuatori, klima uređaji/ventilacioni sistemi za provetravanje, alarmni sistemi za poplavu
Hardver IKTS	uređaji za računanje i skladištenje (desktop PC, radne stanice, laptop, priručni računari, serveri, mainframes, modemi i linijski terminatori, komunikacioni uređaji, (mrežni čvorovi), printeri/kopir/fax mašine itd.
Imovina IKTS	autentifikacioni servisi i administrativni procesi za upravljanje profilom korisnika, hiperlinkovi (brauzeri), *firewalls*, *proxy* serveri, mrežni servisi, bežični servisi, anti –spam/virus/*spyware*, IDPS, servisi za telerad, servisi zaštite, FTP, e–mail, web servisi, ugovori za podršku i održavanje.
Humana informaciona imovina	
Zaposleni	zaposleno osoblje, glavni/izvršni menadžeri, dizajneri/programeri/ evaluatori programa, menadžer i administrator zaštite, operateri, pravnici, korisnici sa najvećim privilegijama, LAN i administratori zaštite.
Ne-zaposleni	privremeno zaposleni, spoljni konsultanti/specijalisti savetnici, specijalisti po ugovoru, snabdevači, poslovni partneri

Osnovni bezbednosni zahtevi za sistem zaštite informacija su sprečavanje: ugrožavanja bezbednosti ličnosti, organizacija i države; krađe, pronevere, gubitaka i izmene informacija; neovlašćenih aktivnosti u IKTS; povreda intelektualne svojine, privatnosti i poverljivosti ličnih i poslovnih podataka u skladu sa Zakonom o zaštiti podataka o ličnosti i Zakonom o zaštiti tajnosti podataka.

U skladu sa iznetim, zaštita podataka se odnosi na:

• **Privatnost** (privacy): i to kao privatnost korisnika i privatnost subjekta podataka, a obuhvata privatnost pristupanja u sistem, privatnost govora, privatnost podataka, privatnost korisnikove lokacije i identifikacije, kao i privatnost finansijskih transakcija.
• **Sigurnost podataka** (security): obuhvata obezbeđenje podataka od slučajnog ili namernog otkrivanja neovlašćenim licima, kao i zaštitu od neovlašćenog menjanja, brisanja, i korišćenja od strane ovlašćenih korisnika ili celokupnog gubitka.
• **Poverljivost podataka** (confidentiality): pretpostavlja da se poverljivi podaci ne smeju otkriti od strane neautorizovanih pojedinaca i drugih entiteta, ili u neovlaštenim procesima. Kad su u pitanju mreže, proverljivost obuhvata i frekvencije, izvor, destinacije...
• **Raspoloživost podataka** (availability): pretpostavlja da samo ovlašćeni korisnik može blagovremeno doći do podataka, bez barijera.
• **Integritet** (integrity): obuhvata integritet podataka, integritet izvora, i tačnost.

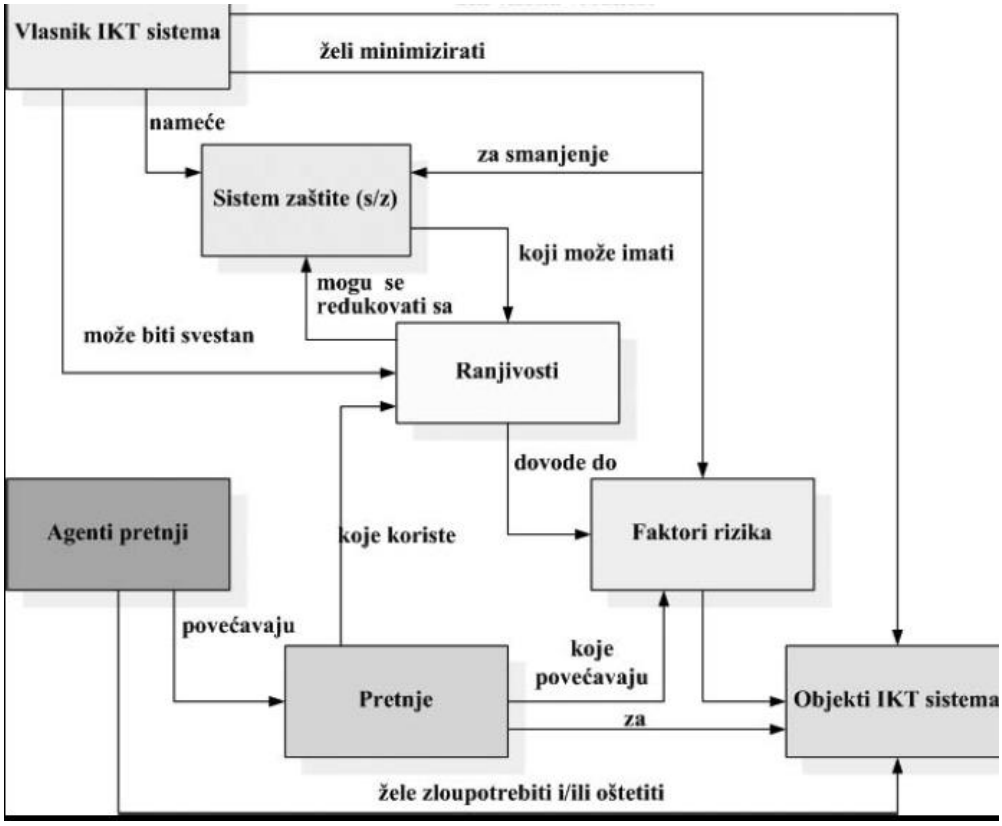
Pravo na privatnost (privacy right) je jedno od osnovnih, neotuđivih i apsolutnih ljudskih prava, garantovanih Ustavom, kojima se obezbeđuje integritet i dignitet ljudske ličnosti, a radi očuvanja tajnosti i slobode njegovog privatnog života. Informaciona privatnost je „pravo pojedinca, grupa ili institucija da sami za sebe odrede kada, kako i u kojoj meri će se informacije o njima saopštavati drugim licima“ (Alan Westin).

Podaci o ličnosti su svi oni podaci koji se odnose na neko određeno i odredivo fizičko lice, koje na osnovu njih može biti identifikovano. Osim podataka o živim fizičkim licima ovi podaci se vode i za lica koja su umrla ili su proglašena umrlim, tim pre što ta lica ne mogu da koriste prava koja bi im inače pripadala (zahtev za brisanje, izmenu itd.). Vrste podataka koje se smatraju podacima o ličnosti su [5,6]:

1) podaci o činjenicama - tu spadaju: ime, adresa, godine, primanja, političke aktivnosti, ispitne ocene, podaci sa IQ testa, religija, rasa i sl.
2) podaci o mišljenjima i sudovima samog pojedinca i drugih subjekata o njemu - u prvu grupu spadaju želja za napredovanje, brak, i sl., a u drugu o kreditnoj sposobnosti, mogućnosti za profesionalno napredovanje i sl.
3) podaci o namerama - uključuje i namere korisnika u vezi sa subjektom na koga se podaci odnose.

3.7 Generički, funkcionalni model sistema zaštite

Mesto i uloga sistema zaštite IKTS najlakše se mogu predstaviti na generičkom modelu sistema zaštite (Slika 6.).



Slika 6. Generički model sistema zaštite i međusobni odnosi komponenti [3]

U generičkom modelu sistema zaštite, vlasnik IKTS definiše vrednost informacione imovine i odgovoran je za njenu zaštitu. Nasuprot njemu, agenti pretnje predstavljaju izvršioce potencijalnih pretnji i uvek deluju protiv interesa vlasnika sistema. Pri tome, pod pretnjom se podrazumevaju akcije agenta pretnje, najčešće posredstvom malicioznih programa i namernih internih i eksternih napada, kojima se narušavaju osnovna svojstva objekata informacione imovine (poverljivost, integritet i dostupnost). Zbog toga se objekti informacione imovine štite sistemom zaštite.

U proceni rizika, vlasnik IKTS analizira moguće pretnje, ceneći njihovu primenljivost u datom okruženju, ranjivost sistema, iskoristivost te ranjivosti sa jednom ili više pretnji, kao i verovatnoću uticaja na poslovanje. Rezultati navedene analize su rizici. Analiza i procena rizika uključuje izbor različitih kontrola zaštite, kojima se rizik svodi na prihvatljiv nivo, što se postiže smanjenjem ranjivosti i izloženosi sistema, u skladu sa zahtevima politike zaštite vlasnika [2].

Nakon implementacije kontrola zaštite, agenti pretnji mogu iskoristiti preostale ranjivosti, što predstavlja preostali rizik na prihvatljivom nivou. Zbog toga, vlasnik IKTS, u neprekidnom (cikličnom) procesu zaštite, svim raspoloživim kontrolama zaštite, uvek nastoji smanjiti preostali rizik.

Pre nego što dozvoli da se IKTS izloži identifikovanim pretnjama, vlasnik mora biti uveren da su primenjene kontrole zaštite adekvatne za ublažavanje faktora rizika. U tom cilju, vlasnik može tražiti evaluaciju – internu i spoljnu reviziju (audit) ili sertifikacijui akreditaciju (testiranje i odobrenje za rad) IKTS i sistema zaštite. Izlazni rezultat procesa evaluacije je izjava o akreditatciji (na bazi rezultata sertifikacije), da će zaštitne mere smanjiti faktore rizika na prihvatljiv nivo. Na osnovu rezultata evaluacije vlasnik odlučuje da li će prihvatiti preostali rizik ili ne, što dokazuje potpisivanjem dokumenta SOA (Statement of Applicability).

3.8 Definisanje optimalnog sistema zaštite

Programom zaštite informacija vrši se identifikacija bezbednosnih ciljeva i razvija, implementira i održava optimalan, odnosno ekonomski rentabilan i funkcionalno efektivan, sistem zaštite. Optimalno zaštićen IKTS ima izbalansirane efektivnosti kontrola zaštite i troškove njihove akvizicije/razvoja, odnosno troškovi kontrola zaštite su potpuno izjednačeni sa procenjenim gubicima.

U zavisnosti od odnosa strategije zaštite i postavljenih bezbednosnih ciljeva, moguća su dva pristupa sintezi optimalnog sistema zaštite:
Primarni: za dati nivo troškova zaštite – Trz obezbediti maksimalno mogućii intenzitet vektora Zaštite - I(s) =>Imax , gde je s – izabrana strategija zaštite;
Sekundarni: obezbediti željene rezultate intenziteta vektora zaštite I(s) > I, pri minimalno mogućim troškovima Zaštite – Ttrmin dopušteni.

Pod efektivnošću kontrole zaštite informacija podrazumeva se efikasnost i efektivnost u aktivnoj zaštiti poverljivosti, integriteta i raspoloživosti informacija u operacijama obrade, skladištenja i prenosa. Ocena efektivnosti procesa zaštite odnosi se na sposobnost kontrole zaštite da reši zadatak zaštite.
U skladu sa arhitekturom sistema zaštite, tehnologijom obrade informacija i preciznom matematičkom formulacijom zadatka, u procesu sinteze optimalnog sistema zaštite, polazi se od izbora matematički produktivnog kriterijuma optimalnosti, pri čemu se uzimaju u obzir svi apriorni zaključci i dopuštena rešenja prema primarnim kriterijumima.

4. Digitalni dokazi

Da bi se rasvetlilo krivično delo i otkrio njegov počinilac, moraju se prikupiti i obezbediti relevantni dokazi koji se u krivičnom postupku izvode i ocenjuju od strane suda, kako bi se stvorilo uverenje o istinitosti činjenica koje se dokazuju, a važne su za krivični predmet [9].

Prema definiciji IOCE[1], u oblasti forenzičkih nauka digitalni dokaz je svaka informacija udigitalnom obliku kojaima dokazujuću, oslobađajuću ili vrednost osnovanesumnje i koja je uskladištena ili prenesena u digitalnom formatu. U skladu sa ovom definicijom, pod pojmom digitalnog dokaza podrazumevamo kompjuterski uskladištene i kompjuterski generisane podatke i dokazne informacije, digitalizovane audio i video dokazne signale, signale sa digitalnog mobilnog telefona, informacije sa digitalnih faks mašina i signale drugih digitalnih uređaja. Prema tome, digitalni dokaz je bilo koja informacija generisana, obrađivana, uskladištena ili prenesena u digitalnom obliku, na koju sud može bazirati svoju presudu. Drugim rečima, to je svaka binarna informacija, sastavljena od digitalnih jedinica (1) i nula (0), uskladištena ili prenesena udigitalnoj formi, kao i druge moguće kopije orginalne digitalne informacije koje imaju dokazujuću vrednost i na koje se sud može osloniti, u kontekstu forenzičke istrage, akvizicije (prikupljanja), analize i prezentacije dokaza pred sudom [10].

Digitalni dokazi mogu posredno ili neposredno ukazivati na bilo koje krivično delo iz Krivičnog zakonika. Tako, dokazi pronađeni na mobilnim telefonima i tablet računarima, uz podatke dobijene od operatera mobilne telefonije, mogu da ukažu na vremenski okvir izvršenja nekog događaja, lokaciju okrivljenih ili oštećenihu vremenu izvršenja i sa kim su komunicirali. Sadržaji komunikacija SMS i MMS servisima mogu da ukažu na to kako je krivično delo planirano ili izvršeno. Na osnovu imena ili nadimaka pronađenih u imeniku mobilnog telefona, dodeljenih im pretplatničkih brojeva i adresa elektronske pošte, mogu da se identifikuju lica, posebno kada se radi o organizovanoj grupi [36].

Digitalni kompjuterski dokaz formira se iz velikog broja posrednih stvarnih dokaza, od kojih se ni jedan ne sme isključiti iz bilo kog razloga. Dokazi moraju biti potpuni, da se međusobno dopunjuju i da su bez tzv. pukotina za donošenje zaključaka, odnosno za utvrđivanje čvrstog digitalnog dokaza.

Opšti principi IOCE za rad sa digitalnim dokazima harmonizuju metode i praksu između država, što garantuje uzajamnu prihvatljivost digitalnih dokaza, ili tzv. transnacionalni menadžment digitalnih dokaza, odnosno prihvatljivost digitalnih dokaza u jednoj zemlji, iako su prikupljeni u nekoj drugoj. Sudska praksa prihvata kompjuterski generisane i kompjuterski memorisane digitalne dokaze pod odgovarajućim uslovima.

[1] *International Organization of Computer Evidence (http://www.ioce.org)*

Transformacija podataka iz serije kodiranih bita u sudski dokaz je apstraktan proces koji može izazvati sumnju u autentičnost i integritet kompjuterski generisanog dokaza.

Da bi se obezbedila održivost dokaza na sudu, u toku istragene sme doći do izmene podataka, ili njihovog oštećenja. Zbog toga je neophodno pridržavati se procedura rukovanja i čuvanja, kao i procedura za akviziciju i analizu digitalnih dokaza.

