



UNIVERZITET SINGIDUNUM
DEPARTMAN ZA POSLEDIPLOMSKE STUDIJE

MASTER STUDIJE

STUDIJSKI PROGRAM: SAVREMENE INFORMACIONE TEHNOLOGIJE

MASTER RAD

FORENZIČKA ANALIZA
WINDOWS NTFS FAJL SISTEMA

MENTOR:
doc. dr GOJKO GRUBOR

STUDENT:
dipl. inž. Gradimir Pantović
br. indeksa: M 9220/08

Sadržaj:

1 - METODOLOGIJA IZRADE MASTER RADA	7
1.1 - Uvodne napomene i obrazloženje rada	7
1.2 - Predmet rada	8
1.3 - Ciljevi istraživanja	8
1.4 - Hipotetički okvir istraživanja	9
- Opšta hipoteza	9
- Radne hipoteze	9
1.5 - Metode koje su primenjene u toku istraživanja	9
I - UVOD	10
1 - NTFS koncepcija	10
2 – Windows baza registara	10
2.1 – Definicija <i>Windows</i> baze registara	11
2.2 – Značaj ispitivanja <i>Windows</i> baze registara	11
2.3 – Istorija nastanka i razvoja <i>Windows</i> baze registara	11
3 – USB uređaji za skladištenje podataka	12
II - NTFS FAJL SISTEM	13
1 - Arhitektura NTFS fajl sistema	13
1.1 - Formatiranje NTFS particije	13
1.2 - NTFS Master File Table (MFT)	18
2 - Tipovi NTFS fajlova	20
2.1 - Atributi NTFS fajlova (<i>NTFS File Attributes</i>)	20
2.2 - NTFS sistemski fajlovi (<i>NTFS System Files</i>)	21
2.3 - NTFS višestruki tokovi podataka (<i>NTFS Multiple Data Streams</i>)	22
2.4 - NTFS komprimovani fajlovi (<i>NTFS Compressed Files</i>)	23
2.5 - NTFS šifrovani fajlovi (<i>NTFS Encrypted Files</i>)	23
2.6 - NTFS „šuplji“ fajlovi (<i>NTFS Sparse Files</i>)	25
3 - Skrivanje podataka u NTFS fajl sistemu	27
III – Forenzička analiza <i>Windows</i> baze registara	28
1 – Struktura <i>Windows 7</i> baze registara	28
1.1 – Funkcije <i>root key</i> segmenata	31
2 – Analiza operativnog sistema uz pomoć <i>Windows</i> baze registara	32
3 – Analiza aplikacija	36
3.1 – <i>Start up</i> programi	36
3.2 – Registrovane aplikacije	36
3.3 – Analiza aplikacije <i>Windows live messenger</i>	37
3.4 – Analiza aplikacije <i>Skype</i>	38

4 – Analiza mreže	39
4.1 – Mrežni adapteri	39
4.2 – Intranet mreže	39
4.3 – Bežične mreže	39
5 – Analiza priključnih uređaja	41
5.1 – Štampači	41
5.2 – USB uređaji	42
6 – Ispitivanje baze registara	43
6.1 – Registar kao dnevnik	43
6.2 – Autorun lokacije	43
6.3 – MRU liste	44
6.4 – UserAssist	45
6.5 – Liste istorije	46
7 – Značaj forenzičke analize <i>Windows</i> baze registara	47
IV – Forenzička analiza USB uređaja za skladištenje podataka	49
1 - Opis i karakteristike USB uređaja za skladištenje podataka	49
2 - USB uređaji za skladištenje podataka u <i>Windows</i> okruženju	54
2.1 - Prvo priključivanje USB uređaja za skladištenje podataka na računar sa <i>Windows</i> operativnim sistemom	54
2.2 - Program <i>USBDeview</i>	55
3 - Program za trajno brisanje podataka sa memorijskih uređaja <i>Active KillDisk</i> .	56
4 - Programi za oporavak obrisanih fajlova sa memorijskih USB uređaja	57
4.1 - <i>Recuva</i>	57
4.2 - <i>Pandora Recovery</i>	59
5 - Javno dostupni (besplatni) softverski alati za forenzičku istragu	60
5.1 - <i>AccessData FTK Imager</i>	60
5.2 - Forenzički softverski paket <i>OSForensics</i>	62
6 - Primer forenzičke analize USB fleš uređaja	64
6.1 - Priprema USB fleš uređaja	64
6.2 - Izrada forenzičke kopije USB fleš uređaja	65
6.3 - Oporavak obrisanih fajlova	69
6.4 - Smernice za dalji rad na forenzičkoj istazi USB fleš diska	70
V - ZAKLJUČAK	71
VI - LITERATURA	74

Slike:

Slika 1 - Arhitektura NTFS fajl sistema	14
Slika 2 - Struktura boot sektora NTFS fajl sistema	16
Slika 3 - Struktura MFT tabele	19
Slika 4 - Neimenovani i imenovani strimovi	22
Slika 5 - Postupak šifrovanja	24
Slika 6 - Postupak dešifrovanja	25
Slika 7 - Postupak oporavka kriptovanih podataka uz pomoć recovery agent-a	25
Slika 8 - Skladište sparse fajla	26
Slika 9 - Struktura Windows Registry baze	29
Slika 10 - Root keys Windows registra	29
Slika 11 - Veza izmedju root keys Windows Registra	30
Slika 12 - Promene u hive files operativnog sistema Windows	31
Slika 13 - Opis hardvera sistema unutar Windows Registry	33
Slika 14 - Opis centralnog procesora unutar Windows Registry	33
Slika 15 - Pojediniosti korisničkog naloga u Access Data Registry Viewer-u	34
Slika 16 - Imena korisničkih naloga unutar Windows Registry	35
Slika 17 - Prikaz brojne vrednosti vremena isključivanja računara u binarnom obliku u Windows Registry bazi	35
Slika 18 - Lista startup programa uz Windows Registry bazi	36
Slika 19 - Lista registrovanih aplikacija unutar Windows Registry	36
Slika 20 - Sadržaj UTL vrednosti	37
Slika 21 - Interesantne informacije Skajp aplikacije unutar Windows Registry	38
Slika 22 - Spajanje Identifikatora bežične mreže sa njemu odgovarajućim u okviru Windows Registry	40
Slika 23 - Datum kada je veza prvi put uspostavljena i datum poslednjeg povezivanja na bežičnu mrežu	40
Slika 24 - Konverzija DateCreated vrednost iz Registra u format big endian	41
Slika 25 - Značajni podaci o štampačima unutar Windows Registry	42
Slika 26 - Informacija o USB uređajima unutar Windows Registry	43
Slika 27 - RunMRU ključ	44
Slika 28 - UserAssist ključ	45
Slika 29 - Udeo koji USB uređaji za skladištenje podataka imaju u digitalnim forenzičkim istragama u odnosu na druge tipove uređaja za memorisanje podataka	49
Slika 30 - Izgled unutrašnjosti USB uređaja za skladištenje podataka	51
Slika 31 - Prikaz funkcionisanja FTL i MTD drajvera za dva tipa memorijskih uređaja	53
Slika 32 - Program USBDeview, prikaz podataka o USB uređajima na sistemu	55
Slika 33 - Izgled programa Active KillDisk	57
Slika 34 - Izgled programa Recuva	58
Slika 35 - Izgled programa Recuva u Advaced modu	59
Slika 36 - Izgled programa Pandora Recovery	60
Slika 37 - Program AccessData FTK imager	61
Slika 38 - Format forenzičkih kopija koje pravi program AccessData FTK imager	62
Slika 39 - Izgled programa OSForensics odmah po otvaranju	63
Slika 40 - Kopirani fajlovi i folderi na USB fleš disku	64
Slika 41 - Program OSForensics u toku izrade kopije USB diska	65
Slika 42 - Sadržaj fajla koji se generiše pri izradi forenzičke kopije diska	66

Slika 43 - Poređenje hash vrednosti USB diska i hash vrednosti njegove forenzičke kopije	67
Slika 44 - Opcije za mount-ovanje kopije diska na sistem	68
Slika 45 - Kopija USB diska postavljena kao virtualni disk na sistemu	68
Slika 46 - Rezultat pretrage USB diska programom Recuva	69
Slika 47 - Rezultati pretraživanja kopije USB diska programom Recuva u advanced modu	70

Tabele:

Tabela 1 - Formatirana NTFS particija	13
Tabela 2 - Arhitektura NTFS komponenata na x86-baziranom sistemu	14
Tabela 3 - NTFS Boot Sector	15
Tabela 4 - BIOS Parameter Block polja na NTFS logičkom disku	16
Tabela 5 - MFT zapis za male fajlove ili foldere	19
Tabela 6 - Atributi fajlova koji su definisani na NTFS fajl sistemu	20
Tabela 7 - Metapodaci u <i>Master File Table</i>	21
Tabela 8 - Opis polja <i>type</i> MSN objekta	37
Tabela 9 - Liste istorije	46

ABSTRACT:

Information technologies are the most powerful and most versatile technologies ever designed. These technologies have changed the way of life on the planet. They became indispensable in performing daily activities, shopping, voting, entertainment, fun ... This fact has led to the misuse of information technology for the purpose of attacks on privacy, data theft in the area of operations, attacks on information systems and carry out serious crimes.

The first and the second part of this paper covers the elements and principles of the NTFS file system and Windows Registry. The third part is dedicated to the USB storage devices in terms of digital forensic analysis.

The development of a USB flash memory devices has led to changing attitudes about where the digital evidence can be found. Recently there is great interest in investigating these types of digital devices. Continuous monitoring of innovations in this area contributes to a better acquisition of evidence from a USB flash device.

Keywords:

NTFS, Registry, USB flash drive, forensic

SAŽETAK:

Informacione tehnologije su najmoćnije i najprilagodljivije tehnologije koje su ikada smišljene. Ove tehnologije su promenile način života na celoj planeti time što su postale neizostavne u obavljanju svakodnevnog posla, kupovini, glasanju, zabavi, druženju... Ova činjenica je dovela do toga da se informacione tehnologije zloupotrebljavaju u svrhe napada na privatnost, krađe podataka u oblasti poslovanja, napada na informacione sisteme i vršenje teških krivičnih dela.

U prvom i drugom delu rada prikazuju se elementi i principi na kojima počiva NTFS fajl sistem i *Windows Registry*, jedna od esencijalnih komponenti *Microsoft Windows* operativnih sistema. Treći deo rada posvećen je razmatranju funkcionisanja USB uređaja za skladištenje podataka sa aspekta digitalne forenzičke analize.

Razvoj Usb fleš memorijskih uređaja doveo je do menjanja stavova o tome gde se sve digitalni dokaz može naći. U poslednje vreme dolazi do velikog interesovanja za digitalnu istragu ove vrste uređaja. Neprekidno praćenje noviteta u ovoj oblasti doprinosi boljoj akviziciji dokaza sa USB fleš uređaja.

