



UNIVERZITET SINGIDUNUM

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

HDD, SSD uređaji i Digitalna Forenzika

- Master rad -

Mentor:
Prof. dr. Mladen Veinović

Student:
Miloš Trifunović
Br. indeksa: 410584/2012



Singidunum

Beograd, 2015

HDD, SSD uređaji i digitalna forenzika

Sažetak: Ovaj projektni zadatak razmatraće HDD i SSD tehnologiju. Pre svega razvoj ovih uređaja njihove funkcionalnosti, arhitekturu i način skladištenja podataka njihovu prisutnost na tržištu kao i digitalnu forenziku njenu primenu, svojstva i njene mogućnosti upotrebe nad SSD uređajima.

Ključne reči: HDD, SSD, SATA, Upis, Čitanje, Pokretna ručica, Sektor, Traka, Ploča, Blok podataka, TRIM, Garbage Collection, HDD, FTL, Image, NTFS.

HDD, SSD devices and digital forensics

Abstract: This project assignment will review the HDD and SSD technology. First of all development of these devices to their functionality, architecture, way of storing data, market presence as well as digital forensics its application properties and its possibilities of use of SSD devices.

Keywords: HDD, SSD, SATA, Registration, Read, Moving arm, Sector, Tape, Plate, Block of data, TRIM, Garbage Collection, HDD, FTL, Image, NTFS.

SADRŽAJ

1. Metodologija	1
1.1 Uvodne napomene	1
1.2 Predmet istraživanja	1
1.3 Hipoteza	1
1.4 Ciljevi istraživanja	1
1.5 Naučne metode	1
1. Uvod	2
2. Hard diskovi razvoj i arhitektura	3
2.1 Glavne komponente Hdd-a	8
3. Upis podataka	9
3.1 Greške u sektorima	10
4. Tehničke karakteristike	10
4.1 Vreme i brzina pristupa	10
4.2 Konektori prenosa podataka	12
4.3 Proizvođači i udeo tržišta	15
5. SSD (Solid State Drive)	16
5.1 SSD razvoj i arhitektura	16
5.2 Poređenje SSD-a i HDD-a	19
5.3 Poređenje sa memorijskim karticama	21
5.4 Proizvođači i udeo tržišta	22
6. Hibridni hard diskovi	23
7. SSD i HDD test	25
8. Digitalna forenzika	32
8.1 Digitalni dokaz	33
8.2 Forenzika mobilnih uređaja	34
8.3 Računarska forenzika	35

8.4 Mrežna forenzika	36
8.5 Forenzika baze podataka.....	38
8.6 Forenzički alati	39
9. Forenzička analiza SSD-a ?.....	42
9.1 Brisanje nije moguće.....	42
9.2 Memorijski blokovi.....	43
9.3 Trim metoda	45
10. Zaključak.....	47
11. Literatura.....	48
12. Spisak slika:	50
13. Tabele i dijagrami :	51

1. Metodologija

1.1 Uvodne napomene

U ovom radu predstavljeni su uređaji za skladištenje podataka u dve različite tehnologije prisutne danas na tržištu SSD i HDD uređaje. Njihova poređenja, razvoj i način na koji funkcionišu bitni su za razumevanje samog funkcionisanja čitanja i upisa podataka. Pored navedenog obuhvaćena je tema digitalne forenzike kao i forenzike SSD-a.

1.2 Predmet istraživanja

Predmet ovog istraživanja jeste da se utvrde prednosti ali i mane ove dve tehnologije kao i mogućnost digitalne forenzike uređaja.

1.3 Hipoteza

Opšta hipoteza: Podaci se trajno skladište na HDD i SSD uređaje. Način skladištenja podataka nije isti baš zbog različitosti tehnologija koje su primenjene.

Posebna/radna hipoteza: Razvoj HDD i SSD tehnologije ima različit sistem upisa podataka jedan je potpuno elektronski dok je drugi usklađen sa mehaničkim komponentama. Upravo zbog ovih različitosti imamo i drugačije rezultate u forenzičkim radnjama.

1.4 Ciljevi istraživanja

Naučni cilj: Istraživanje i definisanje koja tehnologija ima veću budućnost tj. da li će obe tehnologije preživeti ili evoluirati zajedno kao i mogućnosti forenzičke analize SSD-a.

Društveni ciljevi: Upoznavanje krajnjih korisnika sa uređajima, mogućnošću povraćaja podataka kao i tendencijama u daljem razvoju istih.

1.5 Naučne metode

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

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

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

1. Uvod

Potreba za smeštanjem podataka u permanentnu memoriju pojavila se sa samom pojavom računara. Danas se podaci čuvaju u nekoliko različitih tehnologija koje će biti predstavljene u ovom radu.

Počinjemo od **HDD (Hard Disk Drive)** tehnologije koja je razvijena sredinom XX veka, isto tako **SSD (Solid State Drive)** tehnologija je otkrivena u približnom vremenskom periodu kao i HDD samo što nije momentalno dobila na značaju. Danas imamo priliku da prisustvujemo borbi ova dva različita koncepta skladištenja podataka.

Hard disk („Tvrđi disk“) predstavlja uređaj za pisanje, čitanje i skladištenje podataka. Za skladištenje podataka HDD koristi svoje rotirajuće diskove i glavu koja vrši upis određenih podataka. Pored HDD-a u radu će se govoriti i o SSD-u uređaju koji je takođe namenjen za skladištenje podataka. Kako mu i samo ime govori SSD uređaji nemaju mehanički pokretne delove i uz pomoć memorijskih „blokova“ čuvaju podatke.

U nastavku opisaćemo na koji to način ovi uređaji funkcionišu u našim računarima kao i njihove tehničke karakteristike, prisutnost na tržištu, razvoj i komparaciju dve tehnologije kao i njihovu koaliciju i mogućnosti ujedinjenja ove dve tehnologije.

Pored predstavljanja ovih skladišnih komponenti upoznaćemo se sa digitalnom forenzikom, šta ona predstavlja, gde je prisutna kao i njene mogućnosti analiziranja podataka sa SSD uređaja.

2. Hard diskovi razvoj i arhitektura

Prvi Hard disk je predstavljen od strane IBM-a 1956. godine model 350 RAMAC i on je imao mogućnost skladištenja podataka reda 5 miliona šesto bitnih karaktera ili 3,75 mb za koje je koristio skladište od 50 diskova i bio je fizičke veličine kao današnja dva frižidera.

Sledeći HDD je isto IBM-ov proizvod i suštinski napredak u odnosu na svog predhodnika, razlika je bila u pokretnoj ručici i magnetnoj glavi koja je čitala i unosila podatke. Pošto je predhodni HDD imao jednu pokretnu ručicu i 50 diskova na kojima su skladišteni podaci očekivano je da je usko grlo upravo brzina upisa i čitanja podataka koja je direktno uslovljena brzinom ručice. Rešenje je ugrađeno u novi HDD pod nazivom IBM 1301. Ova jedinica je imala ugrađene pokretne ručice na svakoj ploči što je značajno ubrzalo procese upisa i čitanja podataka. Ovaj HDD je imao 20 ploča za skladištenje i kapacitet od približno 28 miliona karaktera po modulu. Napredak u odnosu na predhodnika je i u tome što novija verzija HDD-a je imala manje rastojanje između glava za upis i ploča što je rezultiralo povećanju gustine podataka smeštenih na ploče¹.

Veliki korak u razvoju je načinjen 1964. godine kada je proizveden IBM 2311 i to je bio HDD koji je prvi imao standardizovan električni priključak čime je postao pristupačan raznovrsnim računarima toga vremena. Ovakav korak je doneo mogućnost IBM-ovim računarima da ugrađuje kompaktilne hard diskove drugih proizvođača.



Slika 1 : IBM 2311

¹ Kean, David W., "IBM San Jose, A quarter century of innovation

Pri uvođenju IBM 3330 hard diska u upotrebu 1970. godine dolazi do napredka na polju korekcije grešaka prilikom prenosa podataka. Ova tehnologija se prvi put primenjuje na 3330 HDD-u i zasnovana je na uočavanju greške u podacima, tako što se greška ispravlja slanjem podataka od izvora do prijemnika.

Korekcija grešaka danas je prisutna u svim hard diskovima. Ovaj model je imao još značajnih poboljšanja koja su se odnosila na poboljšano vreme odziva, gustinu sektora i pouzdanost samog uređaja je bila unapređena.

1973. godine kompanija IBM počinje proizvodnju svog novog modela IBM 3340 sa tri izmenjiva modula za podatke, oni su uključivali modul od 35MB i dva od po 70MB modula. Ovaj hard disk je nosio i ime „Winchester“. Naziv je dobio prilikom samog projektovanja jer je bilo planirano da svaki modul ima po 30MB (30-30) što se poklapalo sa imenom najpoznatije puške na svetu „Winchester“.

Ovaj model je takođe bio specifičan po tome što je prvi imao podmazane diskove i zatvorene module.

Godine 1979. uvodi se tehnologija tankog filma za diskove na kojima se čuvaju podaci. Ova tehnologija koristi tanak sloj materijala koji se nalazi na spljašnosti diskova za skladištenje podataka, umesto feritnog materijala baziranog na metalu koji je značajno povećavao razmak između glave i ploča hard diska što je neposredno uticalo na kapacitet za skladištenje podataka. IBM je ovaj hard disk nazvao IBM 3370 i on je imao kapacitet od 571MB.

Svi navedeni diskovi su napredovali u pogledu kapaciteta i brzine ali postojala je ta fizička prepreka tj. ploče sa podacima su bile velike u fizičkom smislu te je postojala težnja da se one umanje. Ploče su bile prečnika 14 inča (360mm) tako da su napravljene ploče znatno manjih dimenzija koje su bile ugradjivane u hard diskove sa ne izmenjivim pločama od 130mm što je ekvivalent flopi diskova. Kasnije ova promena je iskorišćena u proizvodnji prvih personalnih računara(PC).

Većina hard diskova ranih osamdesetih godina je prodavana kao dodatak krajnjim korisnicima personalnih računara.

1983. godine je predstavljena unutrašnja verzija hard diska koja je imala kapacitet od 10MB i bila je u sklopu IBM PC/XT računara.

IBM 3380 predstavljen je 1980. godine, isporučivan je sa kapacitetom od 2,5GB što ga je učinilo prvim hard diskom koji je nosio oznaku GB. Skladišne mogućnosti su bile dobre ali ovaj uređaj je imao težinu od preko 500kg.



Slika 2 : IBM PC/XT

Fujitsu M2351A („Eagle-1“) predstavljen je 1981. godine. Ovaj hard disk je bio prvi deseto inčni model i upravo je to bilo ključni korak u smanjivanju fizičkih veličina hard diskova koji su do tada pravljani u veličinama od 14 inča.

M2351A je pravljani u više varijanti koje su varirale po kapacitetu od 474MB do 690MB.



Slika 3 : M2351A

Rad na novom standardu 1981. godine je doneo novi standar SCSI („Small Computer Systems Interface“) ovaj standard je imao novitet skladištenja podataka na osnovu logičkih blokova a ne fizičkih lokacija na diskovima u hard disku.

Standard je odobren tek 1986. godine od strane ANSI komiteta iako je na tržištu bilo prisutno hard diskova sa ovim standardom.

„Shugart Technology“ je 1980. godine predstavio model pod nazivom ST-506 hard disk koji je bio prvi 5,25 inčni uređaj te vrste. Ovaj hard disk je imao kapacitet skladištenja od 5 MB i doneo je novu ideju o odvojivim kontrolerima unutar računarskog sistema. Pomerivši kontrolere iz same jedinice HDD-a u kompjuter bilo je moguće koristiti pomenuti hard disk i u drugim brendiranim računarima. Ovaj korak je učinio mnogo time što je u industriji prihvaćena opcija zasebnog kontrolera kao bolja opcija.

1983. godine pojavljuje se prvi 3,5-inčni hard disk. Kompanija „Rodime“ iz Škotske je prva prešla na ovu veličinu hard diskova.



Slika 4 : Rodime HDD

Kompanija „PrairieTek“ je 1988. godine isporučila prvi hard disk u veličini od 2,5 inča. Ova veličina diska je trenutno jako zastupljena i smatra se da će još dosta vremena ostati na tržištu hard diskova. Međutim iako je kompanija „PrairieTek“ učinila veliki korak ona je ipak ugašena i to ubrzo 1991. godine.

1992. godine kompanija „Hewlett-Packard“ predstavlja svetskom tržištu model HP3013/3014 („Kittyhawk“) koji je bio prvi 1,3-inčni hard disk. Ovaj model je najavljivao upotrebu u mobilnim uređajima ali razvoj u ovom segmentu tekao je sporo tako da danas i nema ovu tehnologiju u današnjim tabletima ili mobilnim telefonima.

SATA Working Group je 2000. godine oformljena sa namerom da razvije novi standard za hard diskove. SATA je razvijana da bi unapredila već zastareo ATA standard koji se već godinama koristio. Razlike SATA i ATA standarda su pre svega u boljim performansama, tanjim kablovima, manjim komponentama i mogućnošću povezivanja više od dva uređaja.

Konačno uvođenje SATA standarda dogodilo se 2003. godine a duplo pojačana verzija prenosa podataka od 3Gb/s je uvedena 2005. godine. Danas ovaj standard je i dalje u masovnoj upotrebi.

Kompanija „Hitachi GST“ 2007. godine isporučuje prvi hard disk kapaciteta 1TB. Ovaj uređaj nosi ime „Deskstar 7K1000“ i isporučivan je u 3,5-inčnoj verziji sa 5 ploča(diskova). Ova kompanija postaje jedan od lidera u prodaji hard diskova i 2012. godine kupuje kompaniju „Western Digital“.