Tokom 1999.godine, IOCE je usvojila principe za navedeno postupanje, a oni se ogledaju u sledećem:

- Pre, tokom i nakon uzimanja digitalnih dokaza, ni jedna preduzeta akcija ne sme da izazove izmenu digitalnog dokaza;
- Kada za to postoji potreba, samo dobro obučeno lice (forenzički kompetentno) može pristupiti originalnom digitalnom dokazu;
- Sve aktivnosti koje se odnose na sakupljanje, skladištenje, pristup ili transfer digitalnih dokaza moraju biti potpuno dokumentovane, sačuvane i raspoložive za stavljanje na uvid, bilo kojoj zainteresovanoj strani u sporu;
- Lice koje rukuje digitalnim dokaznim materijalom odgovorno je za sve aktivnosti u odnosu na digitalni dokaz, kada je isti u njegovom posedu;
- Agencija koja je odgovorna za menadžment digitalnih dokaza, odgovorna je za usklađenost svih postupaka, radnji i aktivnosti u skladu sa ovim principima [37].

Najveću vrednost na sudu imaju takozvani dokazi bez pukotina, koji u potpunosti pokrivaju zaključke i objašnjenja, a njih je najteže prikupiti. Na osnovu čvrstih (neoborivih) dokaza nepobitno se utvrđuje postojanje bića krivičnog dela, odnosno šta se stvarno desilo, šta je izgubljeno i koliki je iznos štete. Pri tome, mora se zadržati potpuna objektivnost. Prikupljanje dokaza počinje postavljanjem hipoteze o događaju, a dokaze treba prikupljati na mestu kompjuterskog krivičnog dela, jer to može biti jedini kontakt sa stvarnim dokazima. Treba raditi metodično, polako, sakupljati ključne dokaze i kritički se vraćati na postavljenu hipotezu, tražeći odgovore na pitanja: zašto dokaz nije dobar, gde se izgubila neka važna činjenica, kako naći dokaz koji popunjava prazninu, šta uraditi ako se pronađe itd. U ovoj fazi istrage jednako je važno dokazati kao i opovrgnuti dokaz.

Sa lica mesta se prikupljaju svi posredni dokazi i indikatori nedozvoljene delatnosti, a ne samo ono što digitalni forenzičar misli da treba. U tom smislu, tokom akvizicije digitalnih dokaza, potrebno je generalno snimiti listu fajlova i logova kao dokaze, čak i da ne postoji percepcija o nedozvoljenoj delatnosti ili konkretnom krivičnom delu. U dokazni materijal treba uvrstiti svaki fajl koji potencijalno može sadržati dokaz, pre nego što se taj fajl prepiše, ili izmeni. Nakon inicijalne pretrage (bez privremenog oduzimanja računara), treba se okrenuti prvobitnoj hipotezi i dograditi je detaljnije prikupljenim dokazima. Velika je verovatnoća da je propušten neki važan dokaz, što je dobar argument da se računar privremeno oduzme, dok traje istraga.

Svaki posredni dokaz, potrebno je tretirati kao da direktno vodi ka nepobitnom dokazivanju izvršenog krivičnog dela, jer su svi dokazi jednako važni i kritični za konkretni slučaj. Tek tada počinje proces izgradnje dokaza bez tzv. pukotina, odnosno, izgradnja neoborivog dokaza [10].

U kompjuterskom incidentu postoje tri osnovne kategorije digitalnih podataka kojimogu činiti digitalni dokaz:

- **Promenljivi podaci -** informacije koje se gube nakon isključivanja uređaja, kao što su podaci u radnoj memoriji (RAM), rezidentni memorijski programi itd. Ovi podaci se mogu izgubiti u toku procesa isključivanja uređaja, pa je veoma važno do kraja precizno sprovoditi proceduru akvizicije. Pre isključivanja uređaja treba ispitati, locirati i izvući osetljive i šifrovane podatke, jerse može desiti da se posle isključivanja ne može doći do njih.
– **Osetljivi podaci -** podaci uskladišteni na memoriji uređaja koji se lako moguizmeniti, kao što je, npr. poslednje vreme pristupa log datoteci itd.
– **Privremeno dostupni podaci -** podaci uskladišteni na memoriji uređaja kojima se može pristupiti samo u određeno vreme (npr. šifrovani podaci).

4.1 Faze istrage

Prvi korak digitalne istrage ili istrage kompjuterskog kriminala je faza obaveštavanja u kojoj se detektuje incident i priprema tim za odgovor (***Notification phase***). Nakon potvrđivanja incidenta od strane tima za odogovor na incident, istraga prelazi u fazu očuvanja dokaznog materijala (***Preservation phase***), sa prvenstvenim ciljem da se osigura lice mesta kompjuterskog kriminala (digital crime scene) i digitalni dokazi što više sačuvaju od modifikacije, tako da istražitelji mogu prikupiti relevantne i precizne dokaze. Istražitelj će obično napraviti tačnu kopiju digitalnog mesta zločina, tako da se dokazi mogu bezbedno analizirati u laboratorijskom okruženju. Posle ove faze, počinje faza pregledanja (***Survey phase***) tokom koje se vrši ispitivanje pojedinačnih delova dokaznog materijala. U toku ove faze, istražitelji koristeći postojeće znanje o incidentu i ranija iskustva, pronalaze očigledne dokaze. Nakon ove faze, istražitelj će imati jednu ili više hipoteza o incidentu i tu počinje faza pretraživanja (***Search phase***) u kojoj se vrši temeljnija pretraga sistema radi pronalaženja dodatnih dokaza, koji mogu podržati ili opovrgnuti ranije postavljene hipoteze.

Nakon prikupljanja digitalnih dokaza kroz prethodne dve faze, počinje faza rekonstrukcije (***Reconstruction phase***) u kojoj se postojeći dokazi i hipoteze testiraju u odnosu na konačnu teoriju. Poslednja faza istrage je faza prezentacije (***Presentation phase***) u kojoj se konačna teorija obrazlaže strankama (organima ili pojedincima - korisnicima digitalnih dokaza) koje su tražile istragu [11].

4.2 Pravosudni aspekt digitalnih kompjuterskih dokaza

Po pravilima klasičnog svedočenja, svedok može svedočiti samo ako je očevidac, odnosno samo o onome što je lično doživeo (čuo, video, zna), a ne iz druge ruke, što se smatra posrednim dokazom, u žargonu poznatim kao “rekla – kazala” [12]. Međutim, digitalni dokazi se mogu svrstati upravo u kategoriju “rekla – kazala” dokaze, jer se na uređaju ne vidi ništa što je direktno povezano sa događajem.

Na uređaju, login fajlova može se naknadno izmeniti, mogu se promeniti datumi fajlova, izbrisati ili izmeniti dokumenti, što praktično znači da samo osoba koja je izazvala kompjuterski incident (kompjuterski kriminalac) ima direktno saznanje o tome i jedini je očevidac, odnosno neposredni svedok. Zato se digitalni dokazi pred sudom mogu koristiti samo ako su veoma pažljivo preuzeti i ako zadovoljavaju neke specifične kriterijume u sudskom veštačenju (forenzičkoj akviziciji i analizi). Ovi su kriterijumi kritični u pogledu sposobnosti digitalnog forenzičara da sakupi što više posrednih dokaza pomoću kojih se dolazi do neoborivog dokaza. Praktično, posredni su svi dokazi u kompjuterskom krivičnom delu koji se sakupe akvizicijom i analizom samog softvera, računara i/ili računarske mreže. Da bi posredni dokaz bio prihvatljiv za sud mora biti takav da potvrđuje hipotezu o čvrstom dokazu, ili da je pobija. Drugo, mora postojati dokaz da je login fajl, kao posredni dokaz, nastao u normalnom radnom procesu.

Da bi digitalni dokaz bio prihvaćen na sudu, mora biti autentičan - nepromenjen u odnosu na orginalno stanje. Prethodno, originalno, stanje digitalnih dokaza moraju utvrditi i na sudu potvrditi sudski veštaci za IKT svojim svedočenjem, kao i forenzičari i organi istrage koji su te dokaze sakupili, čuvali, analizirali i rukovali njima. Da li će na sudu dokazi biti prihvaćeni ili odbačeni zavisi od toga kako su pribavljeni, čuvani, prenošeni, zaštićeni od izmena i kako se sa njima manipulisalo. Digitalni dokazi moraju zadovoljiti i sve ostale zahteve pravosudnih organa, koji se odnose na sudske dokaze, a u ovom slučaju to znači da:

- ako je potrebno koristiti kopiju, ona mora biti najbolja;

- ako je original na raspolaganju onda kopija ne važi;

- kopija može zadovoljiti sve zahteve za izvođenje dokaza (npr. printing login fajlova), ako postoji originalni fajl u kompjuteru za upoređenje i

- sudski veštak za IKT mora posvedočiti kako je kopija (npr. printing login fajlova) napravljena, kao i druge detalje o rukovanju sa fajlom i kopijom (printingom).

Originalni dokaz treba biti sačuvan u originalnom ili stanju što približnijem onom u momentu pronalaženja. Ako je uopšte moguće, potrebno je napraviti preciznu kopiju (digital image) originala da bi se na kopiji vršilo ispitivanje i na taj način sačuvao i zaštitio integritet originala. Kopije podataka napravljenih u svrhu ispitivanja treba da budu kreirane na forenzički sterilnom mediju (medij ili disk na kome prethodno nije bilo podataka, koji je potpuno čist, bez virusa i defekata). Svi dokazi moraju biti propisno označeni i dokumentovani. Lanac nadležnosti, takođe mora biti očuvan, a svaki korak forenzičkog ispitivanja biti detaljno dokumentovan [38].

4.3 Karakteristike forenzičkih alata za kreiranje precizne kopije digitalnih dokaza

Jedan od faktora za određivanje pouzdanosti digitalnih dokaza je postupak akvizicije. Zbog toga, grupa za testiranje računarskih forenzičkih alata pri Nacionalnom institutu za standarde i tehnologiju (NIST) dala je specifikaciju zahteva za alate za snimanje imidža - digitalne slike dokaznog materijala [11]. Pomenuti zahtevi se ogledaju u sledećem:

1. Forenzički alat (instrument) za akviziciju digitalnih podataka će čitati sve digitalne podatke sa izvora i ispisivaće ih na nepromenljivoj (stalnoj) lokaciji. Lokacija koja se zove slika će biti u formatu kojem se može pristupiti.

2. Forenzički alat neće izazvati (uzrokovati) ispisivanje podataka na izvoru;

3. Forenzički alat će slediti ispisanu proceduru koja uključuje korake koji koriste i hardver i softver u čitanju izvornih podataka;

4. Ukoliko se pojave I/O greške (greške na ulazu / izlazu) u toku čitanja izvornih podataka, forenzički alat će napisati specifičnu vrednost koja odgovara lokaciji na slici. Forenzički alat će zapisati tip i lokaciju greške u formatu kojem se može pristupiti;

5. Ukoliko je destinacija podataka veća od izvora, forenzički alat će odrediti početnu i krajnju lokaciju izvornih podataka unutar destinacije;

6. Ukoliko je destinacija podataka manja od izvora, forenzički alat će upozoriti korisnika, kada prekine i kada kopira onoliko podataka koliko može stati u određenoj destinaciji;

7. Forenzički alat će obezbediti ispravnu (tačnu) dokumentaciju .

4.4 Upravljanje digitalnim dokazima

Upravljanje digitalnim dokazima obuhvata sakupljanje, prenos, analizu i čuvanje. Dokazi se čuvaju tokom čitavog lanca istrage, vođenja procesa, dokaznog postupka, suđenja i presude, što znači da je dokaz u posedu suda od trenutka akvizicije do završetka suđenja. Prikupljeni dokaz se mora čuvati od štetnih uticaja koji mogu dovesti do oštećenja: toplote, hladnoće, vode, elektromagnetnog dejstva itd.

Osim pouzdanih svedoka i eksperata, u istrazi kompjuterskog incidenta, moraju biti pouzdani i softverski i hardverski alati za forenzičku akviziciju i analizu digitalnih podataka. Softverski i hardverski forenzički alati, programi za praćenje saobraćaja i detekciju upada u radnu memoriju treba da budu namenski, komercijalno dostupni proizvodi sa sertifikatom o pouzdanosti za ovu vrstu poslova. Dokazi do kojih se došlo primenom nepouzdanih i ne-sertifikovanih forenzičkih alata, mogu biti odbačeni od strane suda.

4.5 Procedura sakupljanja posrednih kompjuterskih dokaza

Akvizicija digitalnih dokaza obuhvata otkrivanje, identifikaciju, izvlačenje i sakupljanje tih dokaza. Sakupljanje digitalnih dokaza zaokružuje se kroz više aktivnosti, a svaka ozbiljnija procedura sakupljanja dokaza treba da obuhvatinajmanje sledeće aktivnosti [10]:

1. Sakupljati sve podatke koji podržavaju osnovnu hipotezu o tome kako je došlo do kompjuterskog incidenta, odakle je napad potekao i šta je urađeno na napadnutom računaru - uređaju.

2. Sakupiti sve podatke koji su kontradiktorni postavljenoj hipotezi, da bi se podržalo dato objašnjenje, ili lakše suprotstavilo argumentima druge strane usporu. U većini slučajeva, posebno u kriminalističkoj proceduri, treba imati na umu da obe strane žele da otkriju i podnesu neoborive dokaze.

3. Sakupiti sve pokretne medije (diskete, CD-ROM,...) otkrivene na lokaciji osumnjičenog računara i analizirati ih. Ta analiza može se vršiti pomoću programa za analizu pokretnih medija (npr. Sydex Anadisk za diskete). Takođe se moraju prikupiti svi štampani materijali, rukopisi, zabeleške i dr. koji mogu ukazati na rasvetljavanje spornog događaja.

4. Napraviti skice ili fotografisati osumnjičeni računar i sve periferne uređaje; označiti i sačuvati sve periferne uređaje i kablove radi ponovne montaže u forenzičkoj laboratoriji.

5. Ako postoje matrični ili impakt printeri, ukloniti ribon i staviti novi; originalni ribon ispitati kao dokazni materijal; ako postoji displej na kompjuterskom ekranu, fotografisati ga.

6. Isključivanje osumnjičenog računara je posebno osetljiva operacija. Zavisno odoperativnog sistema (OS), postoje dve mogućnosti: ispitivani računar se može isključiti na klasičan način bez straha da će se izbrisati dokazi o upadu, ili se nesme isključivati, jer bi se isključivanjem mogli uništiti dokazi o upadu. Naprimer, ako se Unix mašine ne isključe propisno može doći do oštećenja fajlova, ali ako se Windows mašina isključi propisno, može doći do gubitka potencijalnih dokaza. Međutim, u ovim sistemima se lako kreiraju antiforenzičke, tzv. boby zamke za uništavanje fajlova sa dokazima, ako se računar isključuje po propisu.

Zato uvek postoji dilema da li računar isključiti propisno i sprečiti uništavanje nekih fajlova, ili ga isključiti nepropisno čime se omogućava aktiviranje boby zamke koja može da uništi dokaze. Kako će postupiti u konkretnom slučaju, to sam istražni organ mora proceniti. U ovom slučaju najbolje je koristiti pomoć sudskog veštaka, eksperta za IKT, odnosno specijaliste za dati OS i platformu, kome se mora dobro objasniti legalni aspekt zahteva za zaštitu integriteta digitalnih dokaza.

7. Ako je sigurno da postoji ugrađena zamka, najbolje je računar jednostavno isključiti iz mreže izvlačenjem kabla za napajanje sa zadnje strane računara, uz rizik da će biti uništeni neki podaci. Naravno, neki računari tako ne mogu da se isključe, npr., mainframe i mikrokompjuteri. Zato je potrebno angažovanje eksperta za IKT, koji treba da onesposobi svaku logičku bombu sakrivenu u napadnutom računaru.