Ključne reči:

NTFS, baza registara, USB flash drive, forenzika

METODOLOGIJA IZRADE MASTER RADA

1.1 Uvodne napomene i obrazloženje teme rada

Digitalna forenzika je nauka novijeg datuma koja je u kratkom vremenskom periodu zauzela visoko mesto u oblasti postupaka istrage i dokazivanja krivičnih dela kompjuterskog kriminala.

U prvom delu rada "Elementi NTFS fajl sistema operativnog sistema Microsoft Windows", prikazuju se elementi i principi na kojima počiva NTFS fajl sistem operativnog sistema Windows, uz nastojanje da se odrede bitni elementi sa aspekta digitalne forenzičke istrage.

Kako je operativni sistem MS Windows dominantan po broju instalacija na PC računarima u celom svetu, a ne postoji zvanična dokumentacija proizvođača o NTFS (izvorni kod poznat oko 30%) fajl sistemu, ukazuje se potreba za forenzičkim istraživanjem u toj oblasti.

U drugom delu rada "Analiza *Windows* baze registara", prikazuju se elementi i principi na kojima počiva *Windows registry* baza, uz nastojanje da se odrede elementi od velike važnosti sa aspekta digitalne forenzike.

Windows Registry je jedna od esencijalnih komponenti *Microsoft Windows* operativnih sistema. Sve što se dešava u *Windows* operativnom sistemu povezano je ili se nalazi u *Registry* bazi. Počev od *Windows 95* verzije operativnog sistema *Windows*, *Microsoft* je implementirao *Windows Registry* u svoje operativne sisteme. Odmah po implementaciji *Windows Registry* baze u operativni sistem *Windows* postalo je jasno da ona sadrži mnoge elemente od značaja za forenzičku istragu.

Treći deo rada „Forenzika USB memorijskih uređaja“ posvećen je razmatranju funkcionisanja USB uređaja za skladištenje podataka sa aspekta digitalne forenzičke analize.

USB uređaji za skladištenje podataka, tzv. fleš diskovi, su postali veoma čest, može se reći standardan uređaj za skladištenje različitih kategorija podataka u digitalnom obliku. Malih su dimenzija i samim tim pogodni za nošenje u tašni, džepu ili kao privezak za ključeve. Posmatrano sa drugog aspekta, lako ih je sakriti. Iz navedenog se može zaključiti da su ovi uređaji veoma pogodni kako za legalnu tako i ilegalnu upotrebu.

Kapacitet skladištenja podataka ovih uređaja omogućava skladištenje velike količine informacija tako da poznavanje načina funkcionisanja predstavlja imperativ u oblasti digitalne forenzike.

U ovom delu rada razmotreni su neki od mogućih pristupa digitalnoj forenzičkoj istrazi prenosnih USB uređaja za skladištenje podataka.

1.2. Predmet rada

NTFS (*New Technologies File System*) fajl sistem je podrazumevani fajl sistem operativnih sistema MS Windows NT generacije. Pošto je operativni sistem MS Windows na vodećoj poziciji po broju instalacija na PC računarima u odnosu na ostale operativne sisteme, to isto važi i za NTFS fajl sistem. U novije vreme NTFS fajl sistem postaje standard i u nekim UNIX operativnim sistemima.

NTFS je projektovan da obezbedi pouzdanost, visoki nivo bezbednosti i podršku za skladištenje velike količine podataka. Veoma značajna osobina ovog fajl sistema je visok stepen skalabilnosti, interna struktura podataka se može izmeniti i opet smestiti u fajl sistem, a osnova fajl sistema ostaje neizmenjena.

Dizajn NTFS fajl sistema podržava brzo i sigurno izvršavanje standardnih operacija kako što su čitanje, upisivanje, pretraga, kao i naprednih operacija kao što je oporavljanje fajl sistema na tvrdom disku veoma velikog kapaciteta.

Windows Registry je jedna od esencijalnih komponenti *Microsoft Windows* operativnih sistema. Tokom godina otkako je *Microsoft* implementirao *Windows Registry* u svoje operativne sisteme, postalo je jasno da on sadrži mnoge elemente od značaja za forenzičku istragu.

Za digitalnog forenzičara, veoma je bitno da zna šta je *Registry* baza, zašto postoji, kao i tipove informacija koje sadrži. Sve što se dešava u *Windows* operativnom sistemu povezano je ili se nalazi u *Registry* bazi.

USB uređaji za skladištenje podataka malih su dimenzija i imaju relativno veliki kapacitet skladištenja podataka koji neprestano raste sa napretkom tehnologije izrade ovih uređaja. Poznavanje načina funkcionisanja i metoda forenzičke istrage predstavlja važan segment znanja za svakog digitalnog forenzičara.

1.3. Ciljevi istraživanja

Naučni cilj je naučna deskripcija, analiza i razumevanje elemenata *Windows* fajl sistema, *Windows registry* baze i principa funkcionisanja i digitalne forenzičke istrage USB uređaja u *Windows* okruženju sa aspekta značaja za forenzičku analizu.

Društveni cilj je pružanje adekvatnih informacija i znanja onima koji žele da se bave forenzičkom analizom *MS Windows* operativnog sistema i njemu pripadajućih fajl sistema.

1.4. Hipotetički okvir istraživanja

Opšta hipoteza

- Svakim danom se uvećava upotreba interneta i personalnih računara u poslovne i privatne svrhe što kao posledicu ima povećan obim zloupotreba računara. Zloupotrebe vrše kako legalni korisnici tako i lica koja neovlašćeno pristupaju računarima bilo fizički bilo preko lokalne računarske mreže ili interneta. Pošto o gotovo svim aktivnostima na računaru postoji trajan ili privremen zapis koji se nalazi u fajl sistemu od velikog je značaja razumevanje rada tog sistema.

Radne hipoteze

- Operativni sistem *MS Windows* je dominantan operativni sistem u upotrebi na personalnim računarima te se ovim istraživanjem obuhvata veliki broj računara a samim tim i veliki broj potencijalnih izvršilaca raznih nelegalnih i kriminalnih dela.
- Digitalna forenzika, iako nauka novijeg datuma, ima veliki značaj kako pri utvrđivanju mogućih zloupotreba personalnih računara i uređaja koji se priključuju na personalne računare od strane samih korisnika tako i od strane neovlašćenih lica.

1.5. Metode koje su primenjene u toku istraživanja

- Interdisciplinarnost predmeta, ciljevi i hipotetički okvir istraživanja opredelili su nas na dijalektički pristup, upotrebu sinteze i osnovnih analitičkih metoda (indukcije i dedukcije), a od opšte naučnih hipotetičko deduktivne i komparativne metode.
- Kao tehnika prikupljanja podataka koristi se analiza sadržaja dokumenta na primarnom i sekundarnom nivou. Pregled literature i javno dostupnih sadržaja na internetu u oblasti operativnih sistema kao i njima pripadajućih fajl sistema i oblasti tehnologija funkcionisanja USB uređaja za skladištenje podataka.

I - UVOD

1 - NTFS koncepcija

Fajl sistem je zahtevani (obavezan) deo operativnog sistema koji određuje način imenovanja, memorisanja i organizacije fajlova na disku. Fajl sistem upravlja samim fajlovima, folderima i informacijama neophodnim za njihovo lociranje kao i lokalnim ili udaljenim korisničkim pristupom fajlovima.

NTFS (*New Technologies File System*) dizajniran je i proizveden od strane Microsoft-a i predstavlja podrazumevani fajl sistem za Microsoft Windows NT, Windows 2000, Windows XP, Windows Vista i Windows 7 operativne sisteme. Znatno je kompleksniji od svog prethodnika FAT fajl sistema, skalabilniji je i ima mnogo više mogućnosti.

NTFS projektovan je da obezbedi pouzdanost, visoki nivo bezbednosti i podršku za skladištenje velike količine podataka.

Skalabilnost je postignuta upotrebom generičke strukture koja obuhvata strukture podataka specifičnog konteksta. Ovakav dizajn je skalabilan, zato što se interna struktura podataka može nanovo izmeniti i opet smestiti u fajl sistem, a osnova fajl sistema će ostati neizmenjena. Jedan primer generičke strukture je da je svaki bajt u NTFS fajl sistemu alocirani u fajlu.

NTFS postaje standard i u nekim UNIX operativnim sistemima. Microsoft vrši dodatne izmene na NTFS fajl sistemu za svaku novu verziju Windows operativnog sistema.

Windows NT file system – NTFS (New Technology File System) obezbeđuje pouzdanost, kompatibilnost i performanse kakve se ne mogu naći kod njegovog prethodnika - *FAT* fajl sistema. Dizajniran je za brzo izvršavanje standardnih operacija poput čitanja, upisivanja, pretrage, i naprednih operacija kao što su oporavljanje fajl sistema na tvrdom disku veoma velikog kapaciteta.

2 - Windows baza registara

Iz same definicije jasno je da je cilj kompjuterske forenzike da nadje digitalni dokaz koji je prihvatljiv na sudu. Opšte je prihvaćeno da je kapacitet medija za skladištenje podataka u stanju stalnog rasta.

Kao posledica toga, pronalaženje digitalnog dokaza kriminalnog dela je vremenski zahtevno i sve više složeno. Jedan od načina da se taj proces učini bržim i jednostavnijim je traganje za dokazima na lokacijama za koje postoji velika verovatnoća da sadrže informaciju koja je od značaja za forenzičku istragu. Jedna od najpogodnijih lokacija da se počne istraga je *Windows* baza registara - *Windows Registry*.

Windows Registry je jedna od esencijalnih komponenti *Microsoft Windows* operativnih sistema.

Windows Registry ima dve namene koje su od kritične važnosti za operativni sistem *Windows*. Prva je to da se u njemu skladište podešavanja za *Windows* operativni sistem kao i podešavanja za aplikacije koje su instalirane na sistemu. Druga je to da je registar baza podataka sa podacima o instaliranom hardvera.

U ovom radu diskutuje se o nekoliko elemenata *Windows Registry* baze koji bi mogli biti od značaja za forenzičku istragu. Prvo je analizirana struktura *Windows Registry* baze, a zatim elementi unutar *Windows Registry* baze.

2.1 – Definicija *Windows* baze registara

Windows baza registara je definisana kao “Centralna hijerarhijska baza podataka korišćena u Microsoft *Windows* 98, *Windows* CE, *Windows* NT, korišćena da skladišti informacije koje su neophodne da se konfiguriše sistem za jednog ili više korisnika, aplikacije i uređaje hardvera.” (*Microsoft* kompjuterski rečnik, 2002.)