Slika 5 : Deskstar 7K1000

HGST je 2013 predstavio planove razvoja hard diskova koji bi se isporučivali sa helijumskim punjenjem. Ova tehnologija treba da omogući manja trenja medju pločama čime bi se povećao broj ploča u samoj jedinici a izbeglo dodatno trenje koje je prisutno u verzijama bez helijuma. Razvijaju se nove tehnologije za zatvaranje hard diska jer je helijum lakši od vazduha pa ga treba zadržati u samom uređaju.²

² "HGST Ships 6TB Ultrastar® He6 Helium-filled Drives for High-density, Massive Scale-out Data Center Environments" Santa Clara, California: hgst.com. 2013-11-04.

Trenutno na tržištu su prisutna tri velika proizvođača hard diskova u odnosu na oko 200 proizvođača koji su se smenjivali tokom godina.

Proizvođači:

- Seagate (koji je kupio Samsugov ogranak za hard diskove)
- Western Digital (koji je u posjedstvu Hitachi GST-a)
- Toshiba(koja je kupila Fujitsu-ov ogranak za hard diskove)

2.1 Glavne komponente Hdd-a

Kućište predstavlja pravougaonu kutiju u kojoj i na kojoj su smeštene sve komponente jednog HDD-a. Kućište je izrađeno od plastike i metala u skladu sa komponentama koje se nalaze u unutrašnjosti i povezano je zavrtnjevima. Samo kućište se ne sme otvarati u uslovima visoke vlage i u prašnjavim okruženjima.

U slučaju eksternih hard diskova kućišta mogu biti zalivena materijalima od gume koji imaju prvenstveno ulogu očuvanja integriteta jedinice u slučaju pada ili udarca.



Slika 6 : Fioka za HDD



Slika 7 : Eksterni HDD

Diskovi („ploče“) su smešteni unutar kućišta i locirani su u centru uređaja. Kako samo ime i govori diskovi su kružne jedinice napravljene od metala koji je namagnetisan i njihova uloga je čuvanje zapisa tj. podataka. Broj ploča varira od jedne pa naviše neki modeli imaju i 10 ploča kao što su hard diskovi „Barracuda“ kompanije Seagate. Ploče su fiksirane za rotor koji pokreće elektro motor. Broj obrtaja diskova se kreće u zavisnosti od proizvođača od 5400 do 7200 obrta u minutu.



Slika 8 : Ploča unutar HDD-a

Pokretna ručica je vezana za elektro motor koji je pokreće na zadata mesta na kojima je potrebno da se nađe. Na vrhu ručice se nalazi glava koja vrši upis i čitanje podataka. Sama glava koja vrši upis/čitanje podataka ustvari nikad i ne dodiruje ploče, ona je otprilike 5 mikrona iznad nje.

Kontrolna jedinica je smeštena iza ploča i ona je povezana sa elektro motorima i pokretnom ručicom koje kontroliše.

3. Upis podataka

Podaci se čitaju i upisuju u vidu serija bitova. Ovi bitovi su upisani na pločama hard diska tj. magnetno osetljivoj površini ploča. Magnetno osetljiva glava koja se nalazi na vrhu ručice prepoznaje da li se podaci čitaju ili upisuju. Karakteri upisani u hard disk nisu upisani bez ikakvog reda već postoje složene matematičke formule koje se koriste za upis. Fabrički u HDD-u se dodaju dodatni bitovi upisanim podacima kako bi se otkrile eventualne greške.

Vertikalno magnetno snimanje omogućava veću količinu podataka ubaciti na dati prostor što takođe omogućava i brže čitanje istih.

Informacije su napisane na obe strane ploče tako da se čitaju i upisuju obostrano. Pokreti ručice koja radi sa upisom/čitanjem i njeno pokretanje od centra ka spoljašnjosti diska naziva se „seeking“ dok je brzina kojom se izvodi „seek time“.

Glava traži prave trake bitova koje su smeštene u vidu kružnica na ploči. Trake su podeljene u logičke jedinice koje zovemo sektori. Svaki sektor ima svoju adresu koja se koristi u organizaciji i lokaciji podataka na disku. U slučaju kada „glava“ ne stigne do željenog sektora onda imamo slučaj rotacionog kašnjenja, ovo se dešava kada je sektor ispod glave i ona mora da obnovi krug radi ponovnog čitanja.

3.1 Greške u sektorima

Danas hard diskovi imaju sisteme za prepoznavanje grešaka (ECC-Error Correction Codes). Takvi sistemi prevashodno su zasnovani na ostavljanju dodatnih bitiova za svaki blok podataka. Tako se mnoge greške ispravljaju neprimetno. Ovi dodatni bitovi sami zauzimaju mesto u hard disku ali pritom omogućavaju znatno veću gustinu podataka upisanih na ploči bez grešaka.

S.M.A.R.T.(Self-Monitoring, Analysis and Reporting Technology) sistem prebrojava totalni broj grešaka koje su popravljene od strane ECC-a i broj blokiranih sektora na disku i na taj način se može predvideti gde je došlo do greške. Usled havarije na hard disku tehničar može da otkrije gde je kvar na osnovu SMART podataka.³

4. Tehničke karakteristike

4.1 Vreme i brzina pristupa

Vreme pristupa podacima generalno je u zavisnosti od brzine obrta diskova kao i glave koja radi na njima. Glavni razlog kašnjenja je već pomenuti slučaj rotacionog kašnjenja koje nastaje zbog toga što željeni sektor ne može uvek biti ispod glave koja vrši upis/čitanje. Ovakva kašnjenja su kašnjenja koja vremenski traju oko nekoliko milisekundi. Brzina prenosa podataka uslovljena je i brojem blokova koji se prenose, oni mogu varirati u dužini.

Pristup podacima se može ubrzati i povećanjem broja obrtaja diskova unutar Hdd-a. Povećanjem gustine upisanih podataka povećava se i protok podataka očitanih od strane glave. Ovim se smanjuje potencijalna potraga za podacima.

³ "HGST Ships 6TB Ultrastar® He6 Helium-filled Drives for High-density, Massive Scale-out Data Center Environments" www.hgst.com

Defragmentacija predstavlja proceduru koja ubrzava proces čitanja podataka sa hard diska. Ovaj proces je zasnovan na premeštanju srodnih sektora što bliže jedni drugima i time se gubi manje vremena u potrazi za određenim sektorima koji čine celinu jedne informacije ili podatka. Danas operativni sistemi poseduju automatsku defragmentaciju što ubrzava proces čitanja podataka ali i smanjuje brzinu ukoliko je pomenuti proces u toku.

Vreme traženja podataka u proseku na današnjim hard diskovima je 4ms(noviji serveri) do 15ms(mobilni računari) dok se ta brzina za desktop računare iznosi 9ms.

Prvi hard diskovi su imali vreme potrage za podacima oko 600ms ta brzina je podignuta krajem sedamdesetih godina na 25ms.⁴

Prenosivi računari kao što su laptopovi imaju mogućnost promene brzine traženja podataka. Ova opcija je prisutna zbog zvuka koji proizvode rotor i vibracija od strane hard diska tako da je omogućen izbor između performansi i tišeg rada samog računara.

Brzina prenosa podataka od diska do bafer memorije se kreće od 1Gb/s do 3Gb/s i ona je uslovljena od toga gde se nalaze podaci na disku. Ukoliko su podaci bliže krajevima diska gde je prečnik diska veći nalazi se i veći broj podataka što čini njihovo čitanje znatno bržim. Trenutno se koristi standard 3Gb/s SATA koji omogućava prenos 300MB/s podataka od bafera do kompjutera što je u prednosti u odnosu na brzinu disk-bafer. Ovakav prenos je omogućen 10-bitnim šifrovanjem.

Jasno je da na brzinu prenosa podataka utiče brzina rotiranja ploča kao i gustina upisa podataka, pojavile su se fizičke prepreke koje onemogućavaju povećanje brzine rotiranja jer ako povećamo brzinu dobijamo vibracije koje su nepoželjne. Za povećanje brzine rotacija potrebni su i jači motori koji bi stvarali višu temperaturu tako da se razvoj usmerava ka povećanju gustine kako broja traka tako i broja sektora u trakama podataka upisanih na ploči.

⁴ "IBM Archives: IBM 3350 direct access storage"

4.2 Konektori prenosa podataka

- **SCSI**(Small Computer System Interface) je prvenstveno korišćen kao standard na računarima srdinom devedesetih godina.
- **IDE**(Integrated Drive Electronics) kasnije preimenovan u AT Attachment (ATA) kao i PATA (Parallel ATA)
- **EIDE** predstavlja prepravku IDE standarda od strane kompanije „Western Digital“. Ključna prepravka se nalazi u pristupu memoriji DMA(Direct Memory Access) koja prenosi podatke između diska i kompjutera bez angažovanja centralne procesorske jedinice. Ovo unapređenje je kasnije usvojio ATA standard.
- **Fibre Channel** (FC) predstavlja naslednika paralelnog SCSI-a. Ovo je serijski protokol koji se koristi sa FC-AL (Fibre Channel Arbitrated Loop) tehnologijom. Imao je značajnu ulogu u razvoju Eterneta.
- **Serial Attached SCSI** (SAS) je novija generacija serijskih komunikacionih protokola za uređaje koji koriste velike brzine prenosa podataka, takođe je i kompatibilan sa SATA. SAS koristi identične konektore za prenos podataka i napajanje hard diska kao i 3,5 inčni SATA/1 i SATA/2 diskovi.
- **Serial ATA**(SATA) kabl za prenos podataka ima jedan par za diferencijalni prenos i jedan par za diferencijalni prijem podataka. Ovakav sličan signalni sistem imaju i USB,FireWire,LocalTalc.

SATA je kompjuterski interfejs kojim se povezuju hard diskovi i optički uređaji na matičnu ploču. Serijski ATA je zamenio prethodni ATA standard i time smo dobili manje kablove(uže pre svega) i brži prenos podataka pre svega.

Verzije :

SATA verzija 1.0 je ušla u upotrebu 2003. godine poznata i pod imenom SATA 1,5Gb/s kao i što samo ime kaže brzina prenosa podataka je bila 1,5Gb/s.

SATA verzija 2.0 ima brzinu prenosa podataka 3Gb/s .

SATA verzija 3.0 ima brzinu prenosa podataka od 6Gb/s.

SATA verzija 3.1 pojavila se sredinom 2011. godine , ova verzija ima poboljšanja vezana za SSD tehnologiju.

SATA verzija 3.2 poseduje brzinu prenosa podataka od 16Gb/s.

SATA Express ova verzija je specifična po tome što kombinuje SATA i PCI Express konektore.

SATA M.2 je standard koji je unapredio SATA Express sa USB 3.0 portom.

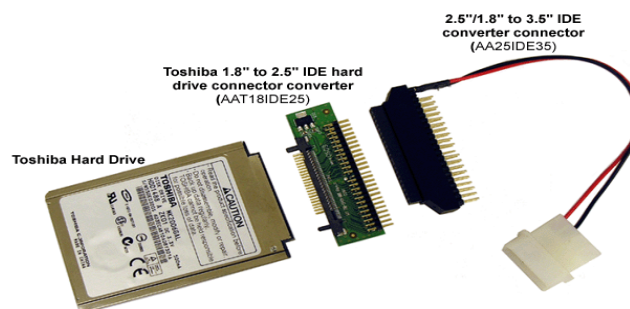
eSATA je standard prihvaćen 2004. godine i njegova namena je za spoljno povezivanje uređaja, standard je sličan SATA standardu samo je za konekciju potreban kabl koji je bolje izolovan od mogućih smetnji iz spoljašnjosti.

Mini SATA (mSATA) je standard koji se danas koristi u prenosivim računarima kao što su laptopovi, noutbukovi i drugi.

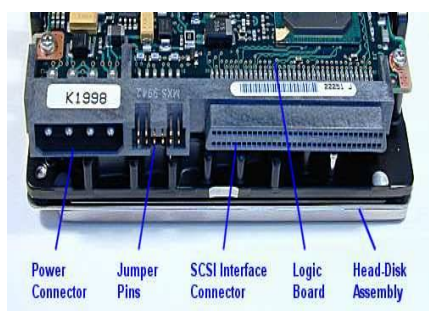
Pregled pomenutih standarda :

Ime:	Brzina prenosa(MB/s):
eSATA	300
SATA 1.0	150
SATA 2.0	300
SATA 3.0	600
SATA 3.2	1659
PATA(IDE)	133,5
Fibre Channel(optika,kabl)	1000/400
SCSI Ultra 640	640
SCSI Ultra 320	320

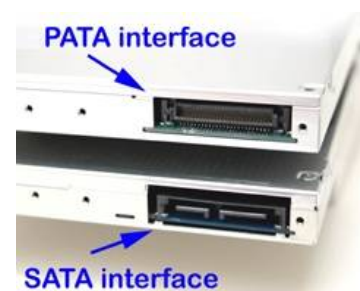
Tabela 1 : Standardi



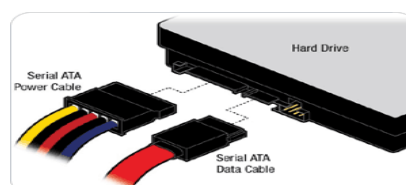
Slika 9 : IDE standard za različite veličine HDD-a



Slika 10 : SCSI konektor HDD



Slika 11 : PATA-SATA HDD



Slika 12 : SATA konekcija

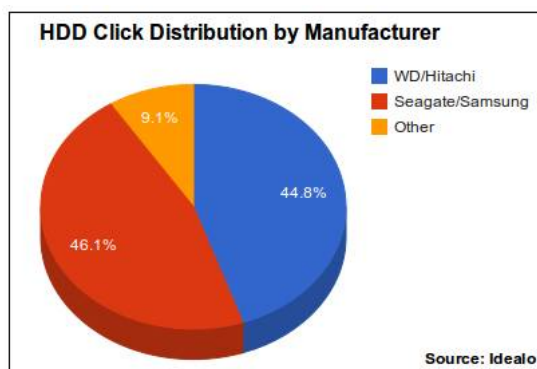
4.3 Proizvođači i udeo tržišta

Lista proizvođača hard diskova nije tako velika, postoje firme koje su se reformisale i opstale ali i one koje su ugaše a spadale su u pionire u proizvodnji HDD uređaja.