8. Za rebutiranje ispitivanog računara nikada ne treba koristiti njegov OS i komandnu liniju. Računar treba butirati sa butabilnog diska, koji je fizički zaštićen od upisivanja, čime se sprečava unošenje virusa, ili sa CD ROM–a koji je fizička slika OS.

9. Kada se završi rebutiranje sistema, prvo se uzima fizička slika HD–a (alatom tipa Drivespay, X-Way Forensic i sl.), zatim se sakupljaju drugi dokazi i preliminarno ispituju. Najbolji način za skladištenje fizičke slike HD je optički disk (CD), jer je otporan na oštećenja usled elektromagnetnih zračenja iz okruženja, tj. ne možese brisati (osim ako je rewritable tipa), a može se lako kopirati.

10. Privremeno oduzeti osumnjičeni računar sa svim pokretnim medijima, treba uskladištiti na bezbedno mesto, zaštićeno od uticaja okoline, posebno elektromagnetnih polja i obezbediti od neovlašćenog pristupa, jer se veštak mora zakleti na sudu da dokazni materijal nije bio dostupan neovlašćenim licima.

11. Za razliku od pisanog dokaza, digitalni dokaz često može egzistirati u različitim formatima ranijih verzija koje su još dostupne na HD. Poznavanjem lokacija njihovog postojanja i korišćenjem adekvatnih alata za forenzičku akviziciju sa različitih apstraktnih slojeva računarskog sistema, čak i izmenjeni formati istih podataka mogu se lako otkriti. Proces akvizicije najbolje poznaje iskusni forenzičar, koji najbrže otkriva moguće dokaze. Osim toga, u slučaju preliminarnog ispitivanja i identifikacije digitalnih dokaza na licu mesta, kada se računar iz nekog razloga ne oduzima u cilju istrage, niti se pravi forenzička kopija HD, forenzičar najbrže identifikuje skrivena, nealocirana i izbrisana mesta koja treba gledati, znake koje treba tražiti i dodatne izvore informacija za relevantne dokaze, kao što su raniji formati podataka, npr. u Memos, Spreadsheets koje postoje na HD, ili u bekap mediju, ili različito formatirane verzije podataka, npr. .**templets**, .**doc**, .**pdf** i sl., bilo da su tako namerno formirane ili su tretirane drugim aplikativnim programima, npr. *Wordprocessing*, *spreadsheet*, *e-mail*, *timeline*, *sheduling*, *graphic*.

12. Zaštita integriteta dokaza je kritična faza. Iskusan forenzičar mora obezbediti:

- da ni jedan mogući dokaz ne bude oštećen, uništen ili kompromitovan na neki način tokom procedure forenzičke akvizicije i analize računara,

- da se ni jedan mogući kompjuterski virus ne ubaci u ispitivani računar u toku procesa akvizicije i analize,

- da se sa potencijalno relevantnim dokazima propisno manipuliše i dase štite od eventualnih mehaničkih ili elektromagnetskih oštećenja,

- da se uspostavi neprekidni lanac čuvanja i održavanja integriteta dokaza,

- da funkcionalni aspekt ispitivanog sistema bude ugrožen što je moguće kraće vreme,

- da se dobije bilo koja potrebna informacija u toku forenzičke akvizicije i analize, od saslušavanih lica ili advokata koji su prema etičkom kodeksu dužni pružiti sve neophodne informacije forenzičaru.

4.6 Korisnici digitalnih dokaza

U procesu istrage, digitalne dokaze mogu zahtevati i koristiti tužilaštvo, pravosudni organi u privatnom parničkom postupku (pronevera, razvod, diskriminacija, uznemiravanje i sl.), osiguravajući zavodi (u slučajevima prevara oko kompenzacija oštećenim licima i sl.), organizacije (vlasnici napadnutog informacionog sistema), zvanični istražni organi (MUP, BIA, VBA), pojedinci (vlasnici napadnutog sistema) i udruženja i samostalni IKT veštaci za potrebe veštačenja [10].

4.7 Priprema digitalnih dokaza za veštačenje pred sudom

Nezavisni ekspert za IKT koji pomaže istražnom organu u otkrivanju i akviziciji podataka treba da ima iskustvo iz široke oblasti informaciono komunikacionih tehnologija. Takav ekspert je uvek od velike koristi kada se obavlja istraga konkretnog kompjuterskog incidenta.

Iako je osnovni dizajn uređaja i aplikativnog softvera često vrlo sličan kod većine OS, te se znanje o jednom sistemu lako koristi sa drugim sistemom, ipak za poslove akvizicije i forenzičke analize uvek treba angažovati kvalifikovanog eksperta za IKT, specijalistu za konkretni OS, program, platformu, mrežu itd.

Digitalne dokaze od trenutka otkrivanja do zaključno sa forenzičkom analizom, treba uvek tretirati kao da će biti prezentirani na sudu. Na sudu u parničkom ili krivičnom postupku, zavisno od težine kompjuterskog incidenta, digitalne dokaze prezentira - veštači zakleti sudski veštak za IKT, kvalifikovan za predmetni hardver i softver, krajnje objektivno, tačno, uverljivo i razumljivo. U najvećem broju slučajeva digitalne dokaze na sudu prezentira forenzičar koji je u toku istrage vršio akviziciju i forenzičku analizu digitalnih dokaza. Naravno, obe strane u sporu mogu zahtevati i druge, nezavisne veštake za IKT, što neminovno podrazumeva unakrsno ispitivanje i sučeljavanje mišljenja dva veštaka za IKT, podjednako istih znanja i iskustava. To je u praksi često faktor odvraćanja jer istaknuti eksperti za IKT odbijaju sudsko veštačenje i sučeljavanje mišljenja sa drugim podjednako dobrim sudskim ekspertom i radije prihvataju ulogu neutralnog stručnog konsultanta tužioca ili samog sudije.

U pripremi za prezentaciju digitalnih dokaza na sudu veštaci za IKT moraju obaviti mnogobrojne konsultacije sa advokatom stranke koja ih angažuje (tužilaštva ili odbrane) za izbor metode prezentacije (korišćenje pomoćnih audio – vizuelnih sredstava, strategiju nastupa i sl.), a sami se psihički pripremaju za unakrsno ispitivanje i eventualno suočavanje sa svedočenjem drugog veštaka [10].

4.8 Preporuke IOCE za upravljanje digitalnim dokazima

Preporuke IOCE definišu postupke sa prikupljenim i obrađenim dokazma:

– Za čuvanje fizičke kopije digitalnih dokaza nisu prihvatljivi instant film paket, indžekt printeri, ink printeri, termalni voštano – papirni printeri, dyesublimacioni printeri, suvo srebreni printeri, laserski printeri i elektrostatički printeri.

— Za čuvanje originalne fizičke kopije digitalnih dokaza prihvatljivi su, zbog kvaliteta, trajnosti i pouzdanosti klasični filmovi na bazi srebro – oksida, CDROM za jedno upisivanje (ne RW) i DVD.

— Za čuvanje originalne fizičke kopije digitalnih dokaza mogu se koristiti, uz kontrolu eventualnih gubitaka podataka posebno razvijan instant film, fotografski print, diskete, magnetne trake, HD, prenosni magnetni mediji, kompakt fleš memorija, PC kartice, smart kartice, prenosni magnetno–optički diskovi i magnetno–optički diskovi za jedno upisivanje.

Za analizu treba koristiti radnu fizičku kopiju, a jednu fizičku kopiju sumnjičenog računara sačuvati kao referentni dokaz integriteta.

– Dokumentacija za analizu fizičke slike osumnjičenog računara mora biti precizna, detaljna, neporeciva i napravljena na poverljivom forenzičkom sistemu.

– Verifikacija referentne i analizirane radne kopije mora biti obavezna i da nepobitno potvrđuje da nije bilo povrede integriteta originalnih dokaza.

– Čuvanje referentne fizičke kopije u lancu istrage je stroga obaveza od pokretanja istrage i otkrivanja dokaza do svedočenja na sudu.

Procedura se mora administartivno propisati u svakom pravosudnom sistemu i mora postojati zakonska obaveza svakog pojedinca da čuva integritet dokaza.

5. Digitalna forenčka analiza prenosnih računara i USB memorija

5.1 Specifičnosti fleš tehnologije od značaja za izbor forenzičkih alata i procedura

Prenosni uređaji kao što su mobilni telefoni, PDA, muzički plejeri, USB diskovi, digitalni fotoaparati, Solid stejt diskovi (Solid state drives) i mnogi drugi, za smeštaj podataka koriste fleš (flash - eng.) memoriju, koja je dostupna u dve varijante [13], [14], [39]:

1. NOR fleš (Not OR) – na kojoj se mogu skladištiti podaci i koja omogućava rad - izvršenje operacija softvera. Takođe, omogućava i podržava velike brzine slučajnih pristupa. Nedostatak ove vrste fleš memorije je taj što je njena izrada veoma skupa.

2. NAND fleš (Not AND) – i na ovoj memoriji se mogu skladištiti podaci, ali ona ne omogućava rad - vršenje operacija softvera. Zbog toga, softver smešten na ovoj memoriji mora da se kopira na NOR ili RAM memoriju radi izvršenja. Ona predstavlja noviji tip fleš memorije, dugotrajnija je i jeftinija za izradu, uz mogućnost skladištenja većih kapaciteta podataka i niže brzine operacije čitanja/pisanja, u odnosu na tip NOR.

Zajedničko za ove dve vrste fleš memorija je to da će svaki bit u novom fleš čipu biti imenovan logičkom jedinicom (1) samo ako operacija ispisa (WRITE) može da izmeni svoju vrednost iz 1 u 0, a jedini način za ovu promenu odvija se kroz operaciju brisanja (ERASE).

NAND fleš memorijski čipovi su podeljeni u blokove. Svaki blok ima unapred definisan, fiksan broj stranica koje su dalje podeljene po regionima za skladištenje podataka. Između je slobodan prostor - oblast koja održava statuse regiona za skladištenje podataka. Kod prve generacije NAND fleš memorije, stranica je bila tipične veličine od 512 bajtova, uz koji je išlo dodatnih 16 bajtova takozvanog "out of band" skladišnog prostora koji je dizajniran da se koristi za metapodatke i korekciju grešaka.

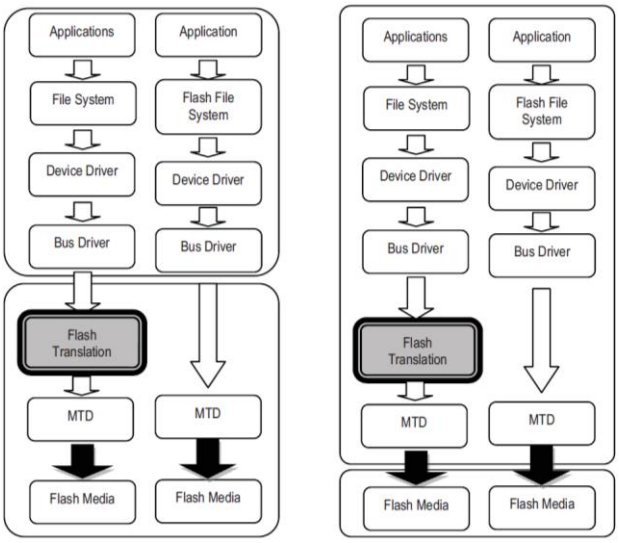
Upisivanje na NAND fleš memoriji vrši se ubrizgavanjem podatka, bajt po bajt, u interni bafer, svaki put zahtevajući komandu za pisanje (WRITE). NOR fleš memorija funkcioniše drugačije, dozvoljavajući da svaki bit bude izbrisan pojedinačno. U NAND memoriji, samo nekoliko ciklusa ispisa (WRITE) se upisuje na svakoj stranici, pre nego što sadržaj stranice postane nedefinisan i mora da čeka sledeći ciklus brisanja blokova u kojima se nalazi stranica. Drugim rečima, prilikom svake promene podataka, novi podaci moraju biti napisani na drugoj dostupnoj stranici i na drugoj lokaciji. Zato se stara stranica, na kojoj je podatak bio prvobitno napisan, smatra mrtvom stranicom. Kada istekne period ciklusa, akumulirane mrtve stranice se brišu (ERASE) i one su ponovo na raspolaganju.

Ovaj proces povraćaja mrtvih stranica poznat je kao "sakupljanje smeća" (“garbage collection”). Blokovi fleš memorija imaju ograničen broj dozvoljenih ciklusa brisanja, pa se nastoji na ravnomernom brisanju/pisanju u svim blokovima, kako bi se produžio životni vek vleš memorije.

Za razliku od ostalih tipova memorija (kao što su memorije sa direktnim pristupom (RAM) i magnetni diskovi, fleš memorije imaju ograničen broj ciklusa upisa i brisanja podataka, obično između 10.000 i 1.000.000 ciklusa, nakon čega postaju nestabilne.

5.1.1 FLASH TRANSLATION LAYER (FTL)

Za svoj rad, NAND fleš memorija zahteva specifičan fajl sistem, ili specifičan drajver. Posebni fleš fajl sistemi su IAFFS, JFFS, UBIFS, aLogFS dok je drajver poznatiji kao Flash Translation Layer. Ovaj drajver radi u sprezi sa postojećim operativnim sistemom (ili kao operativni sistem u nekoj od ugrađenih aplikacija,) kako bi fleš memoriju prikazao u fajl sistemu kao hard disk. Mogu se razlikovati dve vrste fleš memorijskih čipova, kao što je prikazano na slici 1 [13].



Slika 7. - Arhitektura fleš memorijskog čipa u odnosu na MTD

Prvi tip uključuje MTD i FTL drajver u jednom paketu, kao što je to slučaj kod USB fleš diska. Druga vrsta ne uključuje MTD, stoga je ovaj sloj blok nivoa odgovoran za preusmeravanje lokacije ažuriranih podataka sa jedne stranice na drugu. Takođe je odgovoran za upravljanje stvarnom fizičkom lokacijom podataka u tabeli mapiranja. Ovo mapiranje logičke u fizičku lokaciju može se postići samo na nivou stranice (FTL) ili na nivou bloka (NFTL). Glavne razlike između ove dve tehnike mapiranja su u veličini tabele i ograničenju preusmeravanja.

Obe tehnike se mogu primenjivati direktno na FTL sloju. Direktno korišćenje postojećeg fajl sistema može uticati na performanse zbog činjenice da su fajl sistemi dizajnirani i razvijeni za sisteme za skladištenje na hard disku, čiji se način pristupa datotekama i odnosu prema veličini datoteka i metapodacima datoteke razlikuju od uređaja sa fleš memorijom [13].

5.1.2 Kontroleri

Na magistrali USB uređaja smešten je kontroler koji komunicira sa host mašinom i fleš čipom za skladištenje. Fleš memorijski čip je pravougaonog oblika, ravan, tanak, sa nizom pinova sa obe strane. Neki fleš memorijski uređaji imaju više od jednog takvog čipa. Kontroler je odgovoran za obavljanje operacija pisanja/čitanja u konkretnom sektoru. Ukoliko se prekidač prebaci na režim "samo za čitanje", u trenutku ubacivanja uređaja, kontroler će saopštiti host uređaju da je fleš disk samo za čitanje i ignorisaće zahteve za upis. Sa druge strane, domaćin koristi ovu informaciju u upravljačkom sistemu datoteka i upravlja fleš diskom u režimu "samo za čitanje" [40].