Napomena: Kod ove reference, uzima se potpuno isti pristup za *Windows* 2000, *Windows* XP, *Windows* Vista i *Windows* 7.

2.2 – Značaj analize *Windows* baze registara

Tokom godina otkako je *Microsoft* implementirao *Windows Registry* u svoje operativne sisteme, postalo je jasno da on sadrži mnoge elemente od značaja za forenzičku istragu.

Povećanom upotrebom računara i Interneta u svakodnevnom životu, pojavio se jedan novi, neizbežan fenomen, poznat kao kompjuterski kriminal. Kada se govori o kompjuterskom kriminalu, misli se na različite vrste zloupotreba, kao što su: pronevere (*fraud*), krađa identiteta (*identity theft*), prevare socijalnim inženjeringom (*phishing*), upad u mreže (*network infiltration*), DoS/DDoS napad, nelegalna distribucija zaštićenih materijala (*copyrighted*) i drugi tipovi napada sa Interneta i iz intranet mreža^[1].

U borbi protiv kompjuterskog ili kiber (*cyber*) kriminala, digitalna forenzička nauka je nezamenljiv alat. U digitalnoj forenzičkoj istrazi, veoma je važno da digitalni forenzičari imaju sva potrebna znanja o tome kako radi računarski sistem, mrežni uređaji i Internet servisi, kao i potrebne veštine da efektivno i efikasno sakupe sve neophodne digitalne dokaze na putu od računarskog sistema napadača do kompromitovanog računara^[6]. Da bi sve to mogli da urade, najvažnije je da dobro poznaju kako rade operativni sistem računara. *Registry* baza predstavlja srce *Microsoft Windows* operativnog sistema i u njoj je moguće pronaći i prikupiti veliku količinu forenzički relevantnih podataka^[7].

2.3 – Istorija nastanka i razvoja *Windows* baze registara

Za digitalnog forenzičara, veoma je bitno da na početku shvati šta je *Registry* baza, zašto postoji, kao i tipove informacija koje sadrži. Sve što se dešava u *Windows* operativnom sistemu povezano je ili se nalazi u *Registry* bazi. Program, koji se zove *RegMon*, firme *Sysinternals*, može se koristiti za praćenje aktivnosti *Registry* baze u realnom vremenu^[3]. Posle startovanja ovog programa, moguće je ispratiti sve akcije koje je korisnik preduzimao.

Što se tiče same definicije *Registry* baze, *Microsoft knowledge database* a takođe i *Microsoft Computer Dictionary*, definišu je kao: „Centralnu hijerarhijsku bazu podataka, koja se koristi u *Microsoft Windows9x*, *Windows CE*, *Windows NT*, *Windows2000*, *Windows 2003*, *Windows Vista* i *Windows 7*, za čuvanje neophodnih informacija za konfiguraciju sistema za jednog ili više korisnika, za aplikacije i hardverske uređaje“^[9].

Registry baza se prvi put pojavljuje u operativnom sistemu *Windows 95* i koristi se u svim novijim *Windows* operativnim sistemima. Bitno je naglasiti da se *Registry* baza neznatno razlikuje, u zavisnosti od verzije *Windows* operativnog sistema, ali da je struktura slična i da je njena funkcija svuda ista ^[2].

Pre pojave *Windows 95* operativnog sistema, za vreme *MS DOS*-a, *Registry* baza nije postojala, ali su se za istu namenu - konfiguraciju sistema, koristili fajlovi *config.sys* i *autoexec.bat*. Glavna namena *config.sys* fajla jeste učitavanje drajvera za određene hardverske uređaje (CD-ROM, sound card...) dok je namena *autoexec.bat* fajla, da se definišu radne promenljive okruženja (*environment variables*) i da se startuju neki programi, automatski po uključivanju računara, bez akcije korisnika. Međutim, to je prošlost, i u savremenim *Windows* operativnim sistemima te funkcije obavlja *Registry* baza. Bitno je reći da su inicijalni (*.ini*) fajlovi starih verzija *Windows* operativnog sistema, tipa *win.ini* i *system.ini*, koji su se u vreme *DOS*-a koristili za čuvanje parametara operativnog sistema, danas zamenjeni *Registry* bazom ^[2].

3. – USB uređaji za skladištenje podataka

Prenosivi USB uređaji za skladištenje podataka, za razliku od ostalih uređaja za skladištenje podataka, koriste poluprovodničku tehnologiju – čipove za čuvanje podataka. Imaju malu potrošnju energije i napajaju se preko USB priključka na računaru. Ova vrsta memorijkih čipova se naziva fleš (*flash*) memorijom. Otuda se za ovu vrsu uređaja odomaćio naziv - USB fleš.

Fleš memoriji nije potrebno električno napajanje da bi se sačuvali podaci. U idealnim uslovima trajnost upisa podataka je oko 10 godina.

Ovi uređaji su se masovno pojavili 2003 godine, početni kapacitet im je bio 16 megabajta i koristili su USB 1,0/1,1 interfejs. Od 2004 godine ovi uređaji koriste USB 2.0 interfejs koji ima maksimalnu brzinu protoka podataka od 480 Mb/s. Do današnjih dana kapacitet skladištenja podataka USB fleš uređaja drastično je porastao, do više desetina gigabajta.

Veliki kapacitet, male dimenzije, velika brzina čitanja i pisanja su učinili ovu vrstu uređaja veoma popularnom za skladištenje podataka, što ih čini veoma interesantnim u oblasti digitalne forenzike.

II - NTFS FAJL SISTEM

1 - Arhitektura NTFS fajl sistema

Bitan elemenat koncepta NTFS dizajna je da su važni podaci alocirani u fajlovima. Ovo uključuje i osnovne administrativne podatke, koji su tipično skriveni u drugim fajl sistemima. Fajlovi koji sadrže administrativne podatke mogu biti smešteni bilo gde na disku, kao i svi ostali fajlovi. Prema tome, NTFS nema poseban sloj za systemske podatke kao što ga imaju drugi fajl sistemi. Čitav fajl sistem je razmatran u oblasti podataka, a svi sektori mogu biti alocirani u fajlu. Jedini konzistentan sloj je prvi sektor jedinice diska, koji sadrži *boot sector* i *boot code*.

1.1 - Formatiranje NTFS particije

Rezultat formatiranja diska sa NTFS fajl sistemom je kreiranje nekoliko systemskih fajlova i MFT (*Master File Table*) tabele, koja sadrži informacije o svim fajlovima i folderima na NTFS logičkom disku.

Prva informacija na NTFS particiji je boot sektor logičkog diska (*Partition Boot Sector*), koji počinje od nultog sektora i može da bude velik do 16 sektora. Prvi fajl NTFS particije je MFT (*Master File Table*).

Prilikom formatiranja diska skladište se ključne NTFS strukture podataka. Tabela 1 ilustruje raspored NTFS logičkog diska nakon izvršenog formatiranja.

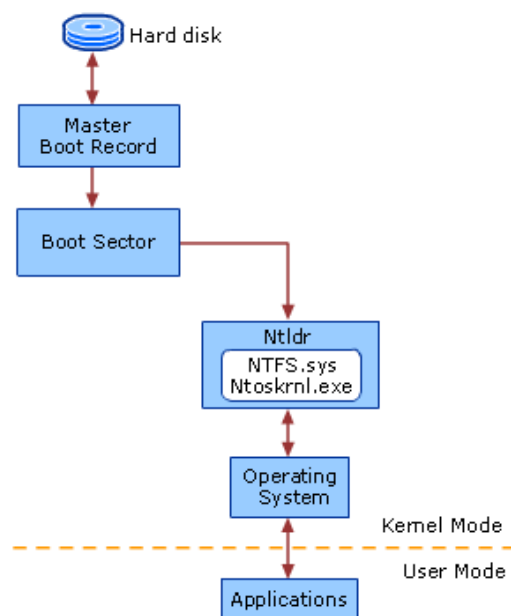
Tabela 1 - Formatirana NTFS particija ^[10]

Boot sektor particije	MFT tabela	Sistemske fajlovi	Oblast podataka
-----------------------	------------	-------------------	-----------------

Za vreme formatiranja i konfigurisanja fajl sistema logičkog diska na disku se kreira *master boot record* (MBR). MBR sadrži malu količinu izvršnog koda zvanog *master boot code* i *partition table* logičkog diska. Kada se logički disk pokrene, MBR izvršava *master boot code* sa odgovarajućeg sektora diska, što omogućava da računar učitava operativni sistem ukoliko se on nalazi na fajl sistemu tog diska. ^[10]

Partition table sadrži brojna polja za opisivanje particije. Jedan od ovih polja je *System ID* polje, koje definiše fajl sistem particije. Za NTFS diskove, system ID je 0x07. ^[10]

Arhitektura ovih procesa pod NTFS fajl sistemom prikazana je na slici 1, dok je u tabeli 2 dat opis komponenta NTFS fajl sistema.



Slika 1 - Arhitektura NTFS fajl sistema ^[1]

Tabela 2 - Arhitektura NTFS komponenata na x86-baziranom sistemu ^[10]

Komponenta	Opis komponente
Hard disk	Sadrži jednu ili više particija
Boot sector	Nalazi se na butabilnoj particiji i čuva informacije o rasporedu elemenata logičkog diska i strukturi fajl sistema, kao i <i>boot code</i> koji učitava Ntldr.
Master Boot Record (MBR)	Sadrži izvršni kôd kojeg sistemski <i>BIOS</i> učitava u memoriju. Kôd skenira <i>MBR</i> da nađe partition table za da bi odredio koja je aktivna primarna particija (butabilna particija).
Ntldr.dll	Prebacuje CPU u zaštićeni režim rada, pokreće fajl sistem, posle čega čita sadržaj <i>Boot.ini</i> fajla. Ova informacija određuje opcije pokretanja i inicijalne <i>boot menu</i> postavke.
Ntfs.sys	Sistemska drajver za NTFS.
Ntoskrnl.exe	Izvlači informacije o vrsti drajvera sistemskih uređaja za učitavanje i poredak učitavanja.
Kernel mode	Režim procesiranja koji omogućava kôdu direktan pristup svim hardverima i memoriji sistema.
User mode	Režim procesiranja u kojem rade korisničke aplikacije.

Tabela 3 opisuje boot sektor logičkog diska formatiranog NTFS fajl sistemom. Nakon formatiranja logičkog diska NTFS fajl sistemom, program za formatiranje alokira prvih 16 sektora za boot sektor i bootstrap kôd (programski kôd za pokretanje sistema).