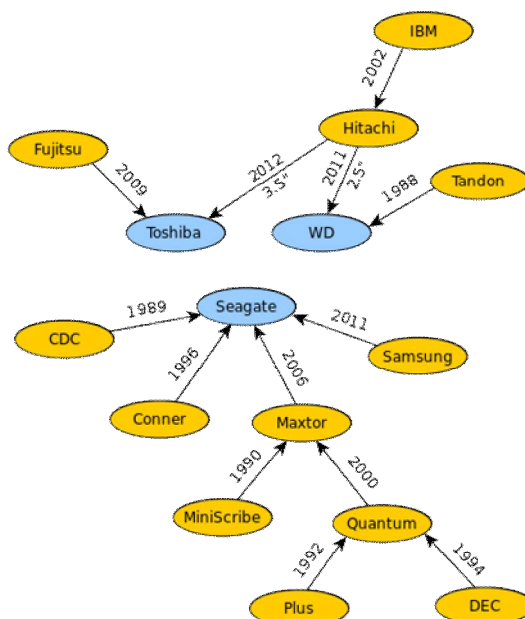
Nabrajaćemo neke od poznatijih proizvođača: Seagate Technology(Maxtor i Samsung), Toshiba, WesternDigital(HGST), Fujitsu, TrekStor, Hp, Intenso, Lenovo, CnMemory, Buffalo, Verbatim...

Danas na tržištu situacija je takva da par kompanija drže većinu tržišta.

U nastavku je prikaz dijagrama sa udelom na tržištu hard diskova u procentima od strane vodećih kompanija.



Dijagram 1: Udeo tržišta za 2013. godinu



Dijagram 2: Udruživanje kompanija

5. SSD (Solid State Drive)

SSD predstavlja uređaj za skladištenje podataka baziran na NAND fleš memoriji(memorija koja je slična onoj koja se koristi u USB fleš uređajima). Kako mu ime govori ovaj uređaj je celovit bez pokretnih delova. Ova tehnologija za skladištenje podataka je i do deset puta brža od standardnog HDD-a. Razlog za ovoliku razliku u brzini tj. performansama se krije u NAND fleš memoriji, pošto HDD mora podatke da pročita rotirajući svoje ploče a SSD ima trenutni pristup memoriji. Pored većeg protoka podataka razlika je i u pogledu komfora uređaji su znatno manji i tiši tj. SSD se ne čuje jer nema pokretnih delova u sebi. Prednost toga što su izradjeni bez pokretnih komponenti vidna je i u pogledu stvaranja toplote. Ovi uređaji ne zahtevaju dodatne kulere radi hlađenja. Kod HDD-a postoji mogućnost oštećenja uređaja ukoliko se on naglo pomeri ili primi udarac u toku rada zbog glave koja radi sa upisom podataka dok kod SSD-a taj problem ne postoji.

5.1 SSD razvoj i arhitektura

Početak priče o SSD tehnologiji počinje pedesetih godina kada su dve slične tehnologije memorija sa magnetnim jezgrom i CCROS(Card Capacitor Read Only Store). Upak ove tehnologije su već prevaziđene sedamdesetih godina i prvi SSD uređaji se ugrađuju u IBM-ove kompjutere. Problem je bio u tome što je to bila preskupa tehnologija i zato su ih retko koristili.

1976. godine Dataram počinje prodaju uređaja „Bulk Core“ koji poseduje 2 MB „čvrste memorije“. Texas Memory Systems predstavlja 1978. godine 16KB RAM sa SSD tehnologijom.

1983. godine Sharp PC-5000 koristi čvrstu memoriju od 128 KB.

1984. godine Tallgrass Technologies Corporation predstavlja bekap traku od 40MB od kojih 20 MB čini čvrsta memorija.

1987. godine EMC Corporation ulazi na tržište SSD tehnologije za male kompjutere.

1991. godine kompanija San Disk napravila je SSD uređaj sa kapacitetom smeštanja podataka od 20 MB.

1995. godine kompanija M-Systems predstavlja SSD zasnovan na fleš tehnologiji. Ova tehnologija omogućava čuvanje podataka bez dodatnih baterija kakve su predhodne tehnologije zahtevale.

1999. godine BiTMICRO je napravio dosta koraka u SSD fleš tehnologiji, jedan od njih je i predstavljanje 18GB SSD uređaja u 3,5-inčnom izdanju.

2007. godine Fusion-io SSD uređaj koji koristi PCIe konekciju koji ima mogućnost 100 000 ulazno/izlaznih operacija po sekundi u jednoj karti sa kapacitetom do 320GB.

2009. godine OCZ Technology predstavlja SSD uređaj sa PCIe konekcijom kapaciteta od 1TB. Ovaj uređaj ima brzinu pisanja od 654 MB/s i brzinu čitanja 712MB/s. Iste godine Micron Tehnology predstavlja SSD koji koristi SATA konekciju od 6Gb/s.

Ključne komponente SSD-a su kontroler i memorija za skladištenje podataka NAND. Pored navedenog imamo i DRAM koji se koristi za baferovanje. Uređaj poseduje i standardne SATA konektore za prenos podataka i napajanje.

Kontroler koristi multi procesor za komunikaciju sa NAND memorijom preko paralelnih kanala. Njegov posao je da ispravlja kodove(ECC), vrši šifrovanje, piše i briše keš, mapira loše sektore.

NAND Flash predstavlja čipove memorije koji čuvaju podatke u uređaju. Prednost ove memorije je što ima sposobnost čuvanja podataka bez konstantnog napajanja električnom energijom. Ova memorija se deli na MLC(Multi Level Cell) i SLC(Single Level Cell). SLC je pouzdanija i brža vrsta memorije.

DRAM se koristi za baferovanje. Kao i na HDD-u i ovde se podaci čuvaju privremeno dok se ne zapišu u permanentnu memoriju. Takođe postoje SSD uređaji bazirani na DRAM-u i njihova odlika je da su jako brži u odnosu na standardne SSD uređaje. Ovakvi uređaji imaju unutrašnju bateriju ili bekap uređaj za napajanje radi očuvanja podataka.

Moderan SSD uređaj dolazi sa SATA 6Gb/s konektorom koji dozvoljava upis i čitanje do brzine od 550 MB/s. Sledeća generacija konektora zove se SATA Express i ona će preko PCI Express dozvoljavati prenos podataka od 16Gb/s.

Sve prethodno navedeno nalazi se u kućištu koje je izrađeno od plastike ili metala u zavisnosti od proizvođača i modela. Ovi materijali pomažu u odvlačenju toplote od memorije iznutra. Kućišta su debljine svega 7 mm čime se primena SSD-a omogućava u raznim uređajima kao naprimer ultrabuk računarima ili laptopovima.



Slika 13 : Anatomija SSD-a

1. *Spoljno kućište*
2. *NAND fleš*
3. *DRAM buffer*
4. *Konektori za prenos podataka i napajanje*
5. *Kontroler*

5.2 Poređenje SSD-a i HDD-a

Komparacija SSD i HDD tehnologija danas je jako aktuelna iz više razloga. Kao što znamo obe tehnologije su se razvijale decenijama ali ipak zastupljenost nije bila podjednaka što se tiče uređaja za trajno skladištenje podataka u računarima. Zastupljenost HDD-a je i danas znatno veća u odnosu na SSD tehnologiju ali već se vide naznake skorije promene snaga na tržištu. Danas SSD uređaji prisutni na tržištu već imaju podjednake performanse pa i bolje u odnosu na HDD uređaje ali ipak problem su i dalje visoke cene ovih uređaja.

U nastavku ćemo videti tabelu sa ključnim razlikama ove dve tehnologije.

Karakteristike:	SSD	HDD
Startovanje (buđenje)	Gotovo trenutno startovanje uz nekoliko milisekundi.	Rotiranje ploča pri startu koje traje nekoliko sekundi
Vreme pristupa podacima	Uobičajeno vreme pristupa oko 0,1ms.	U zavisnosti od HDD-a kreće se od 2,9-12 ms. Zbog pozicioniranja glave za čitanje na pravu lokaciju na ploči HDD-a.
Prenos podataka	Prenos podataka varira od broja pristupa blokovima, što je broj veći to je brzina manja. Inače brzina prenosa se kreće između 100-600 MB/s u zavisnosti od uređaja. Prisutne su i verzije sa prenosom od više gigabajata po sekundi.	Ukoliko je glava za čitanje pozicionirana na traci koja se čita prenos se kreće oko 140 MB/s. Ovo važi za idealni slučaj gde su podaci smešteni odmah ispod glave dok u praksi brzina je znatno manja zbog vremena potrage za trakama(podacima) na pločama. Takođe prenos podataka zavisi i od brzine rotacije ploča kao i od pozicije trake sa podacima na ploči.
Brzina čitanja	Čitanje podataka u odnosu na lokaciju gde se oni nalaze na SSD uređaju nema nikakve razlike. Za razliku od HDD uređaja SSD uređaji su slabi po pitanju NAND čelija koje vremenom pokazuju pad performansi.	Kako i kod prenosa zavisi od pozicije , ukoliko je ploča fragmentirana odziv će biti značajno brži.

Tabela 2 : Poređenje HDD i SSD

Fragmentacija	Fragmentiranje nije od neke koristi u SSD –u dok defragmentacija nije pogodna za ovu tehnologiju jer dodatna pisanja po NAND-u „troše“ ćelije za skladištenje tj. Njihov životni vek.	Fajlovi na HDD-u ukoliko se češće koriste pogotovo veći fajlovi se fragmentuju. Proces defragmentacije je neophodan u ovoj tehnologiji radi očuvanja performansi.
Buka	Pošto SSD uređaji nemaju pokretne delove nivo zvukova koji oni proizvode je zanemarljiv.	HDD uređaji imaju pokretne delove koji prave određene zvukove koji variraju od zavisnosti koji je model u pitanju.
Zagrevanje	SSD uređaji inače lakše podnose više temperature u odnosu na HDD uređaje. Isto tako njima nisu neophodni naknadni sistemi za hlađenje.	U praksi HDD uređaji nemaju naknadne kulere ali ipak je preporučljivo ugraditi ih jer ovi uređaji mogu da se oštete ukoliko njihova temperatura pređe 55 °C.
Otpornost na okruženje	Otporan na vibracije i udarce.	Ploče osetljivije na vibracije i udarce.
Instalacija	Jednostavan bez osetljivih tačaka.	Kola izložena o tome se vodi računa da ne dođe do kratkog spoja sa provodnikom.
Osetljivost na magnetna zračenja	Minimalan uticaj na memoriju SSD-a.	Postoji mogućnost oštećenja podataka.
Veličina i težina	3,5-inča; 2,5-inča i 1,8-inča slične težine kao i parnjaci iz Hdd tehnologije.	Mogu biti nešto teži. 3,5 – inčni Hdd je težak oko 700g.
Pouzdanost i radni vek	Blokovi imaju ograničen broj upisa i prepisa tokom upotrebe uređaja. SSD uređaji koji koriste DRAM tehnologiju nemaju ta ograničenja. Ranjiviji su na gubitak napajanja.	Ovi uređaji u odnosu na SSD uređaje imaju i potencijalne mehaničke kvarove zbog svojih pokretnih delova. Prosečni vek trajanja HDD uređaja je između 9-11 godina. U pogledu čuvanja podataka na duži period HDD uređaji su u prednosti u odnosu na SSD.
Ograničenja u sigurnosti podataka	NAND memorija se može prepisati na prethodno izbrisane blokove. Iako se podaci naknadno prepisu prethodni podaci su nesigurni sve dok se ne iskoristi opcija sigurnog brisanja.	Podaci se u slučaju prepisivanja ne gube u potpunosti tako da i ovaj sistem nije siguran što se tiče podataka koji su „prepisani“.

Cena	Zbog skorije pojave na globalnom tržištu ona je i dalje visoka u odnosu na HDD uređaje ali sa tendencijom opadanja.	Dostupni korisnicima.
Kapacitet podataka	Trenutno na tržištu postoje uređaji od 4TB, sledeće godine najavljene verzije od 8TB.	Trenutno prisutni na tržištu uređaji sa kapacitetom upisa od 8TB podataka.
Napajanje-potrošnja	Potrošnja električne energije znatno manja u odnosu na HDD uređaje. DRAM SSD uređaji imaju sličnu potrošnju električne energije kao i HDD uređaji.	Potrošnja se kreće u zavisnosti od formata HDD uređaja od 2-20 vati.

Tabela 2 : Poređenje HDD i SSD

5.3 Poređenje sa memorijskim karticama

SSD uređaji i memorijske kartice su uređaji različite vrste tehnologija prisutne na danas rastućem tržištu skladišnih komponenata. SSD uređaji se namenski usavršavaju za upotrebu u računarima kao komponente za trajno skladištenje podataka.

Memorijske kartice su skladišni uređaji razvijeni prevashodno za uređaje kao što su kamere, telefoni, GPS uređaji i razni igračke uređaje. One su dizajnirane pre svega za manje uređaje od računara kao i da se mogu lako promeniti tj. izvaditi iz uređaja. Postoje adapteri koji mogu da povežu memorijske kartice i samim tim da ih učine sličnim SSD uređajima za skladištenje podataka samog računara ali ovakav vid korišćenja memorijskih kartica za sada nije aktuelan. Standardne memorijske kartice su nekoliko puta sporije od trenutnih SSD uređaja. Takođe memorijske kartice nisu dizajnirane za veliki broj upisa i čitanja kao SSD uređaji i došlo bi do oštećenja uređaja i gubitka podataka.

Memorijske kartice su tehnologija skladištenja podataka koja ne traži dodatno napajanje radi čuvanja podataka. Kartice su bazirane na fleš memoriji od koje su počele i novije verzije SSD uređaja da se prave. Danas USB fleš jesu predstavnici fleš tehnologije ali ta memorija nije ista fleš memorija kao kod SSD uređaja ona je znatno lošijih performansi.⁵

⁵ <http://danielmiessler.com/blog/the-difference-between-ssd-and-flash-hard-drives/>

5.4 Proizvođači i udeo tržišta

Danas postoji oko 500 kompanija koje učestvuju u proizvodnji SSD uređaja.