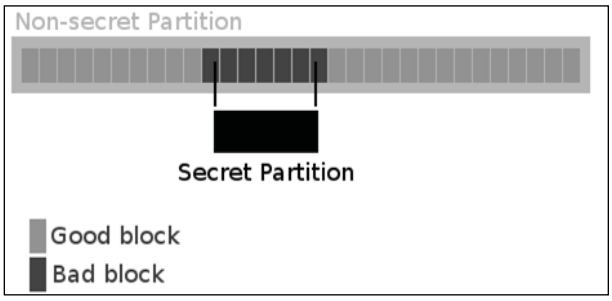
5.1.3 Mapiranje

Da bi se izvršilo čitanje sektora, brojevi sektora moraju biti mapiraniu delu fleš čipa. Ovo je slično načinu na koji se memorija fizički mapira na stranicama virtuelne memorije u pokrenutom procesu. Tako određena adresa sektora za čitanje upućuje se na adresnu magistralu (koja je povezana setom pinova na fleš čipu). Stabilizacijom signala na adresnoj magistrali bira se fleš linija za aktiviranje i očitavaju se podaci. Da bi se izvršilo pouzdano očitavanje čipa, važno je da se naponski nivoi stabilizuju. Čipovi imaju tabelu sa detaljnom specifikacijom nivoa napona i obrazaca pristupa. Ukoliko se prekorače predviđene veličine, sistem postaje nestabilan [40].

5.1.4 Brisanje podataka i manipulacije skrivenim zonama

Brisanje podataka sa uređaja je poznata, ali još uvek nedovoljno istražena aktivnost, što treba imati u vidu kod digitalne forenzičke analize fleš memorija. To je pozadinska aktivnost koju prenosni uređaj, čak i u pasivnom režimu, može aktivirati autonomno, čime bi se uništili korisni podaci u lošim blokovima (kada na bloku postoje greške koje se ne mogu otkloniti). Kao i kod hard diskova, NAND memorija se isporučuje sa listom postojećih loših blokova, čija je mesta mapirao proizvođač. Na ovu listu dodaju se svi budući loši blokovi koji nastaju tokom korišćenja uređaja. Pristup i upravljanje lošim blokovima su otežani ako je FTL ugrađen u fleš memoriju jer će oni biti sakriveni u fajl sistemu uređaja. Ako se koristi FTL fajl sistema uređaja, onda postoje šanse za upravljanje lošim blokovima.

Postoji mogućnost za manipulaciju takozvanom ''BadBlockList'' (listom loših blokova) koja teži da sakrije informacije o postojanju ovih blokova. Imajući u vidu da je kapacitet fleš memorija zbog toga veći od količine podataka koji se može nasnimiti, ovo treba imati na umu tokom digitalne forinzičke istrage prenosnih računara sa korišćenom NAND memorijom. Zloupotreba za skladištenje podataka moguća je i u zaštićenoj zoni memorije (Hidden protected area), iako je ona načelno veličine jednog bloka.

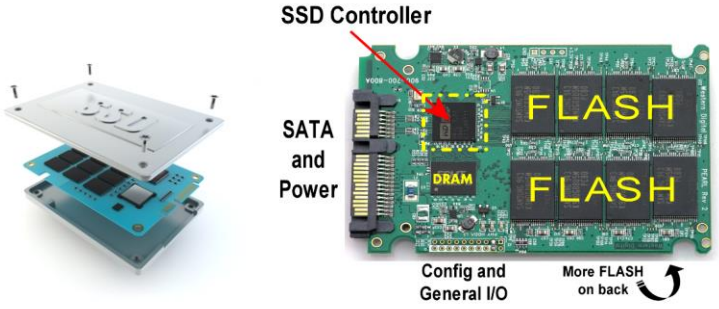


Slika 8. - Skrivanje podataka u lošim blokovima

Kao kod hard diskova (Host Protected Areas (HPA) i Device Configuration Overlays (DCO)) i kod fleš memorija postoji mogućnost da se promeni (duplira) dimenzija zaštićene zone, a zatim uskladište i sakriju podaci [15].

5.2 Solid State Drive (SSD)

Solid Stejt disk (SSD) je najnovija generacija čvrstih diskova, bazirana na fleš tehnologiji. Svojim performansama ugrožavaju opstanak mehaničkih diskova, ali zbog svog odnosa cene i kapaciteta nisu preuzeli primat u primeni (1GB SATA diskova košta od 0,04 € do 0,1 € u zavisnosti od kapaciteta, a 1 GB SSD košta od 0,77 € do 1 €). Nomenklaturno, SATA diskovi odlikuju se brzinama prenosa od 150 (SATAI) do 600 MB/s (SATAIII), dok se brzina prenosa kod SSD kreće od 450 – 500 MB/s. Međutim, SATAIII, iako imaju mogućnost da preko kabla obavljaju pomenuti transfer, u praksi to ne mogu jer su ograničeni zbog svoje strukture, tj. Nepostoje diskovi koji mehaničkim okretanjem glave mogu da isporuče tu količinu podataka, već je upitanju red veličine 150 MB/s i manje [41].



Slika 9. Solid state drive (SSD) controller[2]

[2]preuzeto sa http://webscopia.com/2011/10/what-is-an-ssd-solid-state-disk-basics-andperformance-measures

Za razliku od magnetnih hard diskova, SSD diskovi nemaju pokretne delove i ne oslanjaju se na magnetno polje za upis podataka na disk, jer oni koriste elektricnu sturuju, a ne motore i magnete za skladistenje podataka. Takođe, SSD ne podležu fizičkim oštećenjima od udarca ili velike magnetne sile, što ih čini pogodnim za prenosne računare. SSD koristi niz tranzistora, komade silikona i poluprovodnika za prenos električne struje. Svaki komad je mikroskopski i na svaki deo može da utice transfer nekoliko elektrona.

SSD koristi binarni sistem za upis podataka. Nulu (0) predstavlja tranzistor koji ne može da prihvati električnu struju, dok jedinicu (1) predstavlja tranzistor koji omogućava protok struje.

Prazan disk ili deo praznog diska obeležava se sa svim jedinicama. Svi tranzisotri u ovom delu diska će omogućiti slobodan protok struje. Kada je podatak u procesu snimanja, napon se primenjuje na jedan komad silikona koji je poznat kao (control gate) kontrolna vrata. Ovaj proces prenosi elektrone na drugi deo diska koji se naziva (the floating gate) plutajuća kapija. Kada ta kapija bude ispunjena elektronima, struja neće prolaziti kroz njega i disk će ga čitati kao nulu (0). Na ovaj način informacija se konvertuje u binarni podatak. Ovo se dalje šalje u diskov centar za pisanje podataka, gde se pretvara u električnu struju i koristi za poravnavanje tranzistora. Da bi se pročitao podatak, diskov centar za čitanje podataka šalje struju kroz deo koji drži podatak za čitanje i vraća utrujni signal sekvencama jedinica i nula. Ova sekvenca se šalje do programa i predstavlja se kao informacija koju možemo da pročitamo.

Proces pisanja podataka kod SSD diska nudi nekoliko prednosti, kao što je mogućnost korišćenja diska dok je u pokretu, ali tehnologija je predmet ograničenja. Pre svega, svaki tranzistor može biti korišćen do odredjenog broja puta i nakon toga više neće biti u funkciji. Svaki disk koristi napredne metode, poznate kao nivelisanje potrošnje (wear level), kako bi se sprečila preterana potrošnja samo pojedinih delova diska [42].

Ovo podrazumeva da se podatak koji se menja smešta u drugi blok, pa se na taj način, dok prethodna verzija podatka nije izbrisana, stvara mogućnost da potencijalno interesenatne informacije budu razbacane po čitavom memorijskom čipu. Da bi se povećao vek trajanja i poboljšalo nivelisanje potrošnje blokova kod SSD diskova, pojedini proizvođači čipova povećavaju kapacitet i do 25 % više u odnosu na nomenklaturno prikazani kapacitet. Ovaj dodatni kapacitet se ne adresira od strane operativnog sistema, odnosno ovim fleš čipovima se ne može pristupiti bez prilagođenog hardvera, što utiče na to da je sadržaj na SSD diskovima nemoguće obrisati u potpunosti sigurno, kao što to zahtevaju vojni i standardi pojedinih državnih organa.

Da bi ublažili ovaj problem, neki proizvođači SSD omogućavaju bezbedno uništavanje podataka uskladištenih na svim fleš čipovima implementiranjem ATA Secure Erase (ATA SE) komande koja briše kompletan sadržaj diska na hardverskom nivou. Za razliku od softverskih alata, ATA SE komanda elektronski briše sve blokove na svim fleš čipovima na disku. To u praksi znači da komanda ATA SE vraća SSD na fabričke vrednosti i kada se pravilno realizuje rezultira kompletnim brisanjem svih regiona za skladištenje na SSD disku, uključujući rezervisane i sistemske oblasti [16].

Nivelacija potrošnje blokova utiče na intenzivno korišćenje skladišnog kapaciteta diska jer se za svaku operaciju upisa koriste ranije oslobođeni blokovi. Čak i ponovni upis na postojećem fajlu utiče da ceo sadržaj SSD diska postane "prljav", što dovodi do smanjenja brzine pisanja. Ovo se dešava zato što fleš tehnologija koja se koristi u SSD diskovima zahteva da kontroler briše sadržaj bloka tek pre nove operacije upisa.

Ukoliko nema praznih (prethodno izbrisanih) blokova, SSD disk pun "prljavih" blokova će zahtevati dosta vremena da izvrši komandu upisa jer je proces brisanja upisanih blokova sporiji u odnosu na čitanje i pisanje.

Zbog toga su proizvođači SSD osmislili proces nazvan "garbage collection" - "odnošenje smeća", koje podrazumeva brisanje "prljavih" blokova u pozadini, čineći ih tako ponovo dostupnim za brzo upisivanje. Problem sa "odnošenjem smeća" je da ni diskovi, ni njihovi kontroleri ne prepoznaju koji blokovi su zauzeti datotekama, koji operativnim sistemom, a koji se ne koriste jer su samo "prljavi".

Navedena operacija usporava rad SSD, pa je razvijen interfejs koji omogućava da operativni sistem obavesti kontroler koji blokovi više nisu u upotrebi, prekokomande TRIM[3] [43]. Ovo omogućava elektronsko brisanje sadržaja tih blokova, pripremajući ih za buduće operacije upisivanja. Na ovaj način, blokovi podataka se fizički brišu, pa se informacije iz takvih blokova ne mogu povratiti čak i uz korišćenje skupih, specijalno prilagođenih hardverskih komponenti.

Ovaj proces je nazvan i "samo-korozija", a u forenzičkom smislu predstavlja samo-uništenje sudskih dokaza. Proces "sakupljanja otpada" radi u pozadini i kod većine modernih SSD trajno će izbrisati podatke označene za brisanje. Ovaj proces se ne može sprečiti premeštanjem diska na drugi računar ili aktiviranjem blokiranja pisanja na uređaju. Jedini način da se spreči "samo-korozija" je fizičko odvajanje kontrolera diska iz fleš memorijskih čipova čuvanje podataka, kako bi se potom pristupilo čipovima direktno, preko posebnog hardvera.

Ukoliko nije izdata, ili podržana komanda TRIM, povraćaj podataka je moguć, na isti način kao i sa tradicionalnog hard diska. TRIM protokol je onemogućen u sledećim slučajevima:

[3]Komanda TRIM blokove za brisanje obeležava kao neodređene, do trenutka kada se ovi blokovi fizički brišu u pozadinskom procesu ("sakupljanje otpada").

- Stari SSD diskovi - ne podržavaju TRIM komandu;
- Stare verzije Windows-a- u operativnom sistemu Windows Vista i ranijim verzijama, TRIM protokol nije bio podržan. Izuzetak je moguć, preko pojedinih nezavisnih rešenja (npr. Intel SSD Optimizer, deo Intel SSD Toolbok).

- Stare verzije MacOS X - podršku za TRIM komandu, kompanija Apple isporučuje sa SSD diskovimapočev od verzije 10.6.8.

- **(Windows) fajl sistemi koji nisu NTFS** - u operativnom sistemu Windows, za sada samo particije formatirane kao NTFS imaju punu podršku za TRIM.

- **Eksterni diskovi, USB kućišta i Network Attached Storage** - komanda TRIM je u potpunosti podržana preko SATA interfejsa, uključujući eSATA i SCSI (preko UNMAP komande).

- PCI-Ekpress SSD- komanda TRIM nije izvorno podržana ni u jednoj verziji Windowsa za visoke performanse SSD diskova koji se koriste preko PCI Ekpress slota. Izuzetno, TRIM komanda može biti omogućena preko pojedinih nezavisnih rešenja (Intel SSD Optimizer, deo Intel SSD Toolbok-a).

- RAID- komanda TRIM, generalno nije podržana preko RAID konfiguracije (osim nekoliko vrlo retkih izuzetaka).

- Logička korupcija- SSD diskovi sa oštećenim sistemskim oblastima (oštećene tabele particija, oštećen fajl sistem itd.) lakši su za oporavak podataka od neoštećenih, jer se komanda TRIM ne izdaje preko korumpiranih oblasti. U oštećenim oblastima fajlovi nisu potpuno izbrisani, već su samo nevidljivi, odnosno nedostupni operativnim sistemima.

Mnogi komercijalno dostupni alati za oporavak podataka (npr. Intel ® Solid-State Drive Toolbok sa Intel ® SSD Optimizer, OCZ SSD Toolbok) pouzdano mogu izdvojiti informacije iz logički oštećenih SSD diskova [44].

- Šifrovane particije - informacije izbrisane sa pojedinih šifrovanih particija (neke konfiguracije BitLocker, TrueCript, PGP i drugih) mogu se lakše oporaviti, jer na njih ne utiče komanda TRIM. Fajlovi izbrisani iz tih šifrovanih particija na SSD disku mogu se povratiti (ukoliko nisu izričito obrisane (wipe) od strane korisnika), ako istražitelj zna prvobitnu lozinku, ili binarne ključeve za dešifrovanje particije. Zbog procesa nivelisanja potrošnje, šifrovane particije ne funkcionišu u potpunosti na SSD diskovima. U mnogim konfiguracijama, u kriptovanim particijama šifruje se čitav skladišni prostor, uključujući i slobodni, što utiče na smanjivanje brzine pisanja. Kreirana šifrovana particija fiksne veličine onemogućava efekat komande TRIM za čitav sadržaj šifrovane particije.

Pravi način za akviziciju podataka sa računara sa šifrovanom particijom može se opisati sledećom rečenicom: "Ako je pokrenut, nemojte ga isključili, ako je isključen, nemojte ga uključiti". Originalni ključevi za dešifrovanje keširaju se u memoriji računara, odakle se mogu ekstrahovati iz Live RAM dumpa, putem takozvanog FireWire napada. Ovi ključevi mogu se nalaziti i u page fajlovima i datotekama o hibernaciji. Alati, kao što je Elcomsoft Forensic DiskDecryptor, mogu izdvojiti fajlove za dešifrovanje iz memorije dumpova i page/ fajlova o hibernaciji, kako bi se dešifrovao sadržaj šifrovane particije.