Tabela 3 - NTFS Boot Sector ^[10]

Ofset bajta	Dužina polja	Naziv polja
0x00	3 bytes	Jump Instruction (komanda skoka)
0x03	LONGLONG	OEM ID
0x0B	25 bytes	BPB
0x24	48 bytes	Extended BPB
0x54	426 bytes	Bootstrap Code
0x01FE	WORD	End of Sector Marker

- Jump Instruction – komanda skoka
- OEM ID (*Original Equipement Manufacturer ID*) – identifikator proizvođača originalne opreme
- BPB – blok parametara BIOS-a

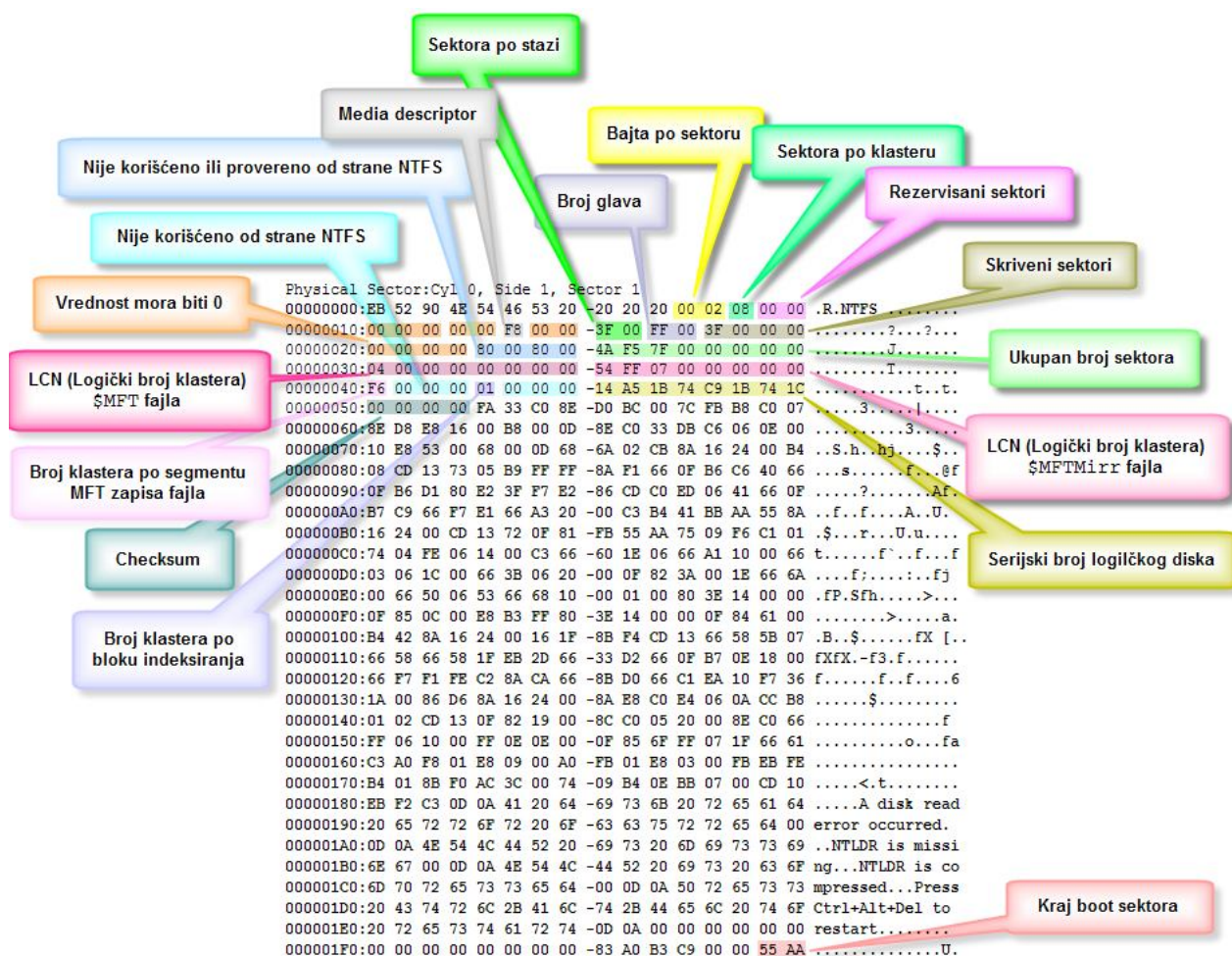
Na NTFS logičkom disku, polja podataka koja slede iza BPB (*BIOS parameter block*) formiraju prošireni BPB. Podaci u ovim poljima omogućavaju da Ntldr nađe MFT (*master file table*) za vreme podizanja sistema. Na NTFS diskovima, MFT nije lociran u predefinisane sektore. Ovo omogućava da NTFS, u slučaju da je sektor neispravan, premesti MFT na drugu lokaciju. Međutim, ako je podatak oštećen (*corrupted*), MFT ne može biti lociran i Windows pretpostavlja da logički disk nije formatiran. Sledeći primer ilustruje boot sektor na NTFS logičkom disku formatiranom korišćenjem Windowsa.

Rezultat formatiranja dat je u tri sekcije:

Bajtovi od 0x00 do 0x0A su instrukcije skoka i OEM ID.

Bajtovi 0x0B – 0x53 su BPB i prošireni BPB.

Preostali kôd je izvršni programski kôd za podizanje sistema (*bootstrap code*) i marker za kraj sektora (*end of sector marker*)



Slika 2 - Struktura boot sektora NTFS fajl sistema

U tabeli 4. opisana su polja BPB i proširenog BPB na NTFS logičkim diskovima. Polja od 0x0B, 0x0D, 0x15, 0x18, 0x1A i 0x1C poklapaju se sa poljima na FAT16 i FAT32 logičkim diskovima. Vrednosti odgovaraju podacima u ovom primeru.

Tabela 4. BIOS Parameter Block polja na NTFS logičkom disku ^[10]

Byte Offset	Dužina polja [B]	Vrednost (heksdecimalni zapis)	Naziv polja i opis
0x0B	2B	00 02	Bajta po sektoru. Sadrži informaciju o broju bajta po jednom sektoru. Hardverska veličina sektora. Za većinu diskova veličina ovog polja je 512B.
0x0D	1B	08	Sektora po klasteru. Broj sektora u jednom klasteru.
0x0E	2B	00 00	Rezervisani sektori. Uvek je 0, zato što NTFS smešta boot sektor na početak particije.

Byte Offset	Dužina polja [B]	Vrednost (heksadecimalni zapis)	Naziv polja i opis
0x10	3B	00 00 00	Vrednost mora biti 0, ili NTFS neće moći da podigne logički disk.
0x13	2B	00 00	Vrednost mora biti 0, ili NTFS neće moći da podigne logički disk.
0x15	1B	F8	Media Descriptor. Polje za indeksiranje medija. Sadrži informacije o korišćenom mediju. Vrednost F8 ukazuje na hard disk, a F0 da je medij high-density 3.5-inčni floppy disk. Media descriptor-i su prevaziđeni, potiču od MS-DOS FAT16 diskova i Windows ih ne koristi.
0x16	2B	00 00	Vrednost mora biti 0, ili NTFS neće moći da podigne logički disk.
0x18	2B	3F 00	Nije korišćeno ili provereno od strane NTFS sistema.
0x1A	2B	FF 00	Nije korišćeno ili provereno od strane NTFS sistema.
0x1C	4B	3F 00 00 00	Nije korišćeno ili provereno od strane NTFS sistema.
0x20	4B	00 00 00 00	Vrednost mora biti 0, ili NTFS neće moći da podigne logički disk.
0x24	4B	80 00 80 00	Nije korišćeno ili provereno od strane NTFS sistema.
0x28	8B	1C 91 11 01 00 00 00 00	Total Sectors. Ukupan broj sektora hard diska.
0x30	8B	00 00 04 00 00 00 00 00	Logical Cluster Number za \$MFT fajl. Logički broj klastera identifikuje lokaciju MFT tabele koristeći njen logički broj klastera.
0x38	8B	11 19 11 00 00 00 00 00	Logical Cluster Number za \$MFTMirr fajl. Logički broj klastera mirror MFT tabele, identifikuje lokaciju mirror kopije MFT tabele koristeći njen logički broj klastera.
0x40	1B	F6	Broj klastera po MFT zapisu. Broj klastera jednog MFT zapisa. Veličina svakog MFT zapisa. NTFS kreira zapis za svaki kreirani folder na NTFS logičkom disku. Fajlovi i folderi koji su manji od veličine MFT zapisa, ostaju u njemu. Ukolio je ovaj broj pozitivan (veći od 7F), onda reprezentuje broj klastera po MFT zapisu. Ako je broj negativan (80–FF), tada je veličina zapisa fajla duplo veća od apsolutne vrednosti ovog broja.
0x41	3B	00 00 00	Nije korišćeno od strane NTFS sistema.
0x44	1B	01	Klastera po bloku indeksa. Veličina svakog indeks bafera za alociranje foldera. Ukoliko je

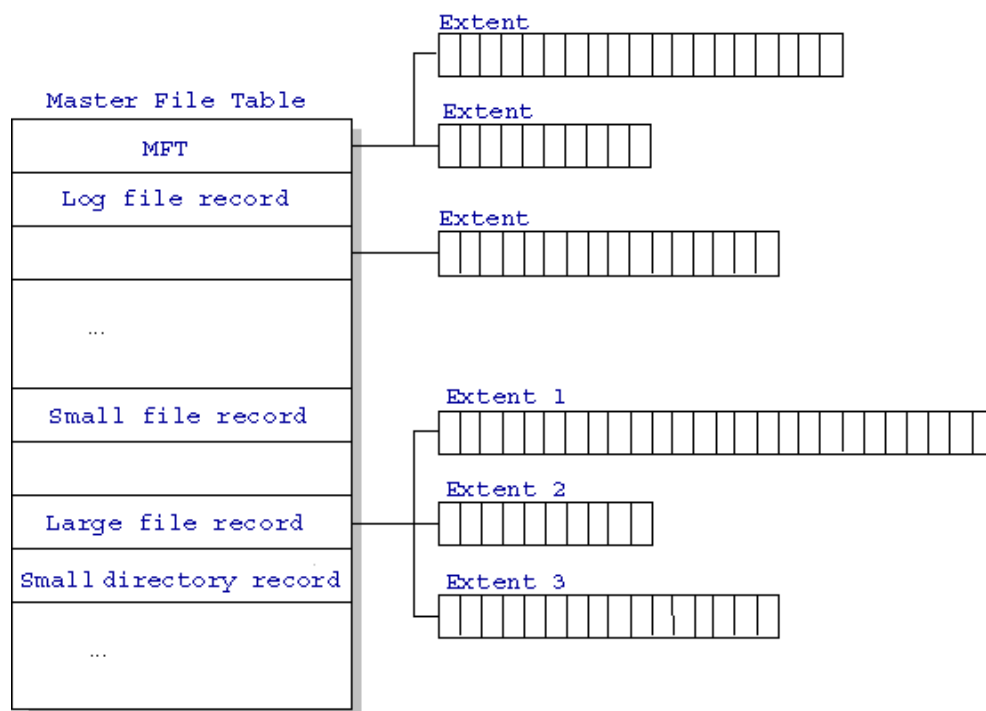
Byte Offset	Dužina polja [B]	Vrednost (heksdecimalni zapis)	Naziv polja i opis
			ovaj broj pozitivan (veći od 7F), onda reprezentuje broj klastera po MFT zapisu. Ako je broj negativan (80–FF), tada je veličina zapisa fajla duplo veća od apsolutne vrednosti ovog broja.
0x45	3B	00 00 00	Nije korišćeno od strane NTFS sistema.
0x48	8B	3A B2 7B 82 CD 7B 82 14	Serijski broj logičkog diska.
0x50	4B	00 00 00 00	Nije korišćeno od strane NTFS sistema.