Fusion –io, IBM, LSI, HGST, OCZ, SanDisk, Virtium, Samsung, Micron, Toshiba, Intel...

U nastavku tabela sa najvećim proizvođačima SSD uređaja kao i udeo u tržištu za 2014. godinu.

Proizvođači	Prodate jedinice(milioni)	Procenat u tržištu(%)
Samsung	5634	28%
SanDisk	4656	23%
Kingston	1944	9,7%
Intel	1408	7%
Toshiba	1369	6,8%
Micron	1235	6%
SK Hynix	525	2,5%
HGST	125	0,6%
OCZ	46	0,2%
Ostali	3150	15,7%

Tabela 3 : Proizvođači i udeo u tržištu SSD uređaja⁶

⁶ <http://www.storagenewsletter.com/rubriques/market-reportsresearch/market-share-of-ssd-suppliers-in-2q14-trendfocus/>

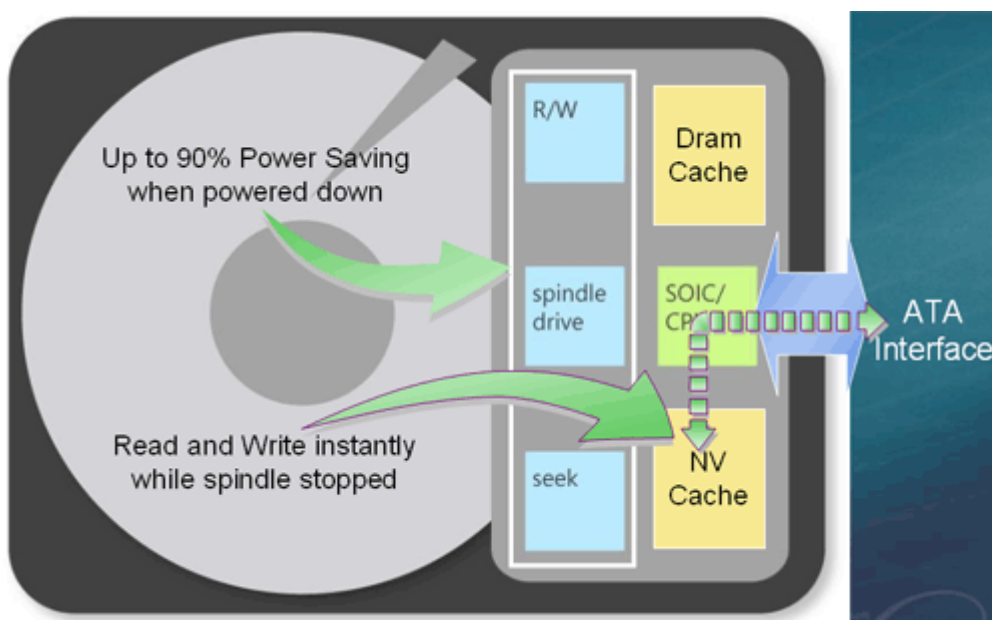
6. Hibridni hard diskovi

Hibridni hard diskovi kao što im i ime govori sačinjeni su od dve tehnologije. U ovom slučaju iskorišćene su rotirajuće ploče standardnih HDD uređaja koji su povezani sa manjom količinom brze fleš memorije u jednom uređaju.

Hibridni uređaj prati podatke koji se čitaju sa hard diska i najčešće korišćene podatke kešuje u brzoj NAND fleš memoriju. Ovako sačuvani podaci skladišteni u brzom memoriji omogućavaju uređaju znatno brži rad tj. čitanje podataka, ovi podaci se tokom vremena menjaju u skladu sa potrebama korisnika tj. njegovim korišćenjem određenih podataka. Performanse su neuporedive u odnosu na standardni hard disk i približne su SSD uređajima.

Prednosti hibridnih uređaja za skladištenje podataka jesu i njihova cena koja je znatno povoljnija u odnosu na SSD uređaje, takođe kapacitet hibridnog diska je znatno veći u odnosu na SSD uređaje jer kombinuje skladištenje na pločama (HDD) i NAND memoriji koja se koristi u SSD uređajima. Za postizanje ovakvih performansi zaslužena je mala količina brze memorije i time je izbegnuta ugradnja veće količine brze memorije koja bi znatno povećala cenu uređaja i učinila ga neisplativim.

Cena je glavni razlog konkurentnosti ovih uređaja jer je ona nešto veća od HDD uređaja ali znatno ispod cenovnog ranga SSD-a.⁷



Slika 14: Hibridni hard disk

⁷ www.pcoworl.com/ssds-vs-hard-drives-vs-hybrids-which-storage-tech-is-right-for-you-.html

Slabosti hibridnih uređaja su vidljive u procesima obrade novih podataka. Kada se upisuju novi podaci u uređaj ili čitaju hibridni uređaj se ponaša kao standardni hard disk. Hibridni hard disk ima određen vremenski period koji mu prilikom korišćenja podataka omogućava da „nauči“ koji podaci se najčešće koriste i da te podatke ubaci u brzu memoriju.

Za korisnike koji ne rade konstantno sa novim podacima ili ne upravljaju sa više particija hibridni hard disk može da bude dobra opcija koja će poboljšati performanse njihovog računara. Ovim se korisniku omogućava da bez kupovine dodatnog SSD-a i odricanja velikog kapaciteta memorije za skladištenje dobije brži uređaj za skladištenje podataka.

Za korišćenje hibridnih uređaja postoje i specijalizovani softveri za kešovanje podataka. Poznati softver iz ove branše je Intelov Smart Response Technology(SRT). Takođe postoje i dual uređaji koji kombinuju SSD i HDD komponente u jednom uređaju ali su dve komponente vidljive za operativni sistem.

Takođe da bi ovaj softver funkcionisao potrebna je podrška od strane OS proizvođača. Microsoft je dodao ovu podršku u Windows 8.1 verziju⁸ dok je podrška za Linuks dostupna od oktobra 2014. godine.⁹

⁸ Andy Herron (2013). „Advancements in Storage and File Systems in Windows 8.1“. SNIA.

⁹ Michael Label , „Linuks Kernel Finally Being Optimized For SSHDs“. Phoronix. 29.10.2014.

7. SSD i HDD test

Trenutno u ponudi na tržištu prenosivih(laptop) računara postoje uređaji sa klasičnim HDD, SSD i hibridnim skladišnim uređajima. Klasičnom kupcu skraćenice SSD i HDD ne znače puno već se pri izboru uređaja vode logikom „što više - to bolje". Upravo zbog toga u nastavku će biti prikazana analiza više skladišnih uređaja, samim time i različitih tehnologija koje će dati bolju sliku pri odabiru ovih komponenti prilikom nabavke istih. Cilj analize jeste odgovor na pitanje da li vam je potreban SSD, HDD ili možda hibridni uređaj koji je kreiran kao kompromis ove dve različite tehnologije.

Za analizu korišćeni su sledeći uređaji:

- Western Digital Scorpio Black 500GB 7200rpm
- Seagate Momentus XT 500GB
- Fujitsu 320GB 5400rpm
- OCZ Agility 2 120GB
- OCZ Vertex Limited Edition 50GB
- Crucial Real SSD C300 64GB



Slika 15 : Hibrid, HDD i SSD

Western Digital-ov HDD uređaj je skladišna jedinica koja ima kapacitet od 500GB i rotaciju ploča od 7200rpm i nosi naziv Scorpio Black.

Seagate je proizveo hibridni uređaj pod nazivom Momentus XT. Ovaj uređaj koristi kombinaciju klasičnog HDD-a i SSD uređaja. Njegova HDD „polovina“ ima kapacitet od 500GB, pored nje ovaj uređaj ima i 4 GB SSD memorije. SSD memorija u ovom uređaju je iskorišćena kao keš memorija tako da najčešće korišćeni podaci se upisuju u SSD memoriju čime bi teorijski ovaj uređaj bio jako blizu standardnom SSD uređaju.

Fujitsu-ov model pod nazivom MHZ2320BH-G2 poseduje standardne karakteristike HDD-a od 5400rpm kao i 320GB memorije.

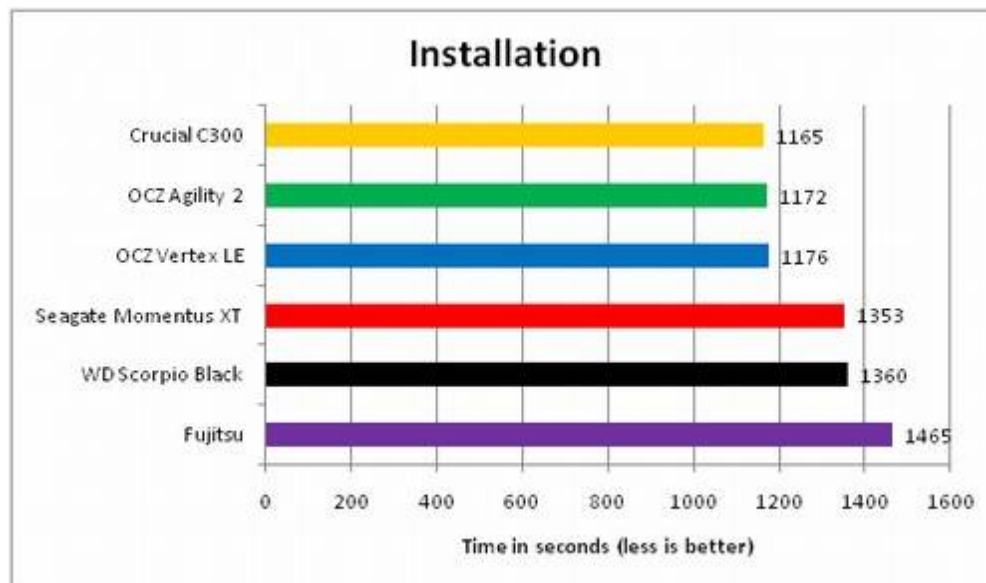
OCZ -ovi predstavnici u ovoj analizi su Agility 2 i Vortex Limited Edition. Ovi uređaji danas su prisutni na tržištu SSD-a koje uzima maha.

Crucial C300 predstavlja SSD uređaj koji je među prvima ponudio potrošačima SATA III interfejs. Ova mogućnost je jako bitna zbog brzine prenosa podataka koja je podignuta sa 3 Gb/s na 6Gb/s.¹⁰

U nastavku ćemo videti dijagrame koji prikazuju performanse prethodno navedenih uređaja. Ispitivanja su vršena u realnim uslovima i prikazuju performanse uređaja koji su testirani prilikom uobičajenog korišćenja računara. Svi navedeni uređaji su instalirani u HP Pavilion dm3 notebook.

Jedna od radnji koja je monotona i oduzima vreme jeste instalacija softvera. U sledećem dijagramu je prikazana brzina testiranih uređaja. Prethodno je instaliran OS na uređaje Windows 7 Home Premium kao i najčešće korišćeni softveri : antivirus, MS Office 2007 i Adobe Photoshop CS4.

¹⁰ „SSD vs HDD : A Beginners Guide to SSD Upgrades“ , notebookreview.com



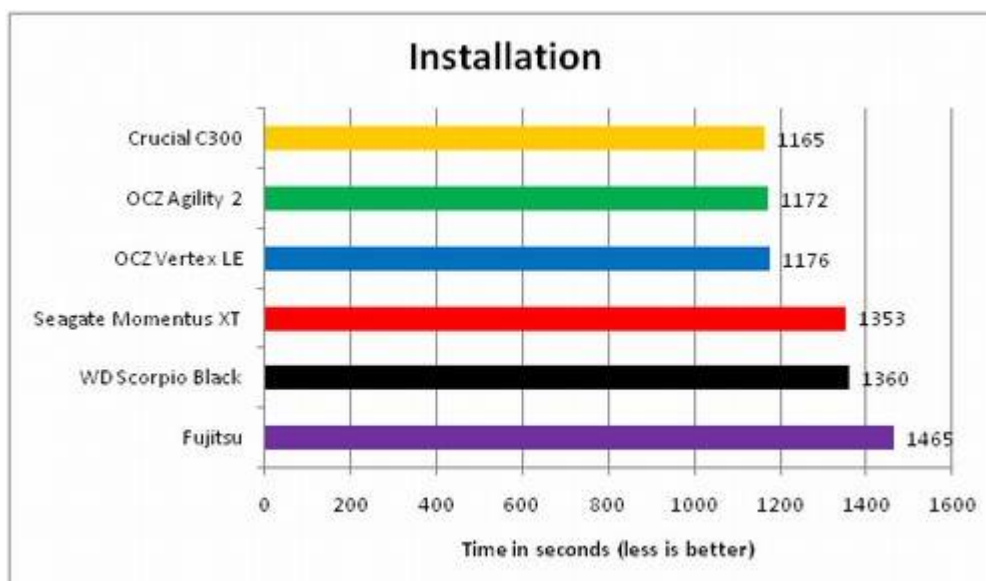
Dijagram 3: Instalacija softvera

Test: 1

Na grafiku je očigledno da SSD uređaji preuzimaju pobjedu. Kao što je i očekivano najsporiji uređaj je Fujitsu. Razlika između WD 7200rpm u odnosu na ostale SSD uređaje iznosi oko 3 minuta što nije zanemarljiv vremenski period kašnjenja.

Test:2

Sledeći test predstavlja butovanje Windowsa 7 preko Boot Timer-a.