Blokatori pisanja ne mogu da spreče brisanje podataka uskladištenih na SSD disku koje je inicirao korisnik uređaja jer ne utiču na komandu TRIM i pozadinsko brisanje diska i uništenje eventualno interesantnih zaostalih izbrisanih informacija. Sprečavanje "prikupljanja smeća" moguće je samo fizičkim isključivanjem ugrađenog kontrolera na fleš čipovima, uz direktno pristupanje informacijama uskladištenim u čipovima. Ova metoda je nepopularna jer zahteva posebne veštine i prilagođeni hardver.

Nakon fizičkog odstranjivanja kontrolera i korišćenjem prilagođenog hardvera moguće je direktno očitavanje informacija iz flash čipova i izdvajanje tragova uništenih podataka koje mogu biti uskladištene u različitim oblastima fleš čipova [44].

5.3 Specifičnosti mobilnih telefona od značaja na digitalnu forenzičku analizu

Mobilni telefoni su laki i kompaktni komunikacioni uređaji koji imaju mogućnost obavljanja niza funkcija. U osnovi se sastoje od mikroprocesora, stalne memorije (ROM), u kojoj je smešten operativni sistem, privremene memorije (RAM) neophodne za rad aplikacija, radio-modula, procesora digitalnog signala, mikrofona i zvučnika, različitih tastera, interfejsa i displeja.

Uz razlike u pogledu interfejsa između pojedinih modela, zajedničko za gotovo sve vrste mobilnih telefona je da podržavaju govornu komunikaciju, razmenu tekstualnih poruka I da sadže osnovne aplikacije za organizovanje ličnih podataka (PIM – Personal Information Management), koje uključuju telefonske imenike i kalendare. Konstantnim tehnološkim razvojem, ovi uređaji inkorporiraju sve veći broj novih mogućnosti i tehničkih unapređenja.

Neprestano se povećava kapacitet interne fleš memorije, a integrisani su i čitači memorijskih kartica, čime je omogućeno skladištenje sve veće količine raznovrsnih podataka (red veličina više desetina gigabajta).

Mobilni telefoni postaju spoj više uređaja poput ličnih organizatora (PDA), uređaja za globalno pozicioniranje (GPS), fotoaparata, video kamera i multimedijalnih reproduktora. Različiti bežični interfejsi, od već prevaziđenih infracrvenih (npr. IrDA) do sada aktuelnih Bluetooth-a, NFC-a (Near Field Communication) i WiFi-a, pružaju mogućnost povezivanja telefona, kako međusobnog tako i sa računarima, i razmene velike količine podataka.

Kad je reč o softveru, pametni telefoni (smartphones) su napravili pravu revoluciju omogućivši instaliranje i korišćenje velikog broja različitih aplikacija (repozitorijum za operativni sistem Android sadrži više od 260.000 aplikacija [45], a App Store više od 500.000 aplikacija za iPhone telefone [46]).

Uz mogućnost obavljanja više poslova u isto vreme (multitasking), po funkcionalnosti, mobilni telefoni teže da dostignu klasu klasičnih desktop računara. Standardni softver najrasprostranjenijih operativnih sistema za pametne telefone, kao što su Android, Symbian, iOS, RIM (Research In Motion), Bada i Microsoft [47], nude aplikacije za pregledanje datoteka paketa Microsoft Office i dokumenata u PDF formatu, aplikacije za mape i navigaciju, Internet pretraživače i brojne aplikacije za rad sa najpopularnijim Internet servisima i društvenim mrežama.

Instaliranjem aplikacija za multimedijalnu komunikaciju preko Interneta (kao što su Skype, Viber I slično), telefon se može koristiti za pozivanje ili slanje poruka i bez korišćenja GSM mreže, na mestima gde postoje pristupne tačke za bežični Internet.

Iz navedenog proizilazi da mobilni telefoni imaju raznovrsne mogućnosti kreiranja, preuzimanja i razmene velikog broja različitih datoteka i informacija potrebnih ili interesantnih korisniku, što ih upravo čini vrlo zanimljivim za forenziku i krivični postupak.

5.3.1 Digitalni dokazi na mobilnim telefonima

Neke od informacija koje se mogu dobiti sa mobilnih telefona i koristiti kao dokazi su [17]:

- sačuvane SMS i MMS poruke i poruke elektronske pošte sa podacima o pošiljaocu, odnosno primaocu i temporalnim podacima;

- podaci o podešavanju parametara (podešenost vremenske zone je posebno zanimljiva jer, ukoliko nije sinhronizovana sa zonom na forenzičkom računaru, može da utiče na pogrešno prikazivanje vremena vezanog za metapodatke datoteka);

- sačuvane fotografije, audio i video zapisi (posebno zanimljivi su oni snimljeni samim telefonom);

- sačuvane datoteke sa računara i one kreirane aplikacijama sa telefona;

- datoteke instaliranih aplikacija;

- podaci iz kalendara, telefonskih imenika i drugih PIM aplikacija;

- podešavanja vezana za Internet komunikaciju i podaci dobijeni korišćenjem telefona u ovu svrhu, poput istorije aktivnosti (*History*), omiljenih stranica (*Favorites* ili *Bookmarks*) i samih Internet stranica, odnosno fragmenata kada su u pitanju dinamičke stranice.

Memorijske kartice su formatirane u FAT (*File Allocation Table*) fajl sistemu i najčešće se mogu izvaditi iz telefona, kod nekih modela i bez skidanja poklopca baterije i same baterije, kao i bez gašenja uređaja i na njih mogu da se primene sve raspoložive forenzičke metode i alati karakteristični za računare, odnosno USB memorije, što značajno olakšava akviziciju podataka i analizu.

5.3.2 Potencijalni dokazni materijal na SIM kartici

Iako se većina podataka na aktuelnim modelima mobilnih telefona smešta na internu fleš memoriju uređaja, korisnici se zbog potrebe da menjaju telefone (često da bi prikrili trag i otežali rad organima otkrivanja i gonjenja) odlučuju da određene podatke čuvaju na SIM (Subscriber Identity Module) kartici. Pored informacija o pretplatniku i ključeva za enkripciju neophodnih za komunikaciju u GSM mreži, SIM kartice sadrže i sledeće podatke od značaja za forenziku mobilnih telefona [18]:

- serijski broj kartice i podatke o mobilnom operateru (na primer logo ili naziv) koji su najčešće odštampani na samoj kartici (npr. to nije slučaj kod micro SIM kartica). To su podaci na osnovu kojih se od operatera mogu tražiti informacije važne za dalju istragu, poput podataka o pretplatniku, ukoliko je registrovan (što je najčešći slučaj kada se radi o postpejd korisniku), ali i pretplatnički broj kartice koji je dodeljen tom serijskom broju na osnovu koga se mogu tražiti listinzi komunikacija, PIN ili PUK kodovi i drugi podaci iz registara operatora;

- Location Area Identifier (LAI) uz pomoć koga se može utvrditi (uz asistenciju operatera) oblast u kojoj se korisnik nalazio u vreme kada je uređaj poslednji put radio;

- primljene tekstualne poruke, kojih može da bude 20 do 30.

- postoji i mogućnost ponovnog pristupa određenom broju obrisanih porukajer se prilikom brisanja poruke samo bitovima statusnog bajta dodeljuje vrednost 0, dok sadržaj ostaje netaknut dok ga ne istisne nova poruka. Nakon istiskivanja od strane nove poruke, delovi sadržaja stare poruke ne ostaju čak ni u slack prostoru, jer se on ispunjava heksadecimalnom vrednošću FF;

- listu kontakata (novije verzije kartica mogu da sačuvaju do 250 kontakata);

- listu poslednjih biranih brojeva.

U postupku forenzičke analize mobilnih telefona mora se uzeti u obzir GSM mreža u kojoj se beleže podaci o korisniku, SIM kartici i aktivnostima telefona. GSM mreža sadrži informacije koje se mogu koristiti kao dokazi, posebno podaci o pozivima (CDR – Call Data Record), datotekama mobilnog operatera koje sadrže podatke o svim komunikacijama u mreži [19].

Osim podataka o pretplatniku, servisima koji su mu na raspolaganju i SIM kartici (brojevi MSISDN, IMSI, ICCID, PIN i PUK), iz CDR datoteka se mogu izdvojiti informacije o datumu, vremenu, trajanju i vrsti bilo koje komunikacije, zatim o uređaju u kome se nalazila SIM kartica, kao i identifikacija ćelije preko koje je poziv ostvaren, što može da se iskoristi za lociranje korisnika.

Određeni podaci iz sistema GSM mreže koji se koriste samo radi uspostavljanja i održavanja komunikacije (podaci koji nisu bitni za naplatu, što utiče na njihovo relativno kratko čuvanje), poput podataka u HLR (Home Location Register) bazi podataka, mogu u određenim trenucima biti od koristi. Primera radi, ukoliko korisnik ne isključi telefon već mu se isprazni baterija ili dođe do prekida neke druge vrste, postojaće podatak u kom reonu se telefon nalazio u momentu gašenja, što može biti od važnosti prilikom istraga o nestalim osobama [19].

5.3.3 Digitalna forenzika mobilnih telefona

Forenzika mobilnih telefona predstavlja pribavljanje digitalnih dokaza iz memorija mobilnih uređaja i SIM kartica, uz poštovanje svih načela kriminalistike, u forenzičkim uslovima i uz korišćenje prihvaćenih metoda, a suštinska razlika u odnosu na forenziku računara je upravo u akviziciji.

5.3.4 Metode akvizicije podataka

Postupak akvizicije podređuje se očuvanju integriteta podataka i shodno tome se prilikom njegovog sprovođenja moraju poštovati određeni principi [20]:
- preduzetim radnjama ne smeju se menjati podaci sadržani na mobilnom telefonu ili na mediju za skladištenje (memorijska kartica);

- pristup originalnim podacima mogu imati samo kompetentna lica, sposobna da objasne sve akcije koje preduzimaju;

- svaki korak u radu je neophodno precizno dokumentovati;

- lice koje vodi istragu odgovorno je da obezbedi poštovanje principa u skladu sa važećim zakonima.

U praksi je otežano poštovanje prvog principa jer da bi se podaci prikupili sa mobilnog telefona, on mora da bude aktivan, a uključivanje uređaja ili njegovo povezivanje sa računarom, utiče na promenu određenih podataka. Ukoliko je menjanje podataka neizbežno, treba da bude u što manjoj meri [21].

Bitan segment za prikupljanje digitalnih dokaza sa mobilnih telefona predstavlja i obuka istražnih organa koji prvi reaguju, jer i oni moraju biti upućeni kako da se sačuvaju dokazi pohranjeni u pomenutim uređajima.

Nije dovoljno da se oduzme mobilni telefon u toku hapšenja, već službenik mora odmah da obezbedi da podaci na uređaju ostanu netaknuti. Uhapšeni može da iskoristi pravo na telefonski poziv i kontaktirati svog saradnika, koji pod određenim okolnostima može da izbriše podatke sa daljine. Ako je telefon bio uključen pre, ili u toku istrage, može doći do promene u podacima čim se poveže na mrežu.

Zato se radi ometanja signala uređaja, teži korišćenju "Faradejevog kaveza", koji omogućavada uključen telefon ne može da se poveže na mrežu (korporacija Paraben Corp dizajnirala je svojevrsno forenzičko rešenjeu vidu Faradejeve dokazne torbe, koju koriste istražitelji koji prvi reaguju). Kod oduzetih telefona, preporučuje se i aktiviranje funkcije - "režim letenja", što omogućava punu funkcionalnost uređaja bez mrežne konekcije [48].

Kada se govori oakviziciji podataka sa mobilnih telefona, pre svega se misli na prikupljanje podataka samemorije samog uređaja jer se forenzika memorijskih i SIM karticamože vršiti nezavisno.Razlikujemo dve vrste pristupa akviziciji podataka sa mobilnih telefona [22]:

• akvizicija na logičkom nivou - prikupljanje podataka sa memorije mobilnog telefona korišćenjem sistema datoteka, odnosno operativnog sistema telefona;
• akvizicija na fizičkom nivou - kopiranje celokupne memorije, bit po bit, što omogućava prikupljanje i podataka iz prostora koji nije lociran od strane operativnog sistema,odnosno oporavak obrisanih podataka.

Prema SWGDE[4], nivoi akvizicije podataka iz mobilnih uređaja zavise od zahteva I specifičnosti istrage na koju se odnose. Viši nivoi zahtevaju obimnije ispitivanje i dodatne veštine, a moguće je da ne budu primenljivi u svakoj situaciji i sa svakim uređajem. [16]. Radi se o sledećim nivoima:

1. **Manuelni** – operacije na tastaturi ili ekranu uređaja radi dokumentovanja podataka prisutnih u internoj memoriji telefona.

2. **Logički uz izvlačenje - ekstraciju dela fajl sistema**

3. **Logički uz pristupanje operativnom sistemuuređaja**.

4. **Fizički (Ne - invazivan)** – fizička akvizicija podataka iz telefona bez otvaranja kućišta uređaja.

5. **Fizički (Invazivan)** – fizička akvizicija podataka iz telefona uz njegovo rasklapanje i pristup štampanoj ploči (ili- JTAG)

6. **Chip-Off** – akvizicija I analiza uz uklanjanje memorijskog čipai njegovo očitavanje.

7. **MicroRead** – Akvizicija uz upotebu moćnih mikroskopa koji pružaju fizički uvid u memorijske ćelije.

[4]Scientific Working Group on Digital Evidence

5.3.5 Akvizicija digitalnih dokaza iz mobilnih telefona i alati za akviziciju

Zbog velike raznovrsnosti mobilnih telefona, ne postoji jedinstven forenzički alat za njihovu analizu. Istražitelj mora odrediti koja je vrsta uređaja i da na osnovu toga odabere alat za akviziciju. Nezavisno od vrste alata, potreban je pun pristup uređaju, čak i ako je on zaključan, odnosno zaštićen od neovlaščenog pristupa.

Alati za akviziciju mogu pristupiti uređaju pomoću kablova, IR, BT, a mogu biti integralni, odnosno da je moguća ekstrakcija podataka i iz memorije telefona i sa SIM kartice, ili da se primene posebni alati za SIM kartice, a posebni za memoriju uređaja.

5.3.6 Manuelni pregled mobilnih telefona

Manuelni pregled mobilnih telefona je jednostavan, ali vremenski zahtevan metod akvizicije podataka na logičkom nivou, korišćenjem aplikacija mobilnog telefona, uz pomoć kojih lice koje prikuplja digitalne dokaze ostvaruje uvid u sadržaje, pri čemu podatke upisuje u izveštaj bez ikakve automatizacije procesa. Za prikupljanje dokaza na ovaj način, potrebno je poznavati svaki telefon sa kojim se radi, da bi se broj pogrešnih koraka koji bi vršili promene na telefonu, sveo na minimum. Aplikacije na telefonima ne prikazuju sve podatake značajne za analizu, pa se vrši pretraživanje različitih menija i podmenija. Na primer SMS poruke, do čijih se detalja vezanih za samu komunikaciju, kao što su datum, vreme i pretplatnički broj pošiljaoca, dolazi putem podmenija, jer ekran koji prikazuje sadržaj poruke najčešće prikazuje samo naziv iz telefonskog imenika).Greške se ne smeju dozvoliti, pa se manuelnom pregledu pristupa samo ako se traži određeni konkretan digitalni dokaz na uređaju [17], ili ako ne postoji drugi način da se pristupi mobilnom telefonu i prikupe dokazi. To je karakteristično za pojedine mobilne telefone koje nude sami operateri, a koji često nemaju interfejs za komunikaciju sa uređajem, ali imaju velike kapacitete za skladištenje SMS poruka. Eventualne promene koje mogu nastati (na primer, primanje poziva i SMS poruka) usled potrebe da u toku manuelne akvizicije uređaj bude uključen sprečavaju se korišćenjem Faradejevog kaveza (najčešće u obliku specijalnih kesa koje blokiraju električno polje) i kloniranjem SIM kartica (na praznu karticu snime se ICCID i IMSI brojevi čime se omogućava rad telefona, ali ne i pristup mobilnoj mreži).