1.2 - NTFS Master File Table (MFT)

Svaki fajl na NTFS disku predstavljena je zapisom u specijalnom fajlu - *master file table* (\$MFT). NTFS prvih 16 zapisa MFT tabele rezerviše za specijalne informacije. Prvi zapis opisuje samu tabelu, a sledeći zapis je MFT *mirror record*. Ukoliko je prvi zapis oštećen, NTFS čita sledeći zapis da nađe \$MFTMirr fajl, čiji je prvi zapis identičan prvom zapisu \$MFT fajla. Lokacije segmenata podataka MFT i MFT *mirror* fajlova zapisane su u boot sektoru. Duplikat boot sektora lociran je u logičkom centru diska.

Treći zapis MFT tabele je log fajl, koji se koristi za oporavljanje. Sedamnaesti i naredni zapisi MFT tabele (NTFS ih takođe vidi kao fajlove) služe za podatke o svakom fajlu i folderu na logičkom disku.

Na slici 3 prikazana je pojednostavljena struktura MFT tabele.



Slika 3 - Struktura MFT tabele

U MFT tabeli se alocira određeni prostor za svaki zapis. U taj prostor upisuju se atributi fajlova. Mali fajlovi i folderi (tipično 1500B i manje) upisuju se u celini u MFT zapis.

Tabela 5 - MFT zapis za male fajlove ili foldere ^[10]

Standardne informacije	Naziv fajla ili foldera	Security descriptor	Podatak ili indeks	Nekorišćeni prostor
------------------------	-------------------------	---------------------	--------------------	---------------------

Zapisi foldera su smešteni unutar MFT tabele isto kao i zapisi fajlova. Umesto podataka, folderi sadrže indeksne informacije. Mali zapisi foldera u celini su smešteni unutar MFT strukture. Veliki folderi organizovani su u B-stabla, sadrže zapise sa pokazivačima (pointerima) na eksterne klastere koji sadrže podatke foldera koji ne mogu da se smeste unutar MFT strukture.

Ovakav dizajn omogućava veoma brz pristup fajlovima.

2 - Tipovi NTFS fajlova

Izvorno, na engleskom jeziku, tipovi fajlova NTFS sistema imaju sledeće nazive:

- *NTFS File Attributes*
- *NTFS System Files*
- *NTFS Multiple Data Streams*
- *NTFS Compressed Files*
- *NTFS Encrypted Files*
- *NTFS Sparse Files*

2.1 - Atributi NTFS fajlova (*NTFS File Attributes*)

NTFS fajl sistem svak fajl ili folder vidi kao skup (set) atributa. Elementi kao što su ime fajla, sigurnosne informacije, pa čak i podaci čine skup atributa NTFS fajla. Svaki atribut se identifikuje kodnom oznakom tipa atributa i, opciono, nazivom atributa. Kada svi atributi fajla mogu stati u jedan MFT zapis oni se nazivaju rezidentnim atributima. Na primer, atributi kao što su ime fajla i vreme kreiranja fajla se uvek nalaze u MFT zapisu. Informacije o fajlu koje ne mogu stati u MFT zapis se nazivaju nerezidentnim atributima i nalaze se na jednom ili više klastera bilo gde na disku. U ovom slučaju NTFS u MFT zapisu kreira atribut sa nazivom lista atributa. U ovom atributu se nalaze podaci o lokacijama svih atributa koji ne mogu stati u MFT zapis.^[11]

U tabeli 6, data je lista definisanih atributa NTFS fajl sistema. Ova lista se može proširiti tako da se u nju mogu dodati novi atributi prema budućim potrebama.

Tabela 6 – Atributi fajlova koji su definisani na NTFS fajl sistemu^[11]

Naziv atributa	Opis
<i>Standard Information</i>	Standardne informacije kako što su vremenska oznaka i broj veza.
<i>Attribute List</i>	Lista lokacija svih atributa koji se ne nalaze u MFT zapisu.
<i>File Name</i>	Višestruki atribut koji sadrži podatke o nazivu fajla. Dugački naziv fajla može sadržati do 255 <i>unicode</i> karaktera. Kratki nazivi su formatu 8.3, s tim da se razlikuju velika i mala slova u nazivu. Dodatna imena i hard linkovi se takođe mogu uključiti u ovaj atribut.
<i>Security Descriptor</i>	Opis vlasnika fajla i prava pristupa fajlu.
<i>Data</i>	Sadrži podatke. NTFS dozvoljava postojanje više <i>data</i> atributa po jednom fajlu. Tipično, svaki fajl ima jedan neimenovani <i>data</i> atribut. Takođe, jedan fajl može imati jedan ili više <i>data</i> atributa, pri čemu svaki može da koristi različitu sintaksu.
<i>Object ID</i>	Jedinstveni identifikator fajla u okviru određenog diska. Nije obavezno da svaki fajl ima svoj identifikator.

<i>Logged Tool Stream</i>	Slično kao tok podataka sa razlikom što se particije sa fajlom pamte isto kao kod promene metapodataka. Koristi se kod EFS-a.
<i>Reparse Point</i>	Tačka redirekcije. Takođe se koristi od strane <i>Installable File System</i> (IFS) filter drajvera da se označe fajlovi od značaja za taj drajver.
<i>Index Root</i>	Koristi se kod implementacije foldera i ostalih indeksa.
<i>Index Allocation</i>	Koristi se kod implementacije foldera i ostalih indeksa.
<i>Bitmap</i>	Koristi se kod implementacije foldera i ostalih indeksa.
<i>Volume Information</i>	Koristi se samo kod \$Volume sistemskog fajla. Sadrži podatak o verziji fajl sistema na tom disku.
<i>Volume Name</i>	Koristi se samo kod \$Volume sistemskog fajla. Sadrži ime diska.

2.2 - NTFS Sistemski fajlovi (NTFS System Files)

NTFS uključuje nekoliko sistemskih fajlova, skrivenih od korisnika. Fajl sistem koristi sistemski fajl za smeštanje svojih metapodataka i za implementaciju samog fajl sistema. Sistemski fajlovi su smešteni na logički disk prilikom formatiranja.^[11]

Tabela 7 – metapodaci u *Master File Table*^[11]

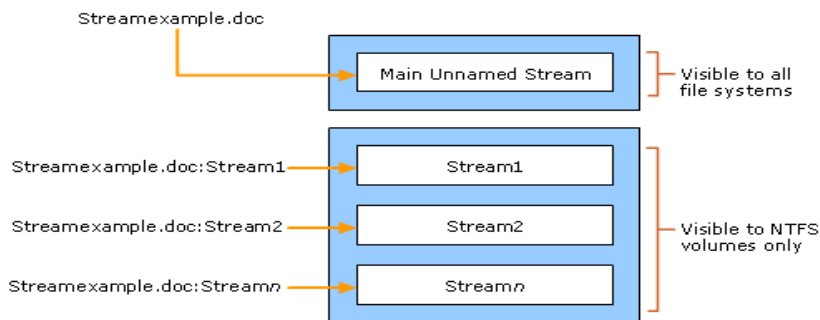
System File	File Name	MFT Record	Opis
Master file table	\$Mft	0	Sadrži po jedan osnovni zapis o svakom fajlu ili folderu na NTFS disku. Ako je informacija prevelika da bi stala u jedan zapis (<i>record</i>) preostale informacije se beleže na drugom mestu.
Master file table 2	\$MftMirr	1	Duplikat prva četiri zapisa iz MFT-a. Ovim se garantuje pristup MFT-u u slučaju oštećenja nekog od sektora na kojima je upisan MFT.
Log file	\$LogFile	2	Lista transakcija koja se koristi za oporavak fajl sistema. Zavisno od veličine diska može biti dužine do 4 Mb. Koristi se za uspostavu konzistencije NTFS-a u slučaju pada sistema.
Volume	\$Volume	3	Sadrži informacije o disku, kao što su naziv i verzija.
Attribute definitions	\$AttrDef	4	Tabela sa imenima, brojnim oznakama i opisima atributa.
Root file name index	\$	5	Osnovni (<i>root</i>) folder.
Cluster bitmap	\$Bitmap	6	Mapa zauzeća klastera.
Boot sector	\$Boot	7	Uključuje BPB koji se koristi za prepoznavanje diska i dodatnog <i>bootstrap code</i> -a ukoliko je disk butabilan.
Bad cluster file	\$BadClus	8	Podaci o lokacijama neupotrebljivih klastera.
Security file	\$Secure	9	Pojedinačni sigurnosni podaci za svaki fajl na disku.

Uppcase table	\$Uppcase	10	Tabela za konverziju malih u odgovarajuća velika <i>unicode</i> slova.
NTFS extension file	\$Extend	11	Razne opcione ekstenzije kao što su identifikatori objekata, tačke priključenja, itd.
		12-15	Rezervisano za buduće namene.

2.3 - NTFS Višestruki tokovi podataka (*NTFS Multiple Data Streams*)

Tok podataka (*data stream*) je sekvenca bajtova. Aplikacija ispunjava stream upisivanjem podataka na određene *offsete* unutar *streama*. Aplikacija tada čita podatak čitanjem istih *offseta* u putanji čitanja. Svaki fajl ima glavni, neimenovani *stream* asociiran na njega, bez obzira na korišćeni fajl sistem.^[1]

Međutim, NTFS podržava dodatne imenovane tokove podataka u kojima je svaki tok alternativna sekvenca bajtova, kao što ilustruje slika 4. Aplikacije mogu da kreiraju dodatne imenovane tokove i da im pristupaju referenciranjem na njihova imena. Ova osobina omogućava da odnosni podatak bude upravljan kao posebna jedinica. Na primer, grafički program može da smesti umanjenu (*thumbnail*) sliku ili *bitmap* sličicu u imenovani *data stream* unutar NTFS fajla koji sadrži sliku.^[1]



Slika 4 - Neimenovani i imenovani strimovi^[1]

FAT diskovi podržavaju samo glavne, neimenovane, tokove tako da se pri pokušaju kopiranja ili premeštanja *Streamexample.doc* u FAT logički disk ili floppy disk, pojavljuje poruka greške.