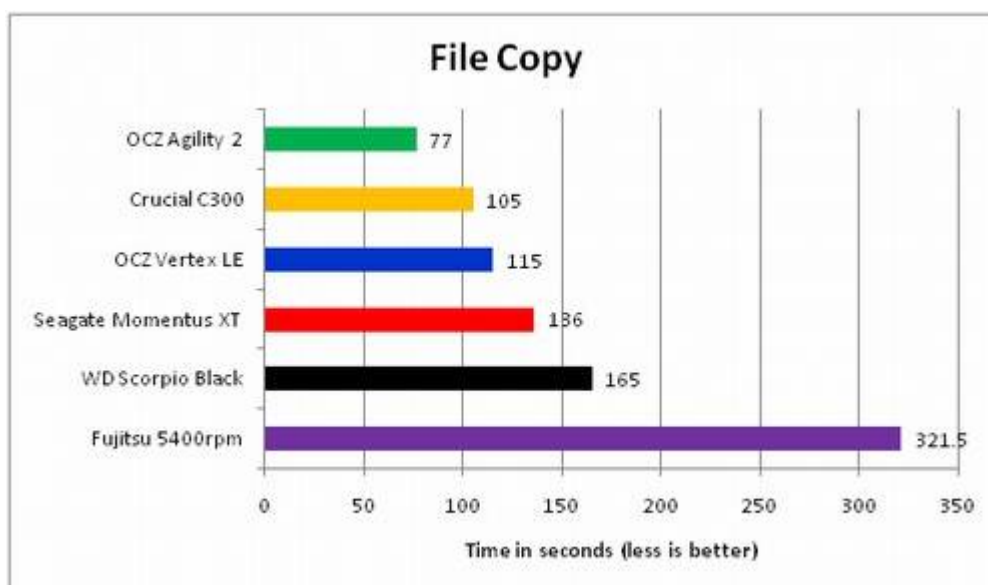


Dijagram 4: Butovanje Windows 7 OS-a

Ovaj test jasno pokazuje razliku u brzini uređaja. Zanimljivost ovog testa je u rezultatu Seagate XT modela koja je bliža klasičnom SSD uređaju. Ovde se vidi prednost hibridnog uređaja nad klasičnim HDD-om.¹¹

Test :3

Da bismo dobili rezultate brzine kopiranja podataka na uređajima kopiranja su dva foldera na istim particijama. Jedan folder sadrži nasumične fajlove i slike dok drugi sadrži HD video zapise. Ukupno se kopira 11GB podataka.



Dijagram 5: Kopiranje fajlova

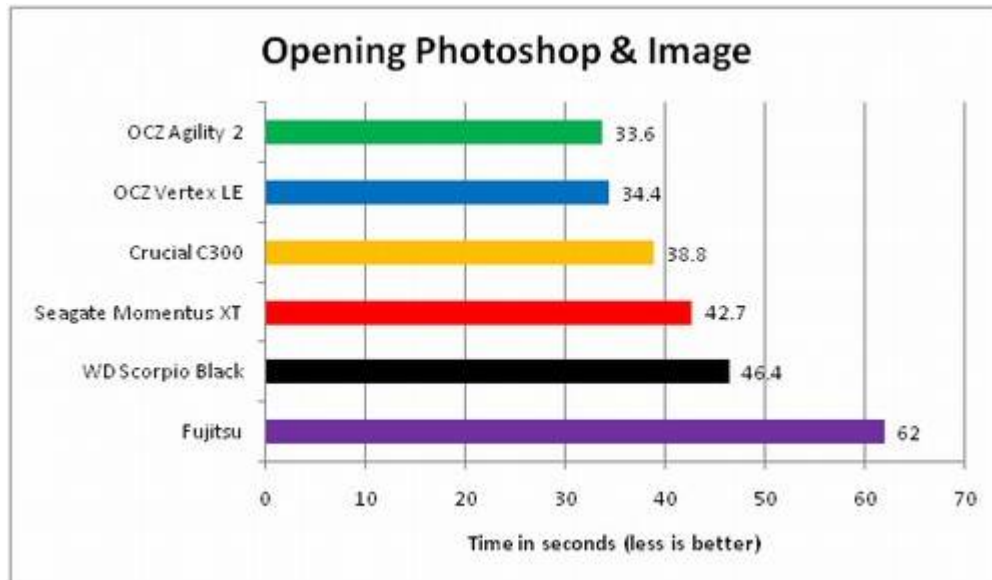
Iz prikazanog jasno je da OCZ Agility ima zavidne performanse u odnosu na ostale uređaje. Dolazimo do zaključka da je prosečna brzina kopiranja kod Agility-a oko 143MB/s. Hibridni uređaj i dalje pokazuje da je brži u odnosu na HDD uređaje.¹²

¹¹ „SSD vs HDD : A Beginners Guide to SSD Upgrades", notebookreview.com

¹² „SSD vs HDD : A Beginners Guide to SSD Upgrades", notebookreview.com

Test : 4

Ovaj test se sastoji od otvaranja velike slike TIFF formata kao i pokretanja Photoshop-a.

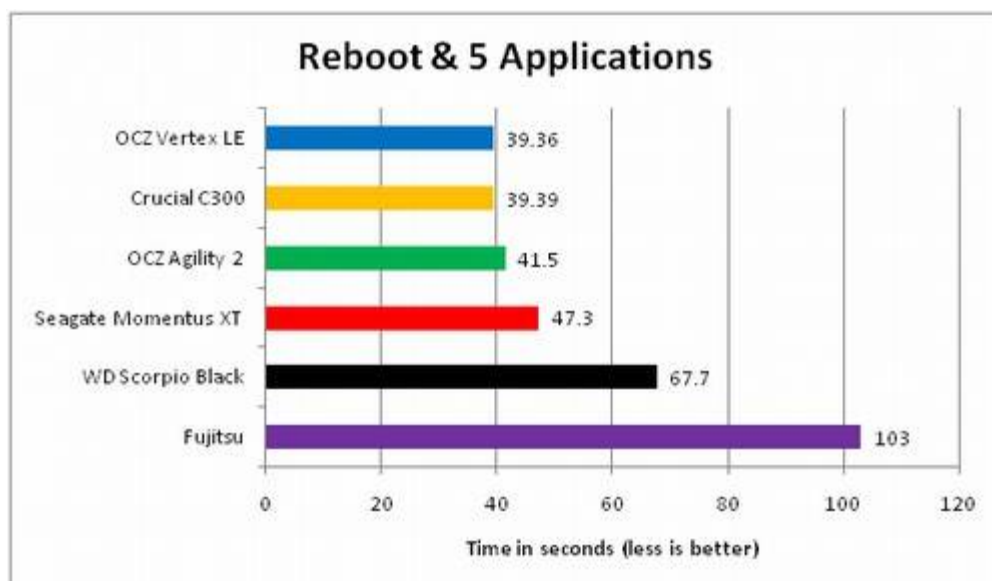


Dijagram 6: Otvaranje slike i softvera

Rezultati ovog testa su slični predhodnom uz zamenu mesta između OCZ Vertexa i Cruciala.

Test: 5

Ovaj test je postavljen tako da je u startup folderu ubačeno 4 aplikacije i prečica ka 720p video fajlu. Ovim se računar testira pri aktivaciji 5 različitih aplikacija i pokretanju video fajla. Merenje počinje od pritiska „restart“ opcije do pokretanja video fajla.



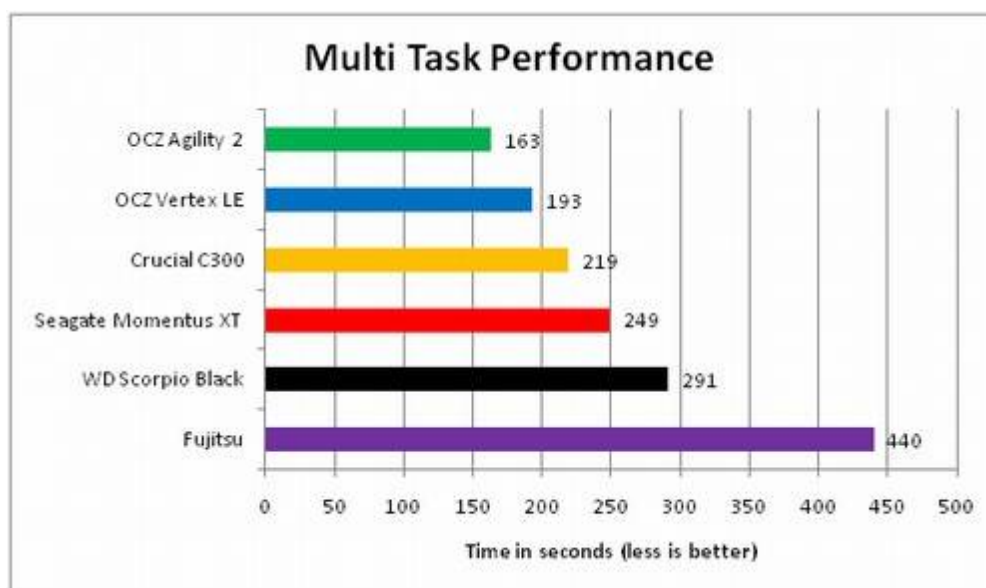
Dijagram 7: resetovanje i pokretanje 5 aplikacija

Rezultati ponovo približni, SSD uređaji ponovo u vodstvu, Momentus XT se približio SSD uređajima.¹³

Test: 6

Danas korišćenje računara podrazumeva i angažovanje više programa koji obavljaju svoje radnje u istom vremenskom periodu(multitasking). Test je sačinjen od korišćenja Avast Virus scanner-a dok se u isto vreme kopira folder i dekompresuje zipovan fajl sa 7zip-om. Drugi test se sastoji iz otvaranja slike visoke rezolucije i Photoshop-a dok se u pozadini odvija proces anti-virus skeniranja. Vreme koje je potrebno za otvaranje slike i Photoshop-a je mereno.

Konačni rezultat oba testa je sabran i prikazan na dijagramu.



Dijagram 8: Multitasking

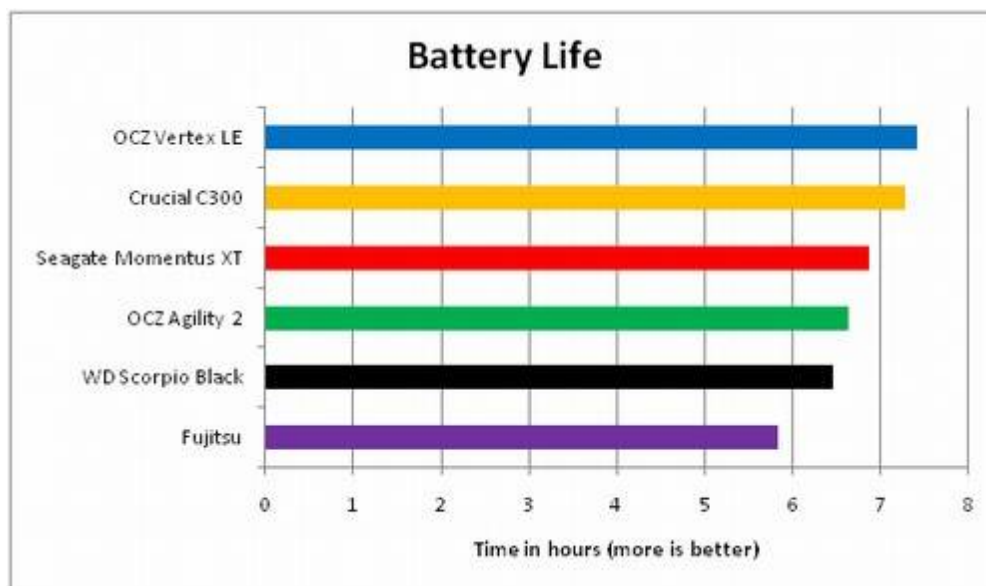
Rezultat pokazuje da je uređaj OCZ Agility 2 najbolji izbor za multitasking. Ostali uređaji su se pokazali standardno u odnosu na prethodne testove.¹⁴

¹³ „SSD vs HDD : A Beginners Guide to SSD Upgrades", notebookreview.com

¹⁴ „SSD vs HDD : A Beginners Guide to SSD Upgrades", notebookreview.com

Test: 7

Računar koji je korišćen za testiranje je takođe i prenosni računar tako da se pokreće pitanje trajanja baterije ovog uređaja. Instaliran je softver pod nazivom „Batterybar 3.4.1“. Računar je korišćen određen vremenski period(nešto više od jednog časa) pri uključenom bežičnom internetu i osvetljenju ekrana od 50%.



Dijagram 9: Trajanje baterije

Pokazalo se da SSD uređaji mogu znatno da poboljšaju vek trajanja baterije. Vertex i C300 su pokazali bolji rezultat u odnosu na Momentus XT i to od oko pola časa. OCZ Agility se nije pokazao kao štedljiv uređaj bar kada je u pitanju potrošnja električne energije.¹⁵

Zaključak ovog testiranja je da su OCZ Agility i Vertex Le pokazali brzim uređajima u svim prethodnim testovima. Oni su izuzetno brzi u multitaskingu. Najveće iznenađenje predstavlja hibridni uređaj Seagate Momentus XT koji se pokazao znatno brzim i jako blizu SSD uređajima daleko bliže nego HDD uređajima iz testa. HDD uređaji su se pokazali sporijim u odnosu na SSD u svim testovima ali njihova konkurentnost nije zasnovana na performansama u odnosu na SSD uređaje već na njihovoj ceni koja je znatno niža a time i pristupačnija prosečnom kupcu.

¹⁵ „SSD vs HDD : A Beginners Guide to SSD Upgrades“, notebookreview.com

8. Digitalna forenzika

Uvođenjem računara u upotrebu kako u kućnim tako i u poslovnim uslovima donelo je olakšanja brojnim korisnicima računara. Računari su prevashodno osmišljeni da pomognu današnjem čoveku maltene u svim sverama života. Ipak postoje i kriminalne radnje koje se vrše putem računara. Prevashodno zbog takvih neželjenih radnji stvorena je nauka koju zovemo Digitalna Forenzika. Ova nauka nije prisutna samo zbog kriminalnih radnji povezanih sa IT sektorom već i zbog gubitka određenih podataka tj. informacija koje su nam bitne.