5.3.7 Akvizicija putem konekcionih servisa

Akvizicija digitalnih dokaza na logičkom nivou obavlja se i putem konekcionih servisa, posredstvom forenzičkih alata koji koriste protokole za slanje komandi i prijem podataka za komunikaciju sa servisima, uz upotrebu otvorenih protokola [18], kao što su AT Command Set, SyncML ili OBEX koji su već zastareli, ili fabrički protokoli poput Nokia FBUS.

Akvizicija preko konekcionih servisa obavlja se pomoću dve vrste alata. Najčešće se koriste alati samih proizvođača mobilnih telefona, ili nezavisnih programera, koji omogućavaju prikupljanje određenog skupa podataka, a namenjeni su pre svega sinhronizaciji računara i mobilnog telefona ili pravljenju rezervnih kopija, a ne forenzici.

Usled nepažnje pri korišćenju ovakvih alata moguće je narušavanje očuvanosti digitalnih dokaza, a dobijeni podaci su uglavnom u formi neupotrebljivoj za kreiranje izveštaja (česti su bili problemi sa Nokia PC Suite, za različite modele ovog proizvođača, koji SMS poruke prikazuje tabelarno, ali ne dozvoljava kopiranje podataka, niti nudi bilo kakav eksport).

U drugu vrstu forenzičkih alata spadajuMicroSystemation XRY, Logicube CellDEK, Cellebrite Universal Forensics Extraction Device (UFED), Oxygen Phone Manager – Forensic Edition, Paraben Device Seizure I drugi.Navedeni alati koriste iste protokole kao i neforenzički alati proizvođača, ali ne implementiraju komande koje eksplicitno modifikuju sadržaj memorije mobilnog telefona.

Međutim, to ne garantuje da akcije ovih alata neće modifikovati sadržaj telefona, pošto komanda, iako samo zahteva podatke, može da prouzrokuje da operativni sistem promeni upravo neki od zahtevanih podataka [26].

Konekcioni agenti su mali programi (na primer, konekcioni agent forenzičkog alata XRY instaliran na telefonu Nokia N95 zauzima svega 34 kB) koji se smeštaju na ciljni uređaj da bi obezbedili konekciju i razmenu podataka između telefona i forenzičkog alata. Ovakav pristup koristi ''klijent-server'' arhitekturu sa agentom u ulozi servera, bez koga alat ne bi mogao da dođe do podataka iz memorije mobilnog telefona. Pošto agent igra ulogu konekcionog servisa, akvizicija podataka je u suštini slična prethodno opisanoj. Metoda se često koristi kod pametnih telefona, a glavni problem je što, kolikogod njegov softver bio mali, agent mora biti smešten u memoriju, čime se njen sadržaj menja.

5.3.8 Direktan pristup memoriji

Direktan pristup memoriji mobilnog telefona je najusklađeniji sa forenzičkim principima, ali predstavlja i najzahtevniju metodu akvizicije podataka [18]. Primenom ove metode, digitalni dokazi se prikupljaju na fizičkom nivou i omogućavaju izradu forenzičke kopije celokupne memorije mobilnog telefona, bez obzira na to koliki memorijski prostor je zauzet.

Direktan pristup memoriji omogućava oporavak obrisanih ili delimično istisnutih unosa, kao i zaobilaženje bezbednosnih mera koje bi inače onemogućile pristup podacima na logičkom nivou i pred kojima su ostale metode akvizicije nemoćne bez intervencija čiji je uticaj na očuvanost digitalnih dokaza neizvestan. Još jedna prednost direktnog pristupa je njegova nezavisnost od toga da li će operativni sistem mobilnog telefona obezbediti ispravne rezultate akvizicije, što nije slučaj sa ostalim metodama.

Mogu se primeniti tri metode direktnog pristupa:

- uklanjanje memorijskog čipa sa štampane ploče mobilnog telefona i čitanje njegovog sadržaja (ovo je za krivični postupak možda isuviše rizična procedura, jer čip može lako da bude uništen temperaturom koja se koristi za njegovo odvajanje od ploče, a samim tim i potencijalni digitalni dokazi);

- upotreba porta za JTAG test (*Joint Test Action Group*, standardizovana procedura za testiranje interkonekcija na štampanoj ploči i podblokova unutar integrisanog kola) radi pravljenja kompletne forenzičke kopije sadržaja promenljive i nepromenljive memorije telefona. Nedostatak je što je na novijim modelima sve teže naći port, odnosno doći do njega, pošto ga proizvođači često kriju;
- upotreba alata za flešovanje (flasher tools) namenjenih za programiranje memorije uređaja (EEPROM ili fleš memorije), ili za otkrivanje grešaka i dijagnostiku, za šta ih proizvođači često koriste. Problem kod primene ove vrste alata je što u određenim slučajevima mogu da pročitaju samo deo memorije, a uz to svaki proizvođač ima svoj, drugačiji, interfejs za pristup, pa je nemoguće postići sveobuhvatnu primenljivost.

Primena bilo koje od tri navedene metode direktnog pristupa zahteva visok nivo tehničke obučenosti i znanja, kao i laboratorijske uslove za rad. Najveći nedostatak u odnosu na ostale metode je što se posao ne završava akvizicijom jer je neophodno analizirati sirove podatke i iz njih izdvojiti smislene i upotrebljive informacije, odnosno dokaze, koji će moći da budu prezentovani u razumljivoj formi.

6. STUDIJA SLUČAJA

6.1 Identifikacija neovlašćene upotrebe USB memorija i oporavak izbrisanih podataka sa USB memorije

6.1.1 Scenario

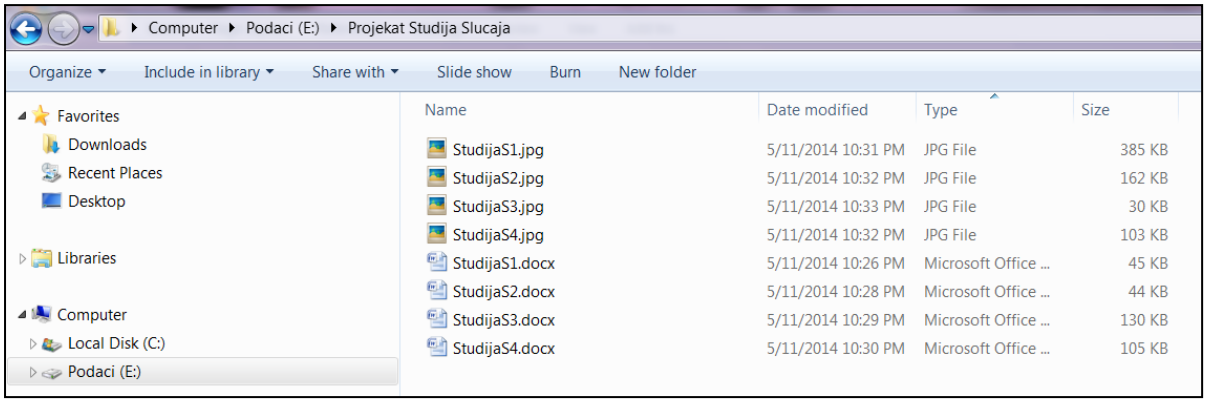
Kompanija ''ABD'' angažovana je na razvoju savremenog naoružanja za potrebe Vojske, a pomenuti projekat je klasifikovan stepenom tajnosti - ''Državna tajna''. Početkom 2014.godine, sa jednim od tehnoloških stručnjaka na tom projektu stupio je u kontakt strani državljanin, član rukovodstva međunarodne terorističke organizacije ''TBD''.

Dana 24.05.2014.godine, prilikom primopredaje dokumentacije o navedenom projektu, uhašeni su i tehnološki stručnjak iz firme ''ABD'' i član terorističke organizacije ''TBD''. Tom prilikom, uz zapisnik o privremenom oduzimanju predmeta, od člana terorističke organizacije, oduzet je USB disk, koji mu je neposredno pre toga predao zaposleni u kompaniji ''ABD''. U skladu sa nalogom nadležnog tužilaštva, organi istrage raspolažu dokaznim materijalom da je zaposleni u kompaniji ''ABD'' predmetni USB disk predao članu terorističke organizacije.

Po nalogu nadležnog tužilaštva, osim drugih istražnih radnji, izvršena je digitalna forenzička analiza predmetnog USB diska i službenog računara firme ''ABD'', radi ustanovljavanja činjenica – dokaza o postojanju krivičnog dela špijunaža.

6.1.2 Priprema USB memorije i igrajućeg službenog računara

Na personalnom računaru sa Windows 7 OS - igrajući računar firme ABD, kreiran je folder sa nazivom **''Projekat Studija Slucaja''** i u njemu 8 dokumenata (četiri *Microsoftword* dokumenta i četiri *JPG* fotografija), koji će biti predmet krađe. Pregled sadžaja navedenog foldera dat je na Slici 10.



Slika 10. Sadržaj foldera ''Projekat Studija Slucaja'' na ''računaru firme ABD''

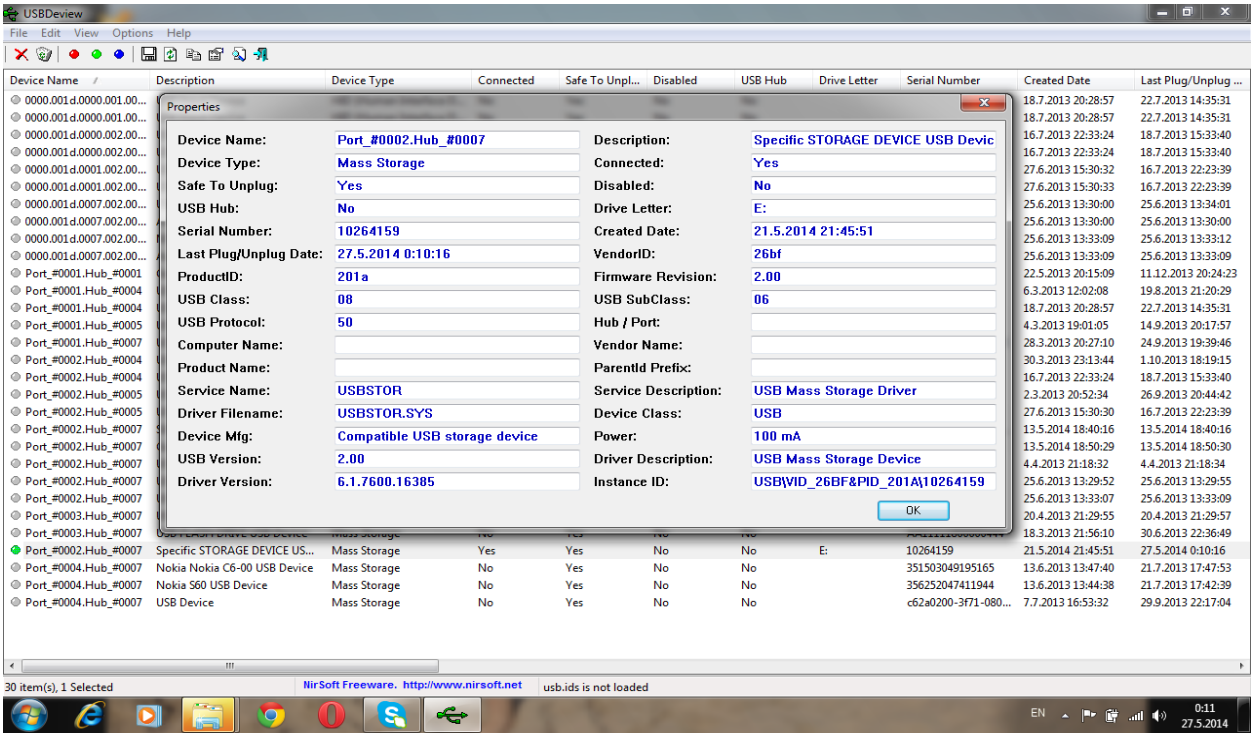
Na drugom nezavisnom računaru, izvršeno je formatiranje igrajućeg USB diska, FAT fajl sistemom, koji je nakon toga pomoću programa ''Ccleaner'' wipe-ovan.

Potom je na igrajući službeni računar povezan igrajući USB disk i nasnimljeni su fajlovi ***StudijaS1.docx*** i ***StudijaS2.docx***, kao i **StudijaS1.jpg** i **StudijaS2.jpg**, koji su nakon toga, na nezavisnom računaru izbrisani. Nakon toga, na igrajući računar ponovo je povezan igrajući USB i nasnimljeni su preostali fajlovi iz navedenog foldera **''Projekat Studija Slucaja''**.

6.1.3 Profilisanje – potpuna identifikacija USB memorije

Profilisanje privremeno oduzetog igrajućeg USB diska, izvršeno je na zasebnom računaru, sa prethodno softverski blokiranjem upisa za sve USB uređaje (preko Window registra: HKLM\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies, tako što je vrednost WriteProtect podešena na 00000001, a to je prema dostupnoj literaturi, ekvivalentno upotrebi fizičkih blokatora pisanja).

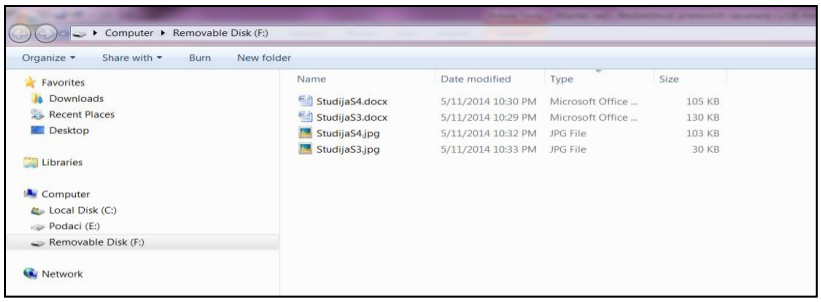
Korišćenjem softverskog alata USBDeview, kompanije NirSoft, koji sortirano prikazuje sve informacije o USB uređajima iz baze Windows registra, prikupljeni su podaci od značaja za ustanovljavanje da li je igrajući USB disk korišćen na računaru firme ''ABD'' radi eventualne proliferacije tajnih podataka. Ti podaci, prikazani su na Slici 11.