2.4 NTFS komprimovani fajlovi (*NTFS Compressed Files*)

NTFS podržava kompresiju pojedinačnog fajla, svih fajlova u folderu, i svih fajlova NTFS logičkog diska. Pošto je kompresija ugrađena unutar NTFS, svaki Windows-bazirani program može da čita i upisuje kompresovane fajlove bez potrebe za određivanjem stanja kompresije fajla. Kompresija je skup bita unutar hедера fajla, a informacija o kompresiji nalazi se u *Data* atributu fajla.^[1]

Fajlovi i folderi su kompresovani i dekompresovani prolaskom FSCTL_SET_COMPRESSION kôda do DeviceIoControl. Kompresovan fajl ili folder koji ima flag FILE_ATTRIBUTE_COMPRESSED asociran sa njim. Aplikacija korišćenjem *GetFileAttributes* može da odredi stanje kompresije fajla ili foldera.^[1]

Kada program otvori kompresovani fajl, NTFS dekompresuje samo onaj deo fajla koji je pročitao i onda kopira taj podatak u memoriju. Ostavljanjem nekompresovanog podatka u memoriji, performanse NTFS nisu opterećene kada program čita ili modifikuje podatke iz memorije. NTFS kompresuje modifikovane ili nove podatke u fajlu kada je podatak naknadno upisan na disk.^[1]

Algoritmi kompresije u NTFS podržavaju veličine klastera do 4kB. Kada je veličina klastera na NTFS disku veća od 4kB, ni jedna od NTFS karakteristika kompresije nije dostupna.^[1]

2.5 - NTFS šifrovani fajlovi (*NTFS Encrypted Files*)

Šifrovani fajl sistem, *EFS*, obezbeđuje jaku, pouzdanu i za korisnika potpuno transparentno šifrovanje bilo kog fajla ili foldera na NTFS disku. *EFS* radi u konjukciji sa *EFS* servisom, *Microsoft Crypto API*-jem i *EFS File System Run-Time Library (FSRTL)*. *EFS* vrši šifrovanje uz pomoć simetričnog ključa, koji se koristi zbog toga što je šifrovanje velike količine podataka daleko brža nego u slučaju kada se koristi asimetrični ključ. Postupak šifrovanja uz pomoć simetričnog ključa je oko 1000 puta brži u odnosu na šifrovanje asimetričnim ključem.

Simetrični ključ koji se koristi za šifrovanje je šifrovan javnim ključem koji je vezan za korisnički nalog korisnika koji vrši šifrovanje i čuva se sa alternativnim strimom podataka pridruženim uz fajl. Za dešifrovanje, fajl sistem koristi privatni ključ korisnika da bi dešifrovao simetrični ključ koji se nalazi u zaglavlju (*header-u*) fajla, a zatim njime vrši dešifrovanje fajla. Pošto se ove operacije vrše na nivou fajl sistema ceo postupak je potpuno transparentan za korisnika.

U slučaju da korisnik, iz nekog razloga, nema pristup svom ključu u NTFS je ugrađena podrška za rezervni par ključeva tako da je moguće podatke oporaviti uz pomoć *recovery agent-a*.

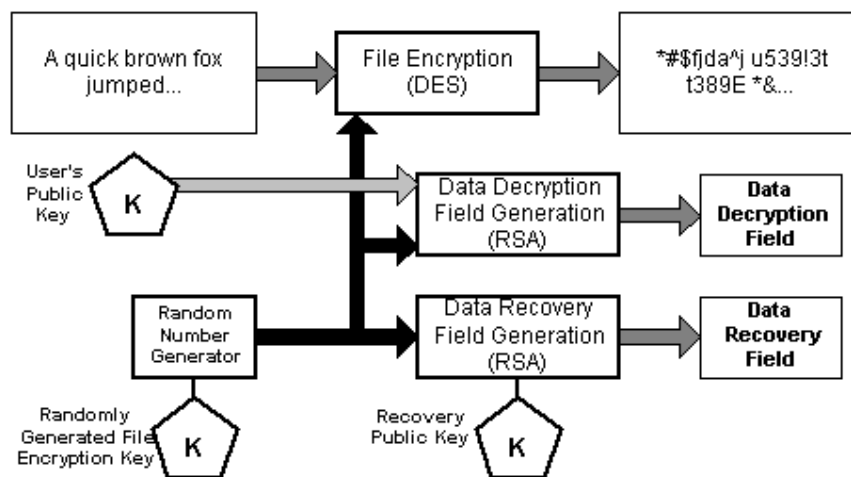
Podrška za EFS nije ugrađena u sve verzije Windows operativnih sistema. Na primer, nije dostupna u *Basic*, *Home* i *Media center* verzijama. U verzijama gde je dostupna mora se aktivirati po instalaciji operativnog sistema.

Ova tehnologija nam omogućava da se zaštitimo od neovlašćenog pristupa podacima u slučajevima krađe ili gubitka računara ili prenosnih uređaja za skladištenje podataka.

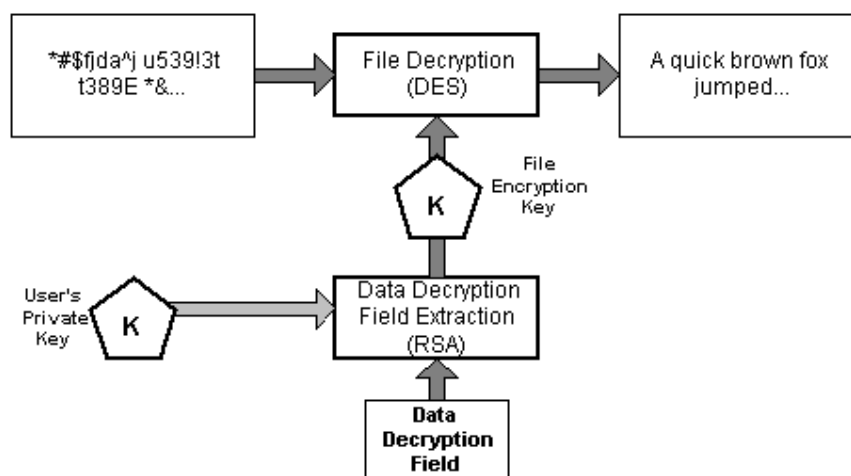
EFS ima sledeće prednosti u odnosu na nezavisne sisteme za šifrovanje:

- transparentan je za korisnika i aplikacije
- kada se folder označi kao šifrovan, sve operacije se obavljaju transparentno, u pozadini, tako da korisnik ne mora da pamti lozinku da bi dešifrovao fajlove
- EFS sam generiše ključeve koji su tolerantni na napade bazirane na rečniku
- ceo postupak se odvija u kernel režimu tako da ne postoji opasnost da se ključevi nađu u tzv. *Paginig* fajlu
- obezbeđuje mehanizam za oporavak vrednih podataka u slučaju otpuštanja i odlaska zaposlenih i sličnim situacijama ^[11]

Na slikama 5 i 6 prikazani su postupci šifrovanja i dešifrovanja.

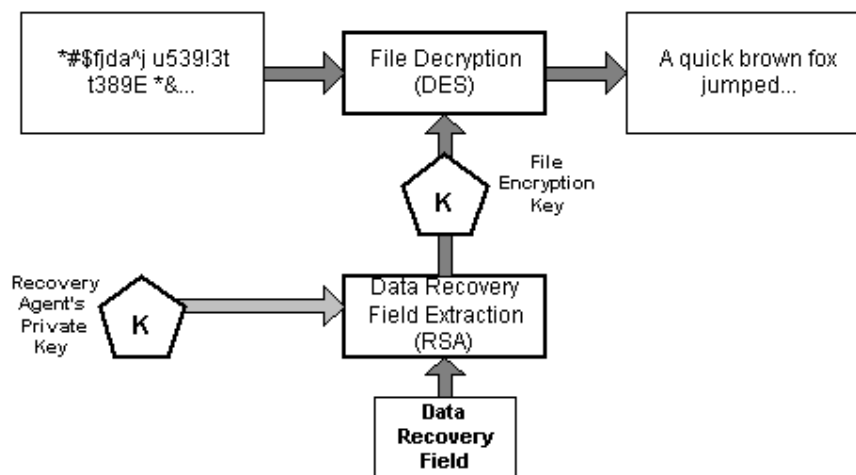


Slika 5 – Postupak šifrovanja ^[11]



Slika 6 – Postupak dešifrovanja ^[11]

Postupak oporavljanja je sličan postupku i dešifrovanja sa razlikom što se koristi privatan ključ *recovery agent*-a i prikazan je na slici 7.



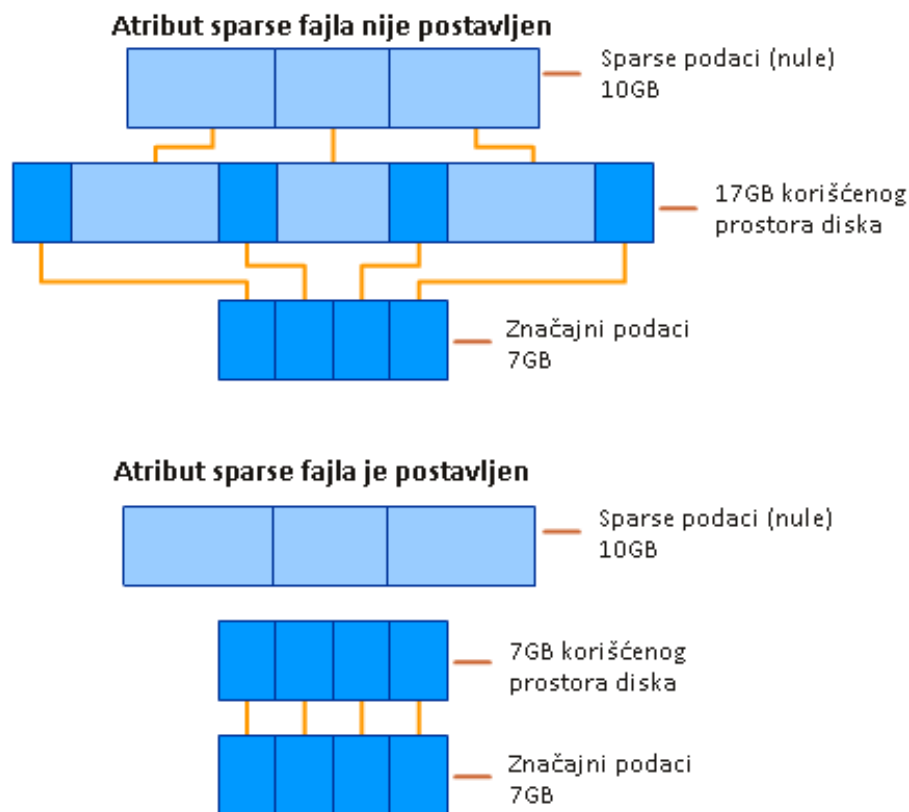
Slika 7 - Postupak oporavka kriptovanih podataka uz pomoć *recovery agent*-a ^[11]