Termin digitalna forenzika ljudi obično prihvate kao forezniku računara ali kada se malo bolje zapitamo danas smo okruženi raznovrsnim računarima, tako da ona obuhvata sve uređaje koji imaju mogućnosti skladištenja podataka. Digitalna forenzika je počela da se razvija podjednako sa razvojem računara što je mogućnost računara rasla tako je i potreba i mogućnosti forenzike nad njima bila sve veća.

Razvoj je počeo krajem sedamdesetih godina prošloga veka i ozbiljniji rast je dostigao devedesetih godina sa visokom stopom zastupljenosti računara. Novi vek je samo pokazao da digitalna forenzika ima konstantnu potrebu razvoja i prilagođavanja mogućnostima današnjih računara.

Nova nauka koja obuhvata oporavak ili povraćaj izgubljenih podataka kao i njihovu istragu zove se Digitalna Forenzika. Termin ove nauke je izmenjen u početku se zvala kompjuterska forenzika zbog njene uloge koja je prevashodno bila da se koristi na računarima. Ipak promena termina je usledila iz razloga što se ova nauka može primeniti na svim uređajima koji imaju veze sa skladištenjem podataka.¹⁶

Uloga d. forenzike u istraživanju podataka ima raznovrsnu korist. Najčešće se koristi kao podrška u vidu elektronskog otkrivanja informacija odnosno tragova i pomoći sudovima u rešavanju sudskih procesa. Takođe d. forenzika ima ulogu kod unutrašnjih istraga kod raznih kompanija.

Uobičajen forenzički proces sastoji se od zaplene tj. oduzimanja uređaja, forenzičkog snimanja i analize digitalnog sadržaja kao i pravljenja izveštaja o prikupljenim dokazima

Tehnički gledano d. forenzika se deli na nekoliko grana i to u zavisnosti o kakvim i nad kakvim se uređajima vrše ispitivanja.

¹⁶ International Journal of Digital Evidence. M Reith, C Carr, G Gunsch.

Imamo računarska forenziku, mrežnu forenziku, forenziku analize podataka i forenziku mobilnih uređaja.

8.1 Digitalni dokaz

Digitalni dokaz ili dokaz u elektronskom obliku predstavlja skup podataka koji se nalaze ili prenose u digitalnom obliku i kao takav se koristi u sudskim procesima. Pre samog korišćenja dokaza on se mora proveriti da li je validan tj. da li je autentičan kao i da li je potreban original ili kopija datog dokaza.¹⁷

Upotreba digitalnog dokaza je znatno povećana u poslednje dve decenije ona se proširila na forenzičke analize i pribavljanje dokaza iz elektronskih pošta, digitalnih fotografija, tekstualnih dokumenata, baza podataka, memorija računara i drugih.¹⁸

U Velikoj Britaniji postoje uputstva za proveru identiteta i integriteta digitalnih dokaza. Ovakva uputstva postaju značajna zbog daljeg toka istrage i sigurnosti digitalnih dokaza i sastoje se iz sledećih tačaka:¹⁹

- Lica koja su angažovana od strane agencije koja sprovodi istragu ne smeju da vrše bilo kakve promene na podacima jer su oni neophodni kao originali na sudu tj. u procesu suđenja.
- Slučaj kada se treba pristupiti originalnim podacima, ta osoba koja ima takvo ovlašćenje mora biti kompetentna da i to učini kao i da objasni dati dokazni materijal, njegov značaj i posledice.
- Potrebno je načiniti rezervnu kopiju svih procesa koji su primenjeni nad digitalnim dokazom i sačuvati istu. Pored kopije potrebno je uključiti nezavisnu(treću) stranu koja će takođe imati priliku da odradi istraživanje digitalnih dokaza. Nezavisna strana treba da dođe do istih rezultata istraživanja kao i istražni organi.
- Osoba koja je zadužena za istragu preuzima potpunu odgovornost da se prilikom istražnih radnji sprovode važeći zakoni i principi.

¹⁷ Eogan Casey, „Digital Evidence and Computer Crime“.

¹⁸ Eoghan Casey, ed. „Handbook of Digital Forensics and Investigation“. Academic Press. September 2010.

¹⁹ Pollitt, MM. „Report on digital evidence“.

8.2 Forenzika mobilnih uređaja

Forenzika mobilnih uređaja kao što joj i ime govori bavi se forenzičkim radnjama nad podacima u mobilnim uređajima. Razlikuje se od forenzike računara upravo zbog toga što mobilni uređaji imaju ugrađene komunikacione sisteme kao što su GSM(Global System for Mobile Communications) kao i skladišne uređaje koji mogu biti nezavisni i lako uklonjivi. Istrage u ovim slučajevima se baziraju prevashodno na podacima o pozivima kao i raznovrsnim komunikacijama putem poruka. Mobilni uređaji danas imaju ugrađene GPS senzore tako da omogućavaju forenzičarima da saznaju lokacije kretanja.²⁰



Slika 16: Forenzika mobilnih uređaja

Upotreba mobilnih telefona u kriminalnim radnjama je učestala ali forenzika mobilnih uređaja je relativno novijeg datuma. Pojava pametnih telefona na tržištu izazvala je potrebu za forenzičkim ispitivanjima nad ovim uređajima. Mobilni uređaji mogu da skladište razne podatke kao što su kontakti, slike, notesi, sms, mms...

Pametni telefoni mogu takođe da sadrže i video sadržaje, email kao i informacije o kretanju po internetu(socijalne mreže danas jako zastupljene).

Počeci ispitivanja mobilnih uređaja bili su slični forenzičkom istraživanju računara i sadržalo se od analiziranja samog sadržaja mobilnog uređaja preko ekrana i fotografisanjem bitnog sadržaja. Ovaj način istraživanja pokazao se kao ne efikasan zbog vremena trajanja samog istraživanja koje je bilo dugo. Vremenom kako se broj mobilnih uređaja povećavao javila se potreba za efikasnijim rešenjem za izvlačenje podataka. Istraživači su počeli da koriste softver za sinhronizaciju i „back up“ podataka sa mobilnih

²⁰ Murphy, Cynthia. „Cellular Phone Evidence Data Extraction and Documentation“

uređaja radi slikanja („imaging“) stanja. Ovakvi softveri su mogli da vrše upis u uređaje ali i ispis podataka ali nisu imali mogućnost povraćaja izbrisanih podataka.

Forenzičari su uspeli da izvuku podatke koji su prethodno izbrisani uz pomoć „Flasher“ i „Twister“ kutija, ovaj alat je razvijen za fleševanje memorije mobilnog uređaja radi otklanjanje grešaka u softveru i obnove istog. Problem je u tome što su ove „kutije“ promenjive i mogu da promene same podatke i komplikovane su za korišćenje jer pre svega nisu namenjene za forenzičko istraživanje.

Vremenom razvili su se softveri za povraćaj „izgubljenih“ podataka sa mobilnih uređaja. Komercijalne verzije softvera su automatizovane tako da je olakšao proces ljudima koji su početnici u ovoj oblasti.

8.3 Računarska forenzika

Računarska forenzika predstavlja trenutno stanje digitalnog sistema kao što je računarski, uređaja za skladištenje podataka kao i elektronskih dokumenata. Ovaj ogranak pokriva računare, sisteme sa elementarnim računarskim procesima i ugrađene memorije kao i statične memorije (USB fleš memorije). Računarska forenzika ima širok spektar u pogledu informacija koje koristi. Ova forenzika koristi razne podatke kao što su istorije pregledača (browsera) pa sve do trajnijih podataka zapisanih na diskovima.

Ranih osamdesetih godina računari postaju dostupni civilnim korisnicima a samim tim raste upotreba računara u kriminalnim radnjama. Ova grana forenzike počinje da se upotrebljava baš od tih godina i njena svrha je prikupljanje digitalnih dokaza za korišćenje u sudskim procesima. Porast kriminalnih radnji u računarskom sektoru u konstantnom je porastu. Samo porast stope kriminalnih radnji izvršenih preko računara između 2002. godine i 2003. godine iznosila je 67%.

Danas ova nauka se bavi istraživanjem raznovrsnih kriminalnih radnji koje su vezane za računar, najčešće se koristi u oblastima dečije pornografije, špijunskih radnji, prevara, rešavanju težih slučajeva kao što su ubistva i silovanja.

Sam proces prikupljanja podataka može se opisati na sledeći način:

Dolazimo do hardvera i pravimo njemu sliku odnosno kopiju koju treba analizirati. Tokom analize forenzičar koristi povraćene podatke uz pomoć različitih softvera kao što su EnCase, ILOOKIX, FTK i drugi.

Vrsta podataka koji se ispituju može zavisi od slučaja na kome se radi ali najčešće su to email servisi, programi komunikacije preko poruka (Skype, Messenger), slike, istorija pregledača kao i različiti dokumenti. Ovakvi podaci se mogu povratiti iz hard diska (slobodno mesto HDD-a), obrisno mesto na disku kao i iz keš fajlova operativnog sistema.

Tipovi oporavka podataka su raznovrsni ali obično se zasnivaju na principu pretrage ključnih reči u okviru slike podataka (kopije sadržaja skladišnog uređaja). Određeni fajlovi imaju specifičan set bitova na kraju i početku samog fajla koji mogu da posluže za lakši povratak podataka ukoliko su obrisani. Forenzički alati su upravo bazirani na tom sistemu da otkriju tražene datoteke ali i da prepoznaju već poznate datoteke.²¹

Na većini uređaja za skladištenje podataka uključujući i HDD uređaje, kada jednom obrišemo podatke opcijom (Secure Delete) podatke nećemo uspeti povratiti. Nakon uspešnog povratka podataka određene informacije se analiziraju i samim tim rekonstruišu određene događaje i aktivnosti koje su rađene na računaru. Forenzičari koji se bave računarima (digitalni forenzičari) u kriminalnim istragama moraju da budu sigurni u zaključke koje su doneli na osnovu stečenih informacija i svog znanja.

8.4 Mrežna forenzika

Mrežna forenzika predstavlja granu digitalne forenzike koja je usmerena ka nadgledanju i analiziranju mrežnog saobraćaja pri računarima za potrebu prikupljanja informacija, legalnih dokaza kao i za otkrivanje upada u računarske sisteme mrežnim putem. Razlika mrežne forenzike i drugih ogranaka digitalne forenzike je u tome što se mrežna forenzika bavi podacima koji su ne postojani i dinamični. Mrežni saobraćaj može biti u jednom trenutku aktivan a u sledećem prekinut tako da mrežna forenzika predstavlja proaktivnu istragu.

Mrežna forenzika ima dve vrste upotrebe, prva je da se ona fokusira na bezbednost što podrazumeva praćenje mrežnog saobraćaja i uočavanja upada. Potencijalni napadač je u mogućnosti da obriše sve log fajlove na određenom hostu stoga dokaz prikupljen putem mrežne forenzike može biti jedini dokaz za forenzičku analizu²².

²¹ „Technology Crime Investigation“ Marten Van Horenbeec. 17. August 2010.

²² Erik Hjelmvik „Passive Network Security Analysis with NetworkMiner

Druga vrsta upotrebe je povezana sa sprovođenjem zakona u slučajevima gde se analizira već uhvaćen mrežni saobraćaj u kome se mogu nalaziti prenošeni podaci putem mreže, razne vrste pretraga, e-mejlovi i druge popularni društveni programi i četovi.

Dva sistema koja se koriste za prikupljanje podataka su sistemi pod nazivima „Catch is as you can“ i „Stop look listen“.

Prvi navedeni metod je zasnovan na tome da se zadržavaju svi podaci određenog mrežnog saobraćaja gde se njihova analiza radi naknadno. Ovakav metod zahteva velike količine skladišnog prostora.

Drugi metod je zasnovan na sistemu analize u kome se samo pojedini podaci čuvaju za naknadnu analizu. Ovakav metod zahteva jake procesorske jedinice zbog nadolazećeg mrežnog saobraćaja.

Eternet predstavlja važan segment mrežne forenzike gde se istraživanje vrši na takozvanim „bitnim potocima“. Istraživanje se vrši prisluškivačkim programima („sniffers“). Najčešći alat koji se koristi je „Wireshark“ koji prikuplja podatke i omogućava korisniku da ih filtrira. Putem ovog alata moguće je rekonstruisati veb sajtove, mejl podatke kao i druge razmene podataka. Prednost prikupljanja ovih podataka je u tome što ukoliko znamo IP i MAC adresu domaćina svi podaci koji se razmene sa ovom adresom mogu se filtrirati. Da bi se uspostavila veza između IP i MAC adresa potrebno je detaljnije pogledati pomoćne mrežne protokole. ARP(Address Resolution Protocol) poseduje listu MAC adresa sa odgovarajućim IP adresama. Radi prikupljanja podataka na ethernet nivou NIC(Network Interface Card) domaćina može se prebaciti u mod gde će se sav saobraćaj slati ka procesorskoj jedinici.

Ukoliko je napadač svestan da se njegova veza prisluškuje on može koristiti opcije šifrovanja(enkripcije) radi dodatne sigurnosti njegove konekcije. Danas je teško probiti šifrovane veze ali znajući da konekcija između napadača i nekog drugog hosta sve vreme šifrovana to nas može uputiti ka zaključku da je i drugi učesnik sumnjiv.

Na mrežnom nivou **IP**(Internet Protocol) je odgovoran za upravljanje paketima koji su generisani od strane **TCP**(Transmission Control Protocol) preko mreže. Radi pravilnog rutiranja(usmeravanja) svaki umreženi ruter mora da ima tabelu rutiranja da bi znao gde da pošalje podatke. Ove tabele za rutiranje su značajan izvor informacija ukoliko se istražuje mrežni prekršaj tj. zločin. Da bi se to uradilo moraju se pratiti paketi samog napadača, suprotna strana veze a samim time i naći računar od koga su potekli podaci. Na ovom nivou imamo i izvor u vidu dokaza o autentifikacionim logovima. Oni nam mogu

reći koji nalozi i koji korisnici su povezani sa određenom aktivnošću a samim time i otkriti napadača ili suziti listu osumnjičenih osoba.