Slika 11. Interfejs programa USBDeview, sa podacima o tretiranom USB disku

6.1.4 Oporavak izbrisanih podataka sa USB memorije

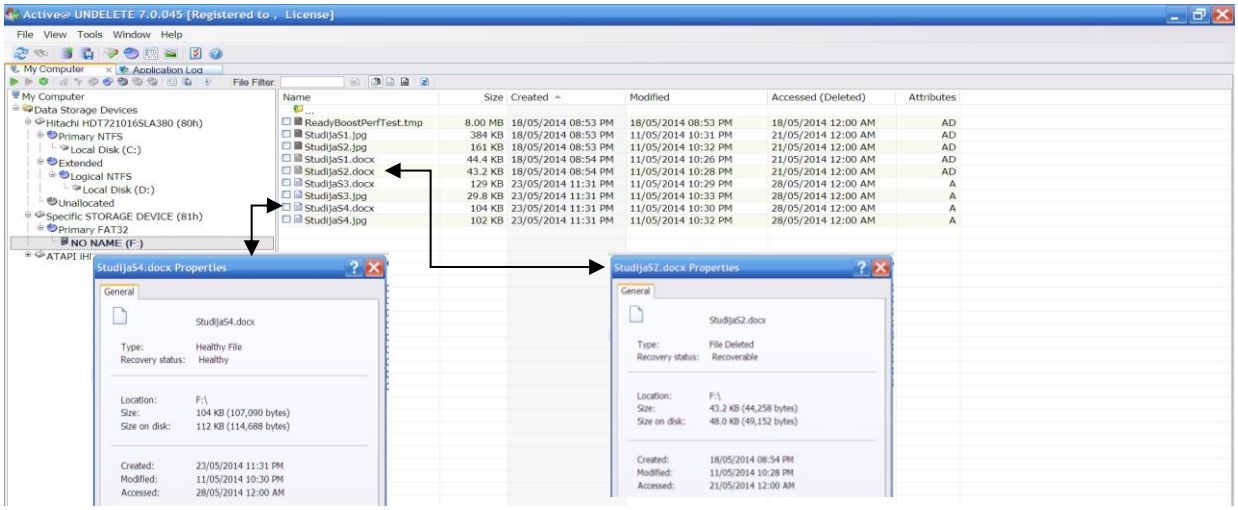
Na zasebnom računaru, sa prethodno softverski blokiranjem upisa za sve USB uređaje, najpre je ostvaren manuelni uvid u sadržaj. Na Slici 12, prikazani su fajlovi koji su se nalazili na igrajućem USB disku, u trenutku primopredaje, čime je delimično potvrđena početna hipoteza, da je zaposleni u firmi ‘’ABD’’ pokušao da oda tajne podatke članu terorističke organizacije.



Slika 12. Sadržaj igrajućeg USB diska, nakon privremenog oduzimanja

Na osnovu indicija, da je inkriminišuća radnja rađena u dužem periodu, moguće uz korišćenje istog USB diska, pristupilo se oporavku eventualno izbrisanih datoteka. U tu svrhu, korišćen je softver ‘’Active@UNDELETE’’, namenjen oporavku izbrisanih datoteka i povraćaju izbrisanih particija, koji oporavlja izgubljene fajlove u NTFS, FAT, FAT32, exFAT, HFS+, Ext2/Ext3/Ext4 i UFS fajl sistemima.

Na Slici 13 prikazan je rezultat skeniranja igrajuće USB memorije, navedenim alatom. Iz priloženog se vidi da je na USB disku osim fajlova koji su ustanovljeni manuelnim pregledom, bilo i drugih fajlova, koji su izbrisani.



Slika 13. Rezultat skeniranja USB diska alatom Active@UNDELETE

Daljom analizom, koja nije predmet ovog rada, moguće je poređenje fajlova sa USB diska (oporavljenih i postojećih) sa fajlovima koji su na računaru firme ''ABD'' (dato na Slici 10).

6.1.5 Identifikacija neovlašćene upotrebe USB memorije

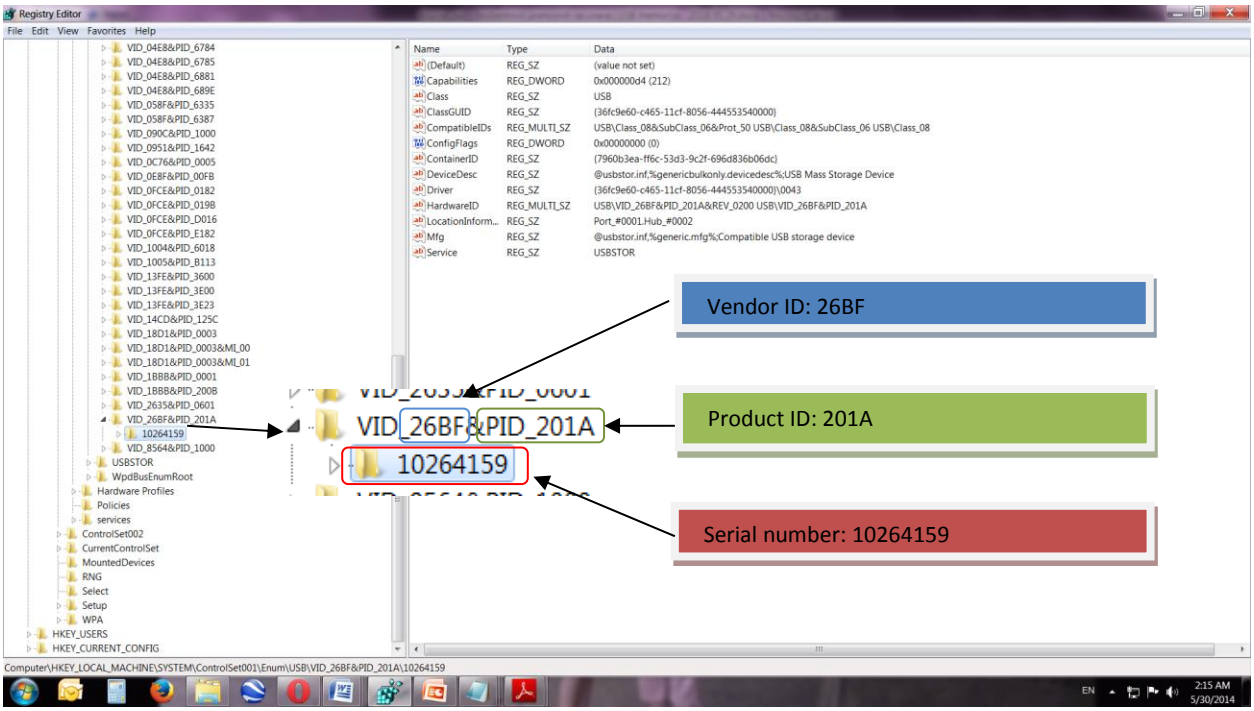
Daljim radom na slučaju, a po važećim nalozima suda, pristupa se forenzikoj analizi računara firme ''ABD''. U ovom delu biće obrađeno angažovanje na identifikaciji neovlašćene upotrebe igrajuće USB memorije na pomenutom računaru. Do identifikacionih podataka o toj memoriji, kao što je opisano, došlo se korišćenjem alata USBDeview.

Eventualnu neovlašćenu upotrebu USB memorije na predmetnom računaru ustanovićemo analizom Windows registara, zato što prilikom povezivanja bilo kog uređaja sa računarom preko Universal Serial Bus (USB), izvrši se pribavljanje drajvera, a informacije o uređaju ubeleže se u više registra.

Jedan od ključeva tih registra je **HKLM\SYSTEM\CurrentControlSet\Enum\USB**. Podključevi u ovom ključu su serijski brojevi uređaja koji su priključivani na sistem. Serijski brojevi uređaja su jedinstvene vrednosti dodeljene od strane proizvođača, tako da konkretan USB uređaj može da se identifikuje kako bi se utvrdilo da li je ili nije bio povezan sa nekim konkretnim Windows sistemom.

Treba imati na umu da nema svaki USB uređaj serijski broj, a to su oni kod kojih drugi i jedanaesti karakter ID uređaja imaju simbol "&". U tom slučaju, sistem dodeljuje uređaju jednistveni identifikacioni broj.

Serijski broj igrajućeg USB uređaja je **10264159**. Preteći tu vrednost u ovom ključu, utvrdili smo da je tretirani USB disk bio povezivan na predmetni računar. Na Slici 14 dat je sadržaj ključa USB, sa označenim igrajućim uređajem.



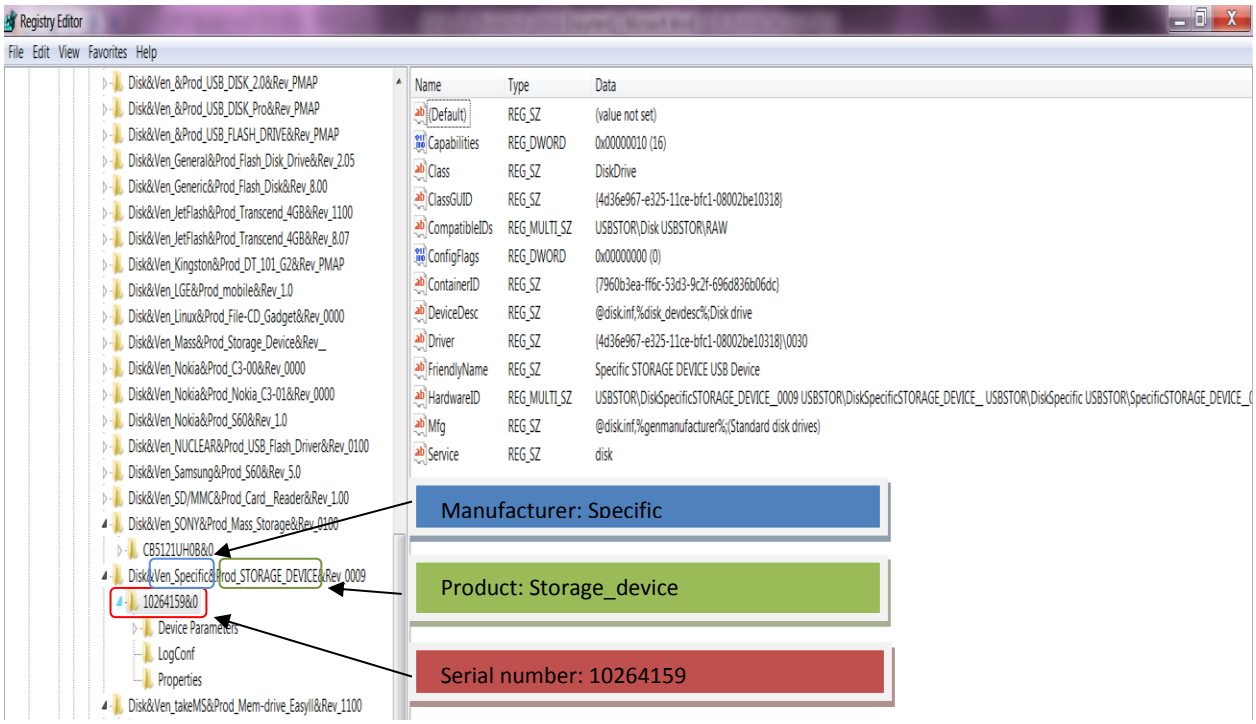
Slika 14. Ključ HKLM\SYSTEM\CurrentControlSet\Enum\USB

Izvođenjem ovog ključa u tekstualnu datoteku, dobijaju se sledeći podaci:

Key Name:
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USB**VID_26BF&PID_201A**
Last Write Time: 5/22/2014 - 1:26 PM
Key Name:
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USB\VID_26BF&PID_201A**10264159**
Last Write Time: 5/23/2014 - 11:30 PM

Pri tome, "**VID_26BF&PID_201A**" je identifikator klase (Vendor ID = 26BF, ProductID = 201A). Svaka od stavki u ovom ključu je specifična za određenu marku i model USB uređaja. Vrednost **"Last Write Time: 5/22/2014 - 1:26 PM"** predstavlja vreme kada je uređaj prvi put bio priključen na sistem, nakon rebutovanja. Ovo vreme se ne menja kada se isti uređaj više puta povezuje i isključuje. Druga vrednost **"Last Write Time: 5/23/2014 - 11:30 PM"** predstavlja vreme u kome je poslednji put isti uređaj bio povezan na konkretni sistem.

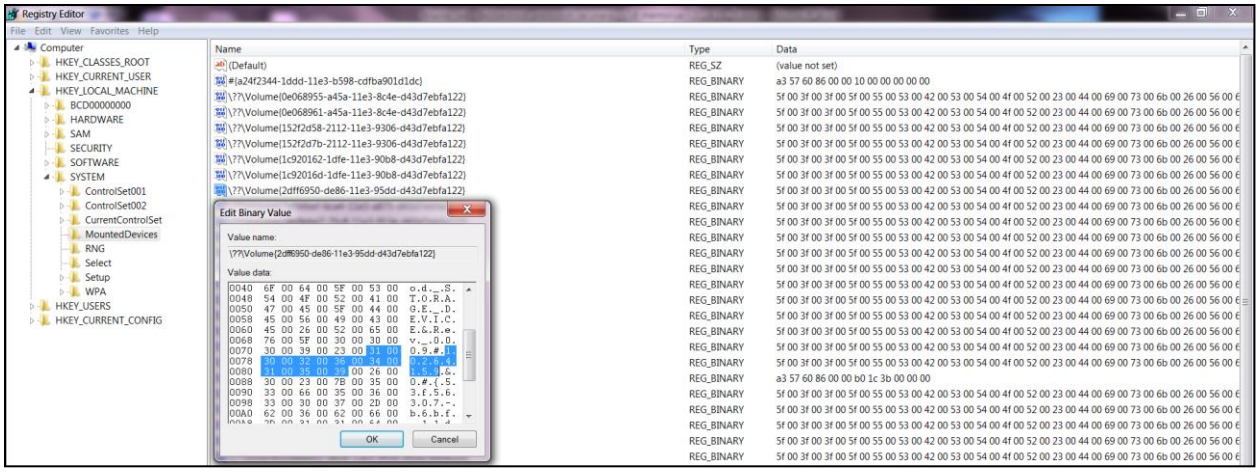
Sledeći ključ koji će nam pomoći da verodostojno ustanovimo neovlašćenu upotrebu konkretnog USB diska je **HKLM\SYSTEM\ControlSet00x\Enum\USBSTOR**. Ovaj ključ skladišti ID vrednosti (identifikacione podatke) svih USB proizvoda i uređaja koji su ikada bili priključeni na sistem. Za svaki uređaj naveden je Device ID, koji je takođe serijski broj. Na Slici 15 dat je sadržaj ključa UBSTOR, sa označenim igrajućim uređajem.



Slika 15. Ključ HKLM\SYSTEM\ControlSet00x\Enum\USBSTOR

Izvoženjem ovog ključa u tekstualnu datoteku, dobijaju se sledeći podaci:
Key Name:
*HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven_**Specific**&Prod_**STORAGE_DEVICE**&Rev_0009*
Last Write Time:** 5/22/2014 - 1:26 PM – **Kao i kod USB ključa, može da predstavlja neko vreme, u koje je uređaj bio povezan, odnosno prvo povezivanje nakon rebutovanja sistema.
Key Name:
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven_Specific&Prod_STORAGE_DEVICE&Rev_0009
Last Write Time:** 5/23/2014 - 11:30 PM – **kao i kod USB ključa, ovo je vreme u koje je igrajući uređaj poslednji put bio povezan na sistem.
Key Name:
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven_Specific&Prod_STORAGE_DEVICE&Rev_0009\10264159&0\Device Parameters\Partmgr
Last Write Time:** 5/18/2014 - 8:52 PM – **Predstavlja vreme u koje je uređaj prvi put povezan na sistem.