2.6 - NTFS „šuplji“ fajlovi (NTFS Sparse Files)

Sparse files (šuplji, raštrkani, proređeni, fajlovi) obezbeđuju metod uštede prostora na disku koji sadrži značajne podatke, kao i velike sekcije podataka sastavljenih od nula. Kada je NTFS fajl markiran kao *sparse*, tada NTFS alokira klastere diska samo za podatke eksplicitno naznačene od strane aplikacije. Nenaznačeni opsezi fajla reprezentovani su nealociranim

prostorom na disku (šupalj prostor). Kada je *sparse* fajl pročitao iz alociranog opsega, ostatak je vraćen kao što je bio uskladišten. Podatak pročitao iz nealociranog opsega vraćen je kao nule.^[1]

File system application programming interfaces (APIs) omogućavaju da fajl bude kopiran ili bekapovan kao aktuelni bitovi i *sparse stream* opsezi. Fajl sistem APIs takođe dozvoljavaju upite alociranih opsega. Tada programi koji primenjuju ove API-je samo treba da pročitaju alocirani opseg i oporave podatke fajla. Rezultat je efikasno fajl sistem skladištenje i pristup. Slika 8 ilustruje način na koji je podatak uskladišten sa i bez setovanog *sparse* fajl atributa.^[1]



Slika 8 - Skladište sparse fajla^[1]

Na primer, osobine fajla mogu prikazati da je fajl 1GB sparse fajl. Iako je fajl 1GB, on zauzima samo 64kB prostora na disku.

Ukoliko kopiramo ili premestimo *sparse* fajl na FAT ili NTFS logički disk operativnim sistemom postavljen na drugačiji način od *prethodnih*, fajl će biti kreiran na svoju originalnu naznačenu veličinu. Ukoliko nema dovoljno slobodnog prostora, operacija neće uspeti.

3 - Skrivanje podataka u NTFS fajl sistemu

Polazni kriterijumi za odabir metode za skrivanje podataka bi trebalo da ispune sledeće uslove:

- standardnom proverom sistemskim alatima kao što je *chkdsk* (*check disk*) ne dobija se nikakva poruka o grešci
- mogućnost prepisivanja ili brisanja skrivenih podataka ne postoji ili je malo verovatna
- standardni korisnik neće primetiti skrivene podatke
- prostor za skrivanje podataka ispunjava potrebe zlonamernog korisnika i razumne je veličine.^[12]

Najefikasniji način za skrivanje podataka je baziran na zloupotrebi \$DATA atributa pošto je to jedini atribut koji nema striktno definisan format. Sadržaj ovog atributa je nije unapred definisan i može biti bilo koje dužine. Zbog navedenih osobina teško je posumnjati u valjanost njegovog sadržaja. Takodje, razumno je očekivati da će ovaj atribut uvek postojati na NTFS sistemima.^[12]

Pored prethodno navedene metode često se koristi *file slack* i *volume slack* kao prostor na disku u koji se upisuju podaci koji se žele sakriti. Sa aspekta zlonamernog korisnika ovo nije naročito pouzdana metoda za skrivanje podataka jer je verovatnoća prepisivanja ovih podataka prilično velika. Ova metoda se primenjuje na *slack* prostoru koji su vezani uz fajlove za koje se ne očekuje promena sadržaja ili brisanje jer se time verovatnoća gubljenja skrivenih podataka znatno umanjuje.^[12]

Višestruki tokovi podataka takodje ispunjavaju uslove koji su neophodni za skrivanje podataka pošto su sastavni deo NTFS fajl sistema, nisu vidljivi za korisnika i neće izazvati nestabilnost sistema. Koriste se i za smeštanje virusa.^[12]

II – FORENZIČKA ANALIZA WINDOWS 7 BAZE REGISTARA

1 - Struktura Windows registra

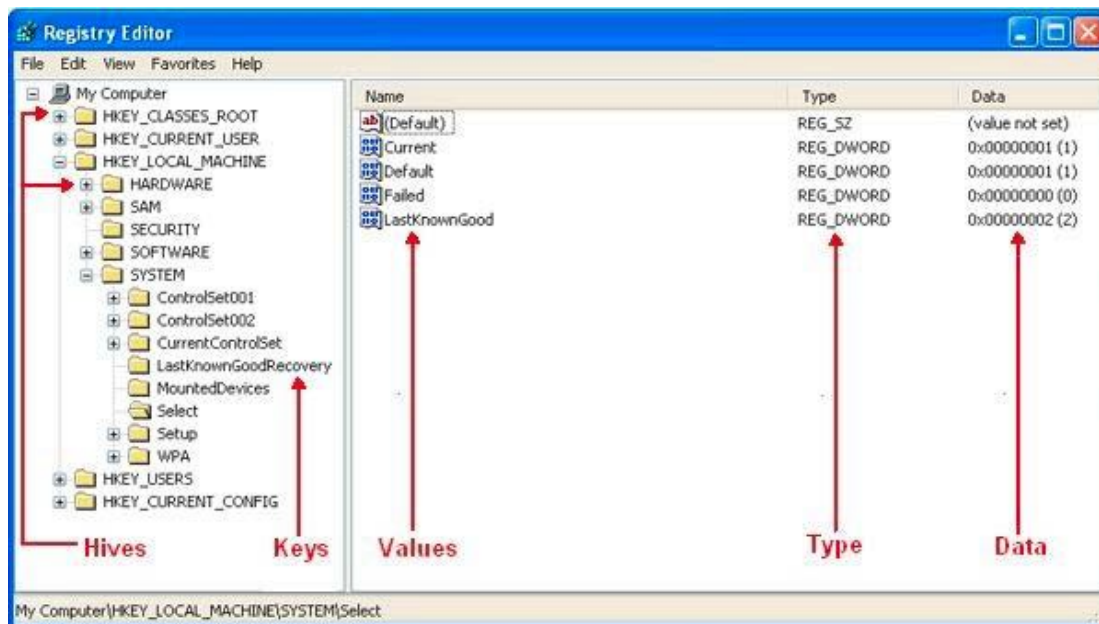
Windows registar je organizovan u nekoliko celina koji se u izvorno nazivaju *root keys*. Za prikaz logičke strukture Windows registra se može koristiti alat *Windows Registry Editor* koji je sastavni deo operativnog sistema Windows ^[2].

Po pokretanju *Registry Editor*-a može se videti da se *Registry* baza prikazuje kao jedna vrsta hijerarhijskog fajl sistema. U levom delu prozora, koji se inače naziva *Key pane*, može se videti da je sve organizovano u foldere, što je veoma slično strukturi samog hard diska, odnosno fajl sistema.

Postoji pet glavnih foldera u hijerarhiji (*hives*) čiji nazivi počinju sa HKEY (skraćenica od *Handle to a Key*). Iako ih ima ukupno pet, kao što se može videti, samo su dva, u stvari, prava (*real*), a to su HKEY_USERS (HKU) i HKEY_LOCAL_MACHINE (HKLM). Ostala tri su prečice (*shortcuts*) ili aliasi nekih od delova dva realna foldera (*hive*), koji, takođe, imaju forenzički značaj. Svaki od ovih pet foldera (*hive*), sastoji se od ključeva (*keys*), koji sadrže vrednosti (*values*) i podključeve (*subkeys*) ^[2].

Najbolja analogija, koja se može koristiti za pomoć prilikom objašnjenja strukture *Windows Registry*-ja je poređenje sa *Windows Explorer* fajl sistemom, koji ima vrlo sličnu strukturu. Levi deo prozora (*key pane*) iz *Registry*-ja podseća na hijerarhijsku strukturu levog dela prozora u *Windows Explorer*-u. Ključevi i podključevi su locirani u pet glavnih foldera (*hives*), slično kao i folderi i podfolderi u *Windows Explorer*-u, dok su vrednosti (*values*) slični fajlovima koji se nalaze u folderu. U desnom delu prozora *Windows Registry*-a imena vrednosti (*name*) su slična kao i imena fajlova, a tipovi (*type*) su slični ekstenziji fajlova, dok su podaci (*data*) slični sadržaju određenog fajla ^[5].

Pet segmenata *Windows* registra (*hives*) sa elementarnim opisom prikazani su na slici 9.

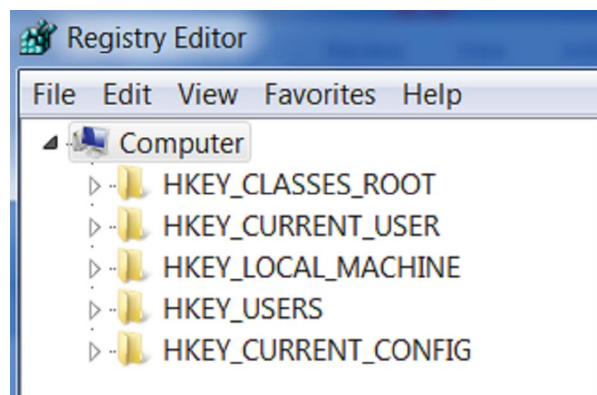


Slika 9 – Struktura Windows Registry baze

U operativnom sistemu Windows 7 registry ima pet osnovnih logičkih celina - root keys:

1. HKEY_CLASSES_ROOT.
2. HKEY_CURRENT_USER.
3. HKEY_LOCAL_MACHINE.
4. HKEY_USERS.
5. HKEY_CURRENT_CONFIG.

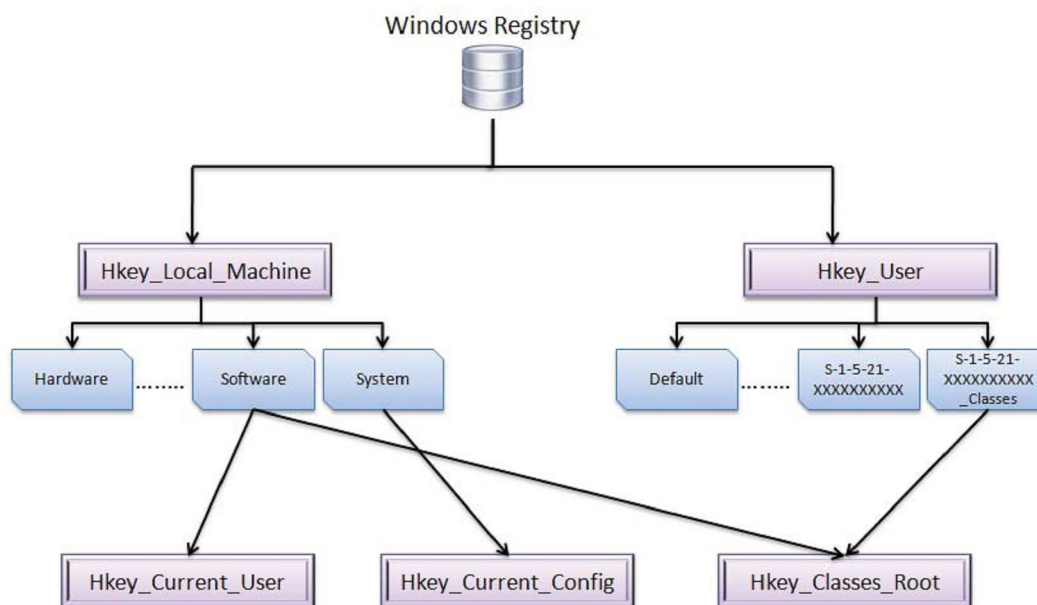
Slika 10 pokazuje pet osnovnih logičkih celina - root keys registra u Windows 7 onako kako se vide u Windows Registry Editor-u.