Bežična forenzika predstavlja granu mrežne forenzike čija je svrha da obezbedi metode i alate potrebne za prikupljanje i analiziranje bežičnih mreža. Saobraćaj u bežičnim mrežama danas je u porastu u skladu sa porastom uređaja koji koriste ovaj vid prenosa podataka. Dokazi koji se prikupljaju su najčešće vezani za komunikacije putem VoIP servisa kao i socijalnih mreža. Analiza protoka podataka kod bežičnih mreža slična je i kao kod žičnih mreža uz dodatak sigurnosnih sistema koji su deo bežične mreže.

8.5 Forenzika baze podataka

Forenzika baza podataka je slična računarskoj forenzici, ona prati procese forenzičke istrage kao i primene istražnih tehnika nad bazama podataka. Forenzička ispitivanja baza podataka mogu se uporediti sa vremenskim markicama koje su vezane za vreme upisa određene kolone u tabeli relacija. Takođe istraživanja se mogu fokusirati na utvrđivanje transakcija u okviru sistema baze podataka ili aplikacija koje ukazuju na grešku ili moguću prevaru. Softverski alati obezbeđuju analizu podataka ali i reviziju logovanja čime obezbeđuju dokaz o radnjama koje ispitivač radi u bazama podataka²³. Postoji dosta softverskih rešenja za forenziku baza podataka ali oni nisu toliko pouzdani. Forenzička ispitivanja vezana za baze podataka zahtevaju poznavanje standarda za kodiranje na disk računara. Danas aktuelni programi za korišćenje i programiranje baza podataka su SQL Server i Oracle²⁴.

²³ Oracle Database Forensics using LogMiner-GIAC Certified Student Practical

²⁴ „SANS Institute“ –Forensic Analysis od a SQL Server 2005 Database Server

8.6 Forenzički alati

U početku digitalna forenzika se svodila na analizu medija tj. ispitivanje računara unutar operativnog sistema koristeći sistem-administrator alatke i na taj način izvlačili podatke. Ova vrsta analize nosi određene rizike promene podataka na disku. Zbog toga tek su devedesetih godina razvijeni alati koji prevazilaze ove probleme.

Potreba za unapređenim softverom prepoznata je krajem osamdesetih i stvoreni su sistemi za policiju IMDUMP od strane Michael White-a i program Safe Back koji je kreirala kompanija Sydex.

Slični softveri su razvijani u mnogim državama, tako je 1991. godine u Velikoj Britaniji u upotrebu ušao softversko-hardversko rešenje DIBS.



Slika 17 : DIBS radna stanica

Ovakvi alati dozvoljavaju digitalnim forenzičarima da stvore tačnu kopiju određenog medija koji je pod istragom i da nastave sa radom bez diranja originalnog medija. Krajem devedesetih razvijaju se napredniji sistemi za digitalnu forenziku kao što su „EnCase“ i „FTK“. Skoriye je razvijen alat pod imenom WindowsSCOPE. Za mobilne uređaje su razvijeni softverski alati pod nazivom „XRY“ i „Radio Tactics Aceso“.

Naziv	Platforma	Opis:
Lantern(Katana Forensics)	Apple	Koristi preciznu bitsku sliku iOS uređaja
Cellebrite Mobile Forensics	Windows	Univerzalni forenzički alat softver-hardver
Secure View Mobile Forensics Software	Windows	Hardver-softver
Radio Tactics Aceso	Windows	Uređaj stanica sa ekranom osjetljivim na dodir
Parabean Device Seizure	Windows	Hardver-softver

MicroSystemation XRY/XACT	Windows	Hardver-sofver specijalizovan za obrisane podatke.
Oxygen Forensic Suite	Windows	Alat za pametne telefone.

Tabela 4 : Forenzički alati za mobilne uređaje²⁵

Naziv	Platforma	Opis:
Elcomsoft iOS Forensic Toolkit	Windows, Mac	Radi sa bitskom slikom Apple iOS uređaja u realnom vremenu.
Elcomsoft Phone Password Breaker	Windows	Omogućava ulazak u bekap fajlove koji su zaštićeni lozinkom na BlackBerry i Apple platformama.
MOBILedit! Forensic	Windows	Hardver konekcioni kit i sofver.
Mobile Phone Examiner Plus	Windows	Hardver-sofver za pametne telefone.

Tabela 4 : Forenzički alati za mobilne uređaje

U nastavku je prikazana tabela sa nazivom i opisom forenzičkih alata koji se koriste na računarima.

Naziv	Platforma	Opis:
ILookIX Perlustro	Windows	Prvi forenzički alat korišćen od strane policije.
Parabean P2 Commander	Windows	Višenamenski forenzički alat, posebno se koristi za imejl analizu.
SANS Investigative Forensics Toolkit	Ubuntu	Višenamenski forenzički alat.
CAINE	Linux	Gnu/Linux forenzički alat.
Registry Recon	Windows	Alat koji oporavlja vindowsove registre i vrši njihovu analizu.
EnCase	Windows	Višenamenski forenzički alat.
EPRB	Windows	Alat za šifrovane sisteme i za dešifrovanje i pronalaženje lozinki.
Digital Forensics Framework	Unix/Windows	Grafički interfejs .
Forensic Explorer	Windows	Višenamenski računarski forenzički alat.
FTK	Windows	Višenamenski alat često korišćen za medije.

²⁵ Mislan Richard, „Creating laboratories for undergradate courses in mobile forensics“ 2010. ACM conference on information technology education.

PTK Forensics	LAMP	Grafički interfejs za Sleuth Kit.
The Coroners Toolkit	Unix	Unix analiza.
COFEE	Windows	Organi reda imaju pristup ovom softveru.
The Sleuth Kit	Unix-Windows	Biblioteka alata za obe vrste operativnih sistema.

Tabela 5 : Forenzički alati za računare

Naziv	Platforma	Opis:
Categoriser 4 Pictures	Windows	Organi reda, organizacija slika.
Open Computer Forensics Architecture	Linux	Forenzički alat za CF-Lab okruženje.
SafeBack	/	Bekap
Track Inspector	Unix	Forenzički alat nije za tehničku istragu.
Windows To Go	/	Botabilni operativni sistem
Wireshark	/	Open-source paket koristi biblioteku [win]pcap.
X-Ways Forensics	Windows	Višenamenski forenzički alat.
Nuix/ Proof Finder	Windows	Forenzička analiza i softver za prevenciju prevara.
Netherlands Forensic Institute/Xiraf	/	Forenzički alat za onlajn servise.

Tabela 5 : Forenzički alati za računare

9. Forenzička analiza SSD-a ?

Poznajući SSD uređaje i način na koji oni čuvaju podatke ostavlja nam malo prostora za pozitivno mišljenje o forenzičkoj analizi ovih uređaja. Sigurno je jedno da forenzičar može pristupiti podacima na SSD-u ukoliko oni postoje na istom. Podaci koje sumnjivo lice obriše sa uređaja u nameri da ih se reši naprimer formatiranjem mogu biti izgubljeni zauvek čak i u opciji brzog formatiranja. Podaci će biti izgubljeni čak i ukoliko se računar odmah isključi sa napajanja nakon komande formatiranja posle svega par minuta podaci su izgubljeni i ukoliko opet uključimo računar ne postoji način da se stopira brisanje podataka sa SSD-a. Doba razvoja digitalne forenzike polako zastaje s obzirom na brzinu razvoja SSD memorije i tehnologije kontrolora. Danas je sve više proizvođača SSD uređaja samim tim imamo i zdravu konkurenciju u proizvodnji i napredak ove tehnologije koja ne ide u prilog digitalnim forenzičarima.

Naučnik sa Australijskog Murdok Univerziteta je napisao „Izgleda da se zlatno doba forenzičkog oporavka i analize obrisanih podataka i obrisanih metapodataka bliži kraju“²⁶

9.1 Brisanje nije moguće

Konstrukcija SSD uređaja ispoljava ograničenja koja su prisutna u ovim uređajima. Postojeće vrste fleš memorije dozvoljavaju ograničen broj upisa podataka. Moderni SSD uređaji poseduju određene tehnike koje pomažu ponovnoj upotrebi postojećih blokova memorije. Podaci se pišu u narednom bloku memorije dok se trenutni blok modifikuje. Ovaj način skladištenja podataka ostavlja potencijalno osetljive podatke razbacane po memoriji uređaja.

Da bi se poboljšao radni vek i smanjilo habanje memorije na SSD-u mnogi proizvođači su ugradili čipove koji mogu da zadrže i do 25% više podataka u odnosu na predhodne verzije. Tu dodatnu količinu nije moguće adresirati od strane operativnog sistema. Ovo takođe čini sadržaj SSD uređaja nemogućim za sigurno brisanje po standardima. Da bi se ublažili problemi neki od proizvođača su ugradili ekstenzije za ATA ANSI specifikacije da bi omogućili sigurno brisanje informacija skladištenih na samoj memoriji.

²⁶ Solid State Drives: The Beginning of the End for Current Practice in Digital Forensic Recovery?
<http://www.jdfsl.org/subscriptions/JDFSL-V5N3-Bell.pdf>

ATA „Secure Erase“ komanda briše celokupan sadržaj uređaja na hardverskom nivou. Softveri za sigurno brisanje će prepisati podatke na samom uređaju²⁷. Međutim problem kod ovakvih softvera je u tome što nisu u mogućnosti da adresiraju a samim tim i da pristupe memoriji SSD-a.

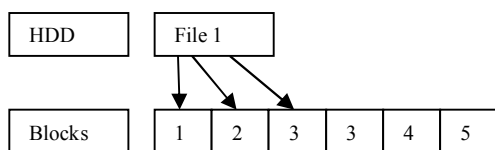
Za razliku od softverski baziranih alata ATA Secure Erase komanda nalaže već ugrađenom kontroleru u SSD uređaju da elektronski briše blokove na svim čipovima memorije za skladištenje podataka. Efektivno obrisani SSD memorije su čiste kompletno gde su svi blokovi prazni i spremni za upis. Ova komanda vraća SSD na fabrički nivo kao i njegove mogućnosti upisa.

9.2 Memorijski blokovi

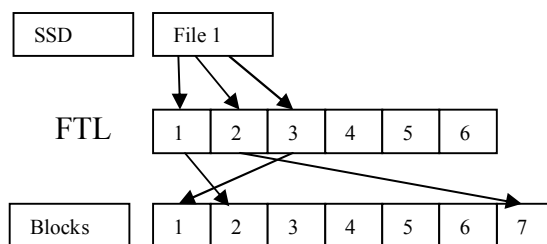
Termin SSD(Solid State Drive) znači da se podaci čuvaju u fiksno raspoređenim elektronskim tranzistorima. Ovi uređaji skladište podatke u 512KB blokovima koji su podeljeni na 4KB stranice koje se sastoje od velikih nizova NAND tranzistora. NAND „plivajuća kapija“ se koristi da zadrži električnu energiju princip je sličan kao kod kondenzatora. Ovo omogućava zadržavanje napajanja memorije i može da čuva podatke godinama bez naknadnog napajanja.

Prve generacije SSD uređaja su imale dva problema. Habanje odnosno kraći vek memorije i usporenje brzine prebacivanja podataka. Životni vek pojedinačnog memorijskog bloka je bila između 10 000-100 000 upisa pre otkazivanja. Zbog ovog ograničenja korišćena je šema koja je za cilj imala izbegavanje upisa podataka na jedno isto mesto u memorijskim blokovima. Ukoliko računar upisuje podatke u jedan blok konstantno onda SSD-ov Flash Translation Layer(FTL) brzo prebacuje podatke na drugo mesto koje je ređe korišćeno. Računar nije svestan da se podaci skladište na drugu poziciju ali ova metoda ipak usporava fizička oštećenja SSD uređaja. Ovaj proces je sličan procesu mapiranja grešaka kod HDD uređaja samo što se u slučaju SSD uređaja koriste skoro svi blokovi memorije. Zbog ovog procesa korisnik ne može da zna gde su tačno smešteni podaci na SSD uređaju. Kontroler SSD uređaja prati blokove i njihovu putanju koju procesuje FTL.

²⁷ Reliably Erasing Data From Flash-Based Solid State Drives
http://www.usenix.org/events/fast11/tech/full_papers/Wei.pdf



Slika 18 : HDD blokovi



Slika 19 : SSD blokovi

Usporeenje brzine prenosa u transveru podataka nastaje usled toga što fleš tehnologija zahteva brisanje u blokovima elektronski pre njihove ponovne upotrebe za razliku od prepisivanja podataka na magnetnom disku u HDD-u. Proces brisanja u SSD uređaju je drastično sporiji u odnosu na čitanje/pisanje. Iz tehničkih razloga ne brišu se samo određeni blokovi već cele stranice blokova. Ukoliko je SSD popunjen promena na jednom bajtu može uticati na ceo blok pri čitanju/pisanju ili prepisivanju i tako usporiti uređaj. Jedna procedura je dodata kontroleru SSD-a i ona se zove „Garbage Collection“ ona konstantno vrši analizu nekorišćeni prostor i resetuje ih čim je moguće. Ključni problem je to što SSD kontroler ne zna koji operativni sistem će se koristiti kao i da ne može biti siguran koji delovi memorije sadrže obrisane podatke a koji ne. Značajni podaci su određene fajl sistemima FAT32, NZFC, HFS+ ...

Kompanija Samsung kao jedan od većih proizvođača kontrolera odlučio je da razvije algoritam koji će raditi isključivo sa NTFS fajl sistemom. Ovaj algoritam bi trebalo da bude u mogućnosti da pretražuje zauzete i slobodne oblasti NTFS fajl sistema pregledajući slobodan prostor bitmape. Ovakvi SSD uređaji su sličniji računaru nego običnoj skladišnoj komponenti, oni reaguju na komande od strane računara ali i nekad preuzimaju sami inicijativu.