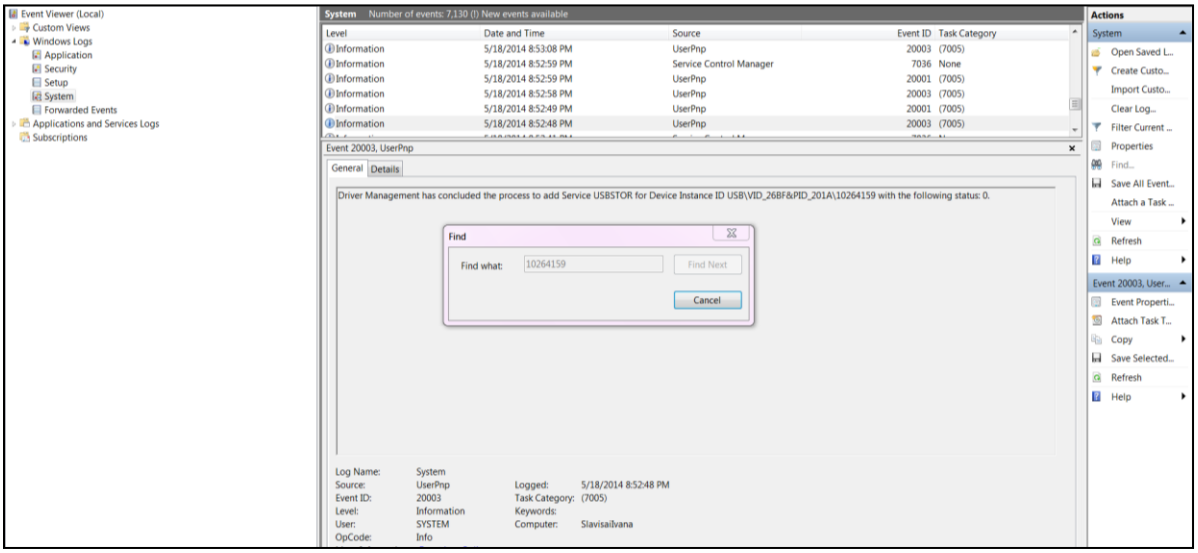
U ključu: **HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices**, kao što je prikazano na Slici 16, pronalazimo vrednost ''Volume GUID''.



Slika 16. Ključ HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices

Eksportovanjem u tekstualni fajl, dobijamo da je Volume GUID za igrajući USB disk: **\??\Volume{2dff6950-de86-11e3-95dd-d43d7ebfa122}**. Na osnovu ove vrednosti u ključu : HKEY_USERS**S-1-5-21-2320401350-1837478337-3990578936-1000** \Software \Microsoft \Windows\CurrentVersion\Explorer\MountPoints2\ {2dff6950 -de86 -11e3-95dd-d43d7ebfa122}, identifikujemo korisnika koji je bio ulogovan na sistem u vreme kada je igrajući USB uređaj poslednji put bio povezan na sistem (**''Last Write Time: 5/23/2014 - 11:30 PM''**).

Osim kroz registre, dodatne informacije o igrajućem USB disku pronašli smo u Event Logu (dnevniku događaja). Korišćenjem poznatog nam serijskog broja, u Event Viewer-u, došli smo do podataka da je ključ HKEY_LOCAL_MACHINE\SYSTEM \ControlSet001\Enum\USB\VID_26BF&PID_201A kreiran od strane korisnika ''SYSTEM'' u vreme ''5/18/2014 8:52:48 PM'', što se poklapa sa vremenom koje smo pronašli u ključu USBSTOR. Navedeno je prikazano na Slici 17.



Slika 17: Prikaz događaja u Event logu, povezanog sa igrajućim USB diskom

ZAKLJUČAK

Prenosni računari i USB memorije, pod uticajem tržišta, sve se više unapređuju po pitanju kapaciteta za skladištenje podataka, brzine manipulacije tim podacima, načinu njihove zaštite, broju funkcija koje objedinjavaju idr. Kao takvi sve više su zastupljeni u službenoj i ličnoj – privatnoj upotrebi, ali postaju interesantniji i sa aspekta primene u nedozvoljenim - kriminalnim radnjama.

Kada su zloupotrebe u pitanju, USB memorije i prenosni računari sve češće se koriste za krađu podataka (takozvano curenje informacija), a pogodne su i za širenje malicioznih programa. Pomenute prenosne uređaje, sa pohranjenim korporacijskim podacima, teško je fizički pratiti, jer mogu da se ponesu sakriveni u odeći, torbicama, slično.

Sve navedeno ukazuje da osim benefita, omasovljavanje njihove upotrebe povećava i bezbednosne rizike. Bez adekvatnih operativnih i logičkih kontrola, masovnost njihove upotrebe može predstavljati ozbiljnu pretnju po poverljivost, integritet i dostupnost informacija (CIA). Takođe, kao nepresušni izvor digitalnih dokaza, predstavljaju izazov za forenzičke stručnjake, zbog povećane potrebe za razvojem i usavršavanjem posebnih forenzičkih procedura, alata i kadrova koji obavljaju digitalnu forenzičku analizu pomenutih uređaja.

Bezbednosne mere, kada je reč o upotrebi USB memorija i prenosnih računara, faktički se mogu podeliti na mere kojima se kontroliše – ograničava pristup korporacijskim podacima USB memorijama i prenosnim računarima (upotreba isključivo službenih prenosnih medija, evidencija korisnika, čuvanje prenosnih medija kada nisu u upotrebi) i mere kojima se štite podaci koji su na ovim uređajima (upotreba jakih lozinki, kriptovanje podataka, vajpovanje slobodnog prostora (WIPE FREE SPACE), fizičko čuvanje – sefovi, zaštitne kutije i sl.)).

U odnosu gotovo svakodnevne inovacije prenosnih računara i USB memorija, broj alata za njihovu digitalnu forenzičku analizu je znatno odgraničen. Ne samo da postoje manje specijalizovani alati i kompleti alata u odnosu na forenzičke alate za digitalnu analizu prenosnih računara, već je sužen i broj vrsta - modela uređaja nad kojima oni funkcionišu, a u pojedinim slučajevima se odnosi samo na najpopularnije uređaje. Takođe, u odnosu na broj forenzičkih alata koji obavljaju samo jednu funkciju, manji je broj alata koji podržavaju pun spektar akvizicije, ispitivanja i izveštavanja.

Na osnovu navedenog može se zaključiti da ne postoji idealan metod akvizicije podataka iz prenosnih računara i USB memorija, već se radi o kompromisu između efektivnosti i efikasnosti, odnosno na osnovu operativnih podataka određuje se prioritet i bira odgovarajuća metoda za svaki pojedinačni slučaj. Savremeni forenzički alati objedinjuju više metoda i pristupa, uz nastojanje da obavljaju što manje izmena na prenosnim uređajima, a da prikupe što više digitalnih dokaza.

U cilju dokazivanja da svojim akcijama nije narušilo očuvanost digitalnih dokaza, lice koje vrši akviziciju mora da u potpunosti ispoštuje proceduru i dokumentuje sve aktivnosti u radu sa prenosnim računarom, a da interakciju sa uređajem svede na minimum. Što je više interakcija, to je komplikovanije dokazati da akcije nisu kompromitovale digitalne dokaze.

Ukoliko je prenosni računar, ili USB disk prilikom privremenog oduzimanja stavljen u omot i zapečaćen (što je u širem smislu i propisano članom 84. ZKP-a), a branilac ili okrivljeni prisustvuje uklanjanju omota i izvođenju akvizicije, ostvareni su svi uslovi da se tako prikupljeni podaci mogu koristiti kao digitalni dokazi, odnosno otklonjene su sumnje u eventualno narušavanje dokaznog materijala. Ovde svakako treba spomenuti i tzv. lanac nadzora (chain of custody), koji podrazumeva hronološko dokumentovanje prikupljanja, kontrole, transfera i analize privremeno oduzetih predmeta, ali samo spomenuti, jer ga kao takvog naš zakon još uvek ne prepoznaje.

LITERATURA

1. Assessing the Security of Hardware-Based vs. Software-Based Encryption on USB Flash Drives, White paper, jun 2008, 80-11-01583, Revision 1.0

2. Computer forensics, investigating Wireless Networks and Devices, EC Counsil Press,2010.

3. Gojko Grubor, Milan Milosavljević, *Osnove zaštite informacija: Metodološko - tehnološke osnove*, Univerzitet SINGIDUNUM, Beograd, 2010.godine.

4. Guidelines on PDA Forensics, Recommendations of the National Institute of Standards and Technology, Gaithersburg, MD 20899-8930, November 2004, Wayne Jansen, Rick Ayers,

5. Jelena Surčulija, *Evropski pravni orvir za elektronske komunikacije — osnov za izgradnju informacionog društva u Srbiji*, Beograd, 2004.

6. Stevan Lilić, *Pravo, informatička tehnologija i zaštita podataka,* Anali pravnog fakulteta u Beogradu br. 2-3, 1989.

7. Ted Fair, Michael Nordfelt i Sandy Ring, Cyber Spying Tracking Your Family's (Sometimes) Secret Online Lives, Syngress Publishing, 2005.

8. Wayne Jansen, Rick Ayers, Guidelines on Cell Phone Forensics, National Institute of Standards and Technology special publication 800-101, 2007.

9. Priručnik za istragu krivičnih dela u oblasti visokotehnološkog kriminala, Savet Evrope, Strazbur, 2008.

10. Milosavljević Milan, Gojko Grubor, Digitalna forenzika, Univerzitet Singidunum, Beograd, 2008.godina.

11. A hardware-based memory acquisition procedure for digital investigations, Published in Issue 1(1), ISSN 1742-2876, February 2004.

12. Icove D., Segar K., VonStorch W., *Computer Crime, A Crimefighter's Handbook,*O'Reilly & Associates, 2004.

13. Krishnun Sansurooah, A forensics overview and analysis of USB flash memory devices, originally published in the Proceedings of the 7th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, December 3rd 2009.

14. Shafik G. Punja & Richard P. Mislan, Mobile Device Analysis, Small scale digital device forensics journal, VOL. 2, NO. 1, JUNE 2008 ISSN# 1941-6164 1.

15.Salvatore Fiorillo, Theory and practice of flash memory mobile forensics, Originally published in the Proceedings of the 7th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia,December 3rd 2009.

16. State of the art in SSD forensics - Why SSD Drives Destroy Court Evidence, and What Can Be Done About It.pdf, 2012.

17. Jansen W., Ayers R., Guidelines on Cell Phone Forensics, National Institute of Standards and Technology, U.S. Department of Commerce, 2007.

18. Willassen S., Forensic analysis of mobile phone internal memory, Norwegian University of Science and Technology, 2005.

19. Willassen S., "Forensics and the GSM mobile telephone system", International Journal of Digital Evidence, 2003.

20. Ayers, R., Jansen, W., Cilleros, N., Daniellou, R., Cell phone forensic tools: An overview and analyisis, National Institute of Standards and Technology, Gaithersburg, Maryland 2005.

21. Carrier, B., Open source digital forensic tools – the legal argument, Research report, At Stake, 2002.

22. Keonwoo Kim, Dowon Hong, Kyoil Chung, Jae-Cheol Ryou, Data Acquisition from Cell Phone using Logical Approach, Proceedings of World Academy of Science, Engineering and Technology, 2007.

23. SWGDE - Best Practices for Mobile Phone Forensics Version: 2.0, 11.02.2013.

24.Casey, E., Digital evidence and computer crime: forensic science, computers, and the Internet", 2nd edition, Academic Press, London, 2004.

25.Mokhonoana P., Olivier M., Acquisition of a Symbian smart phone's content with an on-phone forensic tool, Proceedings of the Southern African Telecommunication Networks and Applications Conference 2007 (SATNAC 2007), Sugar Beach Resort, Mauritius, September 2007.

26. McCarthy, P., Forensic analysis of mobile phones, Master's thesis, University of South Australia, 2005.

Internet izvori:

27. http://blog.lumension.com/6358/dealing-with-todays-information-systems-complexity/, Kevin Beaver, Pristupljeno, 14.01.2013.

28. http://en.wikipedia.org/wiki/Secure_USB_drive, Pristupljeno: 08/11/2012

29. http://go.eset.com/us/resources/threat-trends/ Global_Threat_Trends_ December_2011.pdf, Pristupljeno: 04/10/2012

30. http://sr.wikipedia.org/wiki/USB_memorija, Pristupljeno: 18/10/2012

31. http://ucenickiklub.wordpress.com/2011/11/08/prenosni-racunari/,Pristupljeno: 28/09/2012

32. http://windows.microsoft.com/sr-Latn-CS/windows-vista/Introduction-to-computers, Pristupljeno: 8/10/2012

33. http://www.sciencedirect.com/science/article/pii/S0140673605674843, Pristupljeno: 5/07/2012

34. http://www.wisegeek.com/what-is-a-usb-mass-storage-device.htm, Pristupljeno: 08/04/2013

35. http://en.wikipedia.org/wiki/Mobile_device_forensics#cite_note-casey,Pristupljeno 09.03.2014.godine.

36. http://www.itvestak.org.rs/ziteh_04/radovi/ziteh-19, Pristupljeno 15.03.2014.godine.

37. http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2000/- Digital Evidence: Standards and Principles, Scientific Working Group on Digital Evidence (SWGDE) International Organization on Digital Evidence (IOCE), October 1999, pristupljeno 17.03.2014.godine.

38. http://www.datasolutions.rs/srp/kompjuterska-forenzika/kompjuterska-forenzika-digitalni-dokazi.html, Pristupljeno 16.03.2014.godine.

39. www.micron.com/-/Documents/Products/Technical%20Note/NAND%20Flash/ tn2919_101- Technical Note NAND Flash 101: An Introduction to NAND Flash and How to Design It In to Your Next Product, pristupljeno 10.04.2014.godine.

40. http://articles.forensicfocus.com/2011/07/19/flash-drives-and-acquisition, FILED UNDER EVIDENCE ACQUISITION, FLASH DRIVES, First published June 2010, pristupljeno 24.03.2014.godine.

41. http://www.netplanet.rs/index.php/learning/hardware/46-ssd-vs-sata-3-sta-je-ssd-i-koje-su-prednosti, datum kreiranja 06 mart 2013.godine, pristupljeno 19.03.2014.godine.

42. www.elitesecuriti.org/t433953-0, Pristupljeno 15.03.2014.godine.

43. http://en.wikipedia.org/wiki/TRIM, Pristupljeno 19.03.2014.ghodine.

44. http://hetmanrecovery.com/recovery_news/vosstanovlenie-informacii-s-ssd-nakopit, -Recovering Information from SSD Drives: Myths and Reality, Pristupljeno 24.03.2014.godine.

45. http://www.appbrain.com/stats/number-of-android-apps, Pristupljeno 17.03.2014.godine.

46. http://en.wikipedia/wiki/App_Store_(iOS)#Number_of_launched_applications, Pristupljeno 17.03.2014.godine.

47. http://www.gartner.com/it/page.jsp?id=1764714, Pristupljeno 17.03.2014.godine.

48. http://www.officer.com/article/10248785/the-other-side-of-mobile-forensics, - The other side of mobile forensics, CHRISTA MILLER, created: July 1, 2008, Pristupljeno 14.03.2014.godine.