Moguće je da se neka od tehnologije Garbage Collection može aktivirati tokom fizičkog zarobljivanja, forenzičke analize ili validacije procesa u odsustvu pisanih komandi od strane računara. Ukoliko se ova procedura aktivira pre ili tokom forenzičkog „slikanja“ to bi rezultovalo do trajnog gubitka podataka. Ova mogućnost bi ostavila forenzičara bez dokaza, ovakav slučaj se zove i „Corrosion of evidence“.

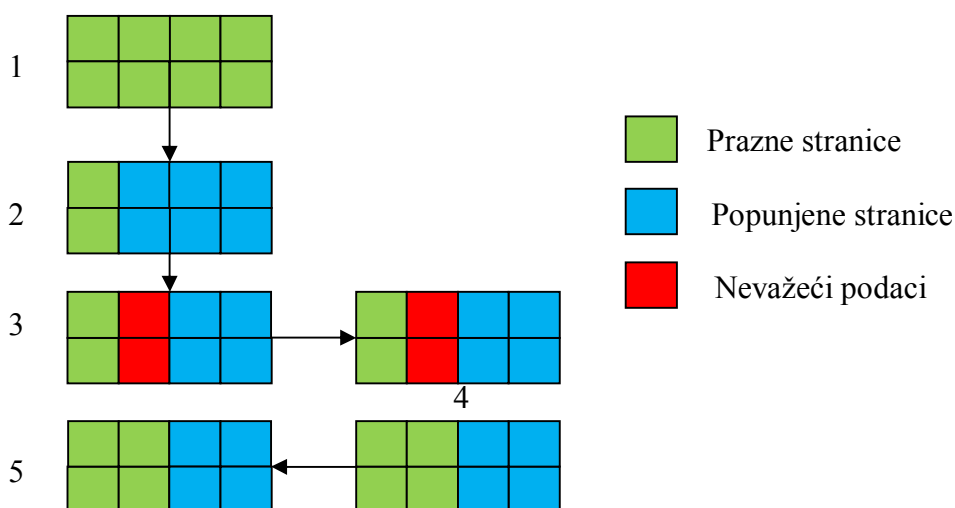
Svaka promena na disku nakon ili tokom izvlačenja podataka može da oteža validnost forenzičkog dokaza. Zamislimo situacija u kojoj bi se našao forenzički istražitelj koji prilikom slikanja(kopiranja) SSD-a. Nakon slikanja uređaj se priprema za validaciju u tom trenutku kontroleri odlučuju da sprovedu fazu „Garbage collection“ i tako brišu

određenu količinu podataka. Kada uporedimo kopiju podataka koju je napravio forenzičar sa originalnom kopijom čini se da je analiza odrađena sa valjanom kopijom ali da je pritom neko veštački dodao podatke. Ovi „dodaci“ su nastali od strane samog SSD-a tj. od kontrolnog čipa koji je modifikovao sadržinu SSD-a. Zbog ovakvog procesa gde nismo sigurni kada se komanda garbage collection odvija nemoguće je biti siguran da kopija koja je napravljena od strane forenzičara bude autentična stanju SSD-a u trenutku njegovog zaplenjivanja.²⁸

9.3 Trim metoda

Trim komanda omogućava operativnom sistemu da obavesti SSD uređaj koji blok podataka se više ne koristi i da se mogu obrisati. Ova opcija je prvi put predstavljena nakon pojave SSD uređaja i njihove pristupačnosti i tendencije da zamene HDD uređaje. Takozvano trimovanje omogućava SSD-u da rukuje sa garbage collection procesom i samim tim da ubrza upis podataka u blokove dakle ova opcija doprinosi performansama SSD-a.²⁹

Činjenica da se odbačeni blokovi u SSD-u odmah brišu nije tačna jer u TRIM opciji kada se aktivira ona razmatra sadržinu odbačenih blokova i stavlja ih u neodređen status do momenta kada ih neki drugi proces ne obriše kao što je garbage collector. Trim opcija ne briše blokove memorije već ih dodaje u vrstu nerešenih blokova gde će biti očišćeni od strane garbage collector-a.



Slika 20 : TRIM proces

²⁸ Lliadis, „Performance of the Greedy Garbage-Collection Scheme in Flash –Based Solid-State Drives“, Computer Science, 26.03. 2010.

²⁹ Shimpi, Anand Lal, „The SSD Anthology“ AnandTech.com 19.06.2010.

Na predhodnom grafiku je prikazan Trim proces:

1. SSD stranica bez podataka(prazni blokovi).
2. Korisnik upisuje podatke na SSD stranice.
3. Korisnik briše određene podatke (stranice označene da nisu u upotrebi od strane operativnog sistema ali podaci ostaju na SSD-u).
4. TRIM komanda govori SSD kontroleru da stranice sadrže nevažeće podatke, stranice sa takvim podacima se brišu.
5. Podaci se ponovo upisuju na SSD memorijske blokove. Nevažeći podaci su obrisani i podaci se mogu ponovo upisati na memorijske stranice.³⁰

Nemogućnost oporavka podataka ne važi u slučaju ako je TRIM komanda ostala neizvršena. U ovom slučaju podaci sa SSD uređaja se mogu povratiti sličnim metodama kao i kod HDD uređaja.

U sledećim slučajevima TRIM protokol je onemogućen za izvršavanje svog zadatka :

- Starije verzije ne podržavaju TRIM komandu.
- U operativnim sistemima tipa Windows se isto javlja problem u vidu prisutnosti ove opcije operativni sistemi počevši od Windows Vista i prethodni nemaju mogućnost TRIM-a.
- Verzije MacOS X su počele sa podrškom TRIM komandi. Apple koristi posebne SSD uređaje za svoj sistem, ostali SSD uređaji ne bi imali mogućnost TRIM-a.
- Samo NTFS formatiranje particija je uključeno u potpunu podršku TRIM opcije kod Windows-a.
- TRIM opcija nije moguća da se sprovodi ukoliko je SSD uređaj priključen preko USB-a. Ova komanda se sprovodi samo preko SATA, eSATA, SCSI standarda.
- Konekcija SSD uređaja preko PCI Express slota ne podržava TRIM funkciju (ovo važi za sve verzije Windows operativnih sistema).
- Opcija TRIM-a takođe nije moguća ni preko RAID tehnologije.
- Kod korumpiranih delova memorije (Logical corruption) Trim se ne izvršava jer te oblasti nisu obrisane na pravi način i one su nevidljive ili nisu prihvatljive za operativni sistem.

³⁰ <http://www.corsair.com/us/blog/how-to-check-that-trim-is-active/>

10. Zaključak

Tematika SSD i HDD uređaja njihovo poređenje i zastupljenost relativno je zastupljena u segmentu hardvera računara. Skladištenje podataka danas nudi kupcima računara odlične performanse kao i izbor tehnologije koju će izabrati za svoj računar. Pored dugogodišnje vladavine HDD uređaja na tržištu pojavila se tehnologija koja je odavno otkrivena ali njene mogućnosti su tek skorije razvijene i predstavljene tržištu. Birati između SSD i HDD tehnologije danas omogućava kupcu izbor koji pre nije imao. Nije moguće odbaciti HDD uređaje i zameniti ih SSD uređajima trenutno, takav proces zahteva određen vremenski period koji čak nije ni 100% siguran upravo iz razloga konstantnog razvoja HDD uređaja. U predhodnim stranicama uporedili smo ove dve tehnologije ali razvoj je i dalje prisutan u oba slučaja. Ključnu igru predstavlja i cena koja je trenutno u koristi starije tehnologije. Cena uređaja je u predhodnim vremenima pokazala ma koliko konkurentan uređaj bio po kvalitetu ako nije konkurentan po ceni vrlo je moguće da je isti osuđen na propast. U slučaju SSD uređaja to nije slučaj jer su relativno novi na tržištu a i tendencija opadanja same cene uređaja je primetna.

Postoje tendencije da se nastavi sa razvijanjem uređaja sa obe tehnologije(hibridna tehnologija) u jednoj jedinici čime bi se iskoristile najbolje strane obe tehnologije. Ova tehnologija je prisutna na tržištu najviše kod prenosnih računara. HDD uređajima daju nadu i novi materijali koji su u planu za proizvodnju ploča na hard diskovima čime bi se znatno povećale kapacitativne vrednosti ovih uređaja.

Digitalna forenzika danas i u budućnosti ima siguran opstanak, to što iz predhodno navedenog teksta zaključujemo da ljudi koji se bave istraživanjem digitalnih podataka ne čeka ni malo lak posao i da su im postavljeni visoki zadaci ne treba da nas brine. Razvoj tehnologije u ovom slučaju SSD uređaja i njihove manipulacije podacima predstavlja korak napred u pogledu razvoja tehnologija za skladištenje podataka. Nikako ne treba zaboraviti da je ova tehnologija u skorijem vremenskom periodu ušla u masovniju upotrebu i da joj sledi određen vremenski period razvoja a samim tim i poboljšanja.

Razvojem novih tehnologija i poboljšanjem već prisutnih samo će pokrenuti neophodni razvoj i forenzičkih alata za ove tehnologije. Kao što je i SSD tehnologija pa i ostale prvo dobila šansu razvoja u vojnim i bezbednosnim sektorima država tako se i alati za digitalno forenzičke alate podjednako razvijaju jer to je neraskidiva sprega borbe očuvanja i dostupnosti određenih informacija.

11.Literatura

- [1]. Whyte Barry, „A brief History of Areal Density“ . IBM DeveloperWorks.
- [2]. „Magnetic head development“. IBM Archives.
- [3]. „The History Of The Hard Drive And Its Future” . www.crn.com
- [4]. „Storage Solutions Guide”. Seagate October 2012.
- [5]. „Investigation: Is your SSD more reliable then a hard drive?”. Toms Hardware.
- [6]. „3,5 vs 2,5 SAS HDDs: In Storage, Size Matters”. Schmid, Patrick and Achim Roos.
- [7]. Report: TDK Technology „More Than Doubles Capacity of HDDs”.
- [8]. Lifehacker.com „The Complete Guide to Solid-State Drives”.
- [9]. „The Difference Between SSD and Flash Hard Drives”. danielmiessler.com
- [10]. „The Top SSD Companies” . www.storagesearch.com
- [11]. „Market Share of SSD Suppliers in 2014-Trendfocus”. www.storagenewsletter.com
- [12] Wilding E. „Computer Evidence: a Forensic Investigations Handbook. London Sweet & Maxwell.
- [13] „Best practice for Computer Forensics“ SWGDE – 20.08.2010.
- [14] „Electronic Crime Science Investigation Guide: A Guide for First Responders” National institute of Justice, 2001.
- [15] Marten Von Horenbeeck „Technology Crime Investigation” , 24.05.2006.
- [16] Olivier, Martin S „On metadata context in Database Forensics” Avgust 2010.
- [17] „Electronic Evidence Guide” Council of Europe. April 2013.
- [18] Belkasoft Evidence Center 2012 , <http://forensic.belkasoft.com/en/bec/Carving.asp>
- [19] Intel SSD, TRIM support, <http://www.intel.com/support/ssdc/hpssd/sb/CS-031846.htm>
- [20] SSD Forensics, [http://www.forensicswiki.org/wiki/Solid_State_Drive_\(SSD\)_Forensics](http://www.forensicswiki.org/wiki/Solid_State_Drive_(SSD)_Forensics)
- [21] Mehling, H. „Solid State Drives Take Out Garbage”. Jun 2013.
- [22] Rent, M.T. „SSD Controller”. Maj 2013.

[23] Andy Herron (2013). „Advancements in Storage and File Systems in Windows 8.1". SNIA.

[24] Michael Label , „Linuks Kernel Finally Being Optimized For SSHDs". Phoronix. 29.10.2014.

[25] [www.pcworld.com/ ssds-vs-hard-drives-vs-hybrids-which-storage--tech-is-right-for-you-.html](http://www.pcworld.com/ssds-vs-hard-drives-vs-hybrids-which-storage-tech-is-right-for-you.html)

[26] „SSD vs HDD : A Beginners Guide to SSD Upgrades" , notebookreview.com

[27] International Journal od Digital Evidence. M Reith, C Carr, G Gunsch.

[28] Lliadis, „Performance of the Greedy Garbage-Collection Scheme in Flash –Based Solid-State Drives“ , Computer Science, 26.03. 2010.

[29] Shimpi, Anand Lal, „The SSD Anthology“ AnandTech.com 19.06.2010.

12.Spisak slika:

- Slika 1 : IBM 2311
- Slika 2 : IBM PC/XT
- Slika 3 : M2351A
- Slika 4 : Rodime HDD
- Slika 5 : Deskstar 7K1000
- Slika 6 : Fioka za Hdd
- Slika 7 : Eksterni HDD
- Slika 8 : Ploča unutar HDD-a
- Slika 9 : IDE standard za različite veličine HDD-a
- Slika 10 : SCSI konetkor HDD
- Slika 11 : PATA-SATA HDD
- Slika 12 : SATA konekcija
- Slika 13 : Anatomija SSD-a
- Slika 14 : Hibridni hard disk
- Slika 15 : Hibrid, HDD i SSD
- Slika 16 : Forenzika mobilnih uređaja
- Slika 17 : DIBS radna stanica
- Slika 18 : HDD blokovi
- Slika 19 : SSD blokovi
- Slika 20 : TRIM proces

13. Tabele i dijagrami :

Tabele:

- Tabela 1: Standardi
- Tabela 2 : Poređenje HDD-a i SSD-a
- Tabela 3 : Proizvođači i udeo u tržištu SSD uređaja
- Tabela 4 : Forenzički alati za mobilne uređaje
- Tabela 5 : Forenzički alati za računare

Dijagrami :

- Dijagram 1 : Udeo tržišta za 2013. godinu
- Dijagram 2 : Udruživanje kompanija
- Dijagram 3 : Instalacija softvera
- Dijagram 4 : Butovanje Windowsa 7 Os-a
- Dijagram 5 : Kopiranje fajlova
- Dijagram 6 : Otvaranje slike i softvera
- Dijagram 7 : Resetovanje i pokretanje 5 aplikacija
- Dijagram 8 : Multitasking
- Dijagram 9 : Trajanje baterije