Slika 10 - Root keys Windows registra

U stvari postoje samo dva *root keys*, to su HKEY_LOCAL_MACHINE i HKEY_USERS. Ova dva *root keys* uskladišteni su na hard disku sistema i nisu promenljivi podaci koji se drže u glavnoj memoriji. Drugi ključevi su podsetovi ovih *root keys* ^[2].

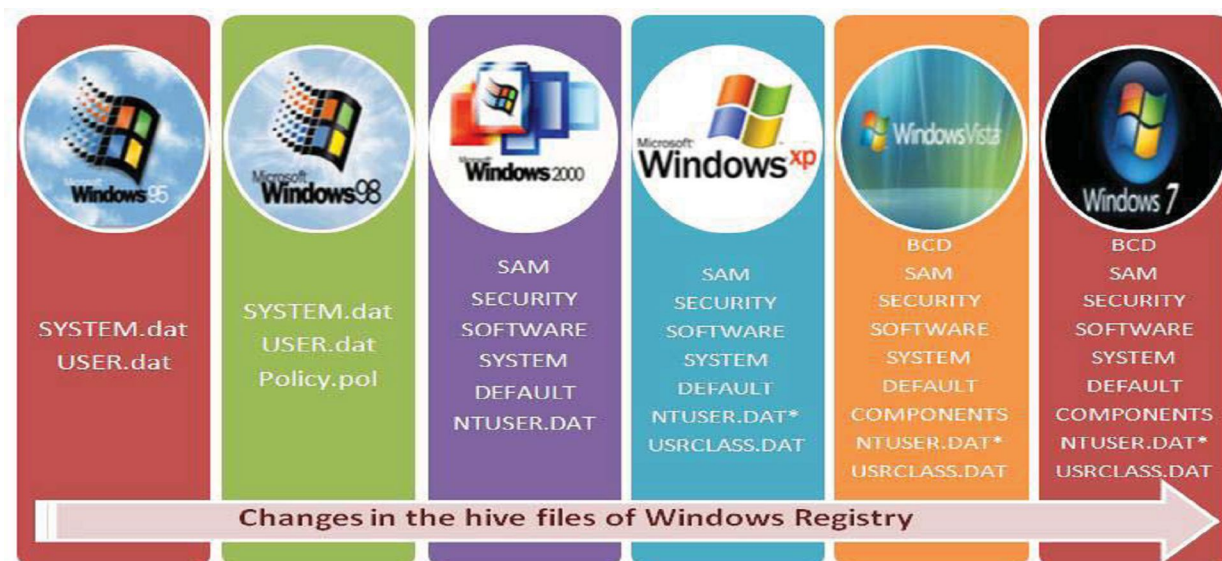
Slika 11 pokazuje veze izmedju *root keys*.



Slika 11 - Veza izmedju *root keys* Windows Registra

Windows Registry Editor prikazuje logičku strukturu Registra. Operativni sistem Windows organizuje registar u jedan broj tzv. *hive files*. *Hive file* je binarni fajl koji se sastoji od jednog ili više ključeva registra, zajedno sa njihovim vrednostima. Ovi fajlovi su modifikovani sa promenama u operativnom sistemu Windows. Promene su načinjene zato što svaki novi Windows operativni system ima novu funkcionalnost.

Slika. 12 pokazuje promene u *hive files* *Windows Registry*-ja u nekoliko generacija operativnog sistema.



Slika 12 - Promene u hive files operativnog sistema Windows

Postoji tri ili više *hive* fajlova koji imaju ime NTUSER.DAT. Prvi se odnosi se na nalog za mrežne usluge, drugi za nalog na lokalne usluge a treći na korisnički nalog. Svaki korisnički nalog ima svoj NTUSER.DAT *hive file* ^[8].

1.1 - Funkcije Root Key segmenata

Pored naziva *root key* segmenta u zagradi je skraćenica koja se uobičajeno odnosi na njega, na koju će se često referencirati kroz ceo rad.

HKEY_CLASSES_ROOT (HKCR)

Informacije koje su ovde uskladištene osiguravaju da se izvrši odgovarajući program pri pokretanju iz *Windows Explorer*-a. On takodje sadrži pojedinosti o pravilima za *drag-and-drop*, prečicama i informacijama na korisničkom interfejsu.

Alijas za HKLM\Software\Classes

HKEY_CURRENT_USER (HKCU)

Sadrži informacije o korisniku koji je trenutno prijavljen na sistem, uključujući korisnikove foldere, boje na ekranu i podešavanja *Control Panel*-u. Alijas za segment u HKEY USERS specifičan za korisnika. Generičke informacije koje se primenjuju na sve korisnike a nalaze se u delu HKU\DEFAULT

HKEY_LOCAL_MACHINE (HKLM)

Sadrži informacije specifične za hardver računara na kome se nalazi operativni sistem. Uključuje listu *drives* i generičke konfiguracije instaliranog hardvera i aplikacija.

HKEY_USERS (HKU)

Sadrži informacije o konfiguraciji svih korisničkih profila u sistemu, konfiguraciji aplikacija i vizuelnih podešavanja.

HKEY_CURRENT_CONFIG (HCU)

Sadrži informacije o trenutnoj konfiguraciji sistema. Alijas za HKLM\Config\profile

2 - Analiza operativnog sistema uz pomoć baze registara

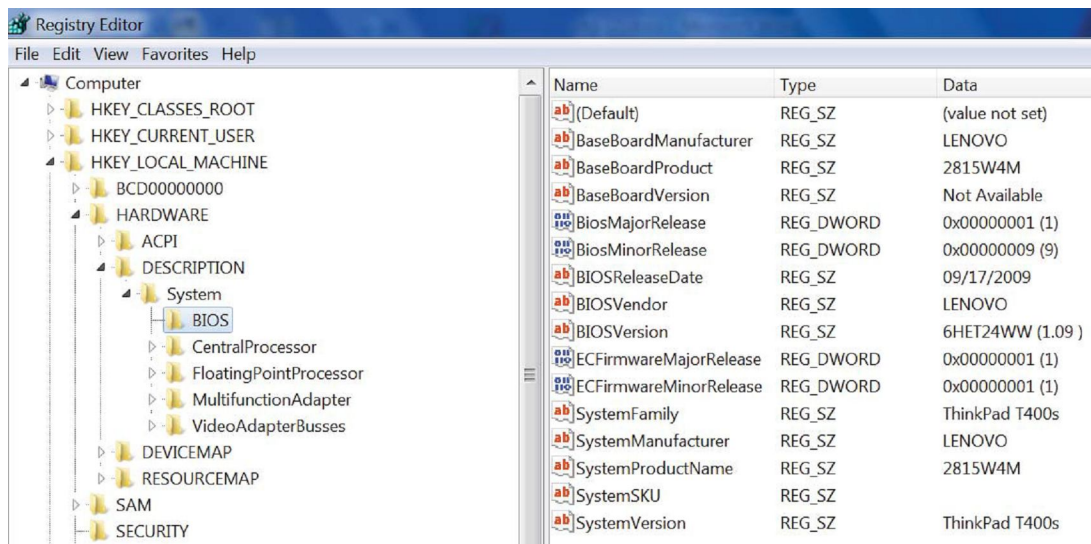
Windows Registry sadrži veliku količinu informacija o sistemu poput podešavanja i konfiguracije sistema. Jedan deo ovih podataka je od velikog značaja forenzičkom istražitelju.

Prvo, ime kompjutera je na raspolaganju u sledećem podključu *Registry* baze:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName

Podključ registra sa informacijama o sistemu ima sledeću putanju:
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\BIOS

Ovaj ključ sadrži nekoliko vrednosti koje sadrže informacije o sistemu poput informacija o *BIOS-u* i informacija o sistemu na kome se nalazi operativni sistem. Informacije o *BIOS-u* uključuju datum objavljivanja *BIOS-a* i verziju *BIOS-a*. Informacije o sistemu uključuju proizvodno ime sistema i ime njegovog proizvođača.

Slika 13 prikazuje podključ *Registry* baze sa informacijama o sistemu.

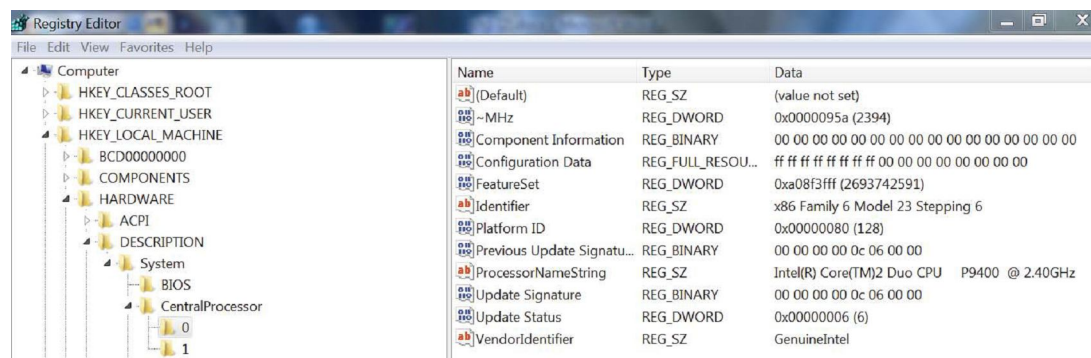


Slika 13 - Opis hardvera sistema unutar Windows Registry

Informacije o procesorima u sistemu uskladištene su u sledećim podključevima *Windows* Registry baze:

HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\1

Ove informacije uključuju ime procesora, njegovu brzinu i identifikator kako je prikazano na slici 14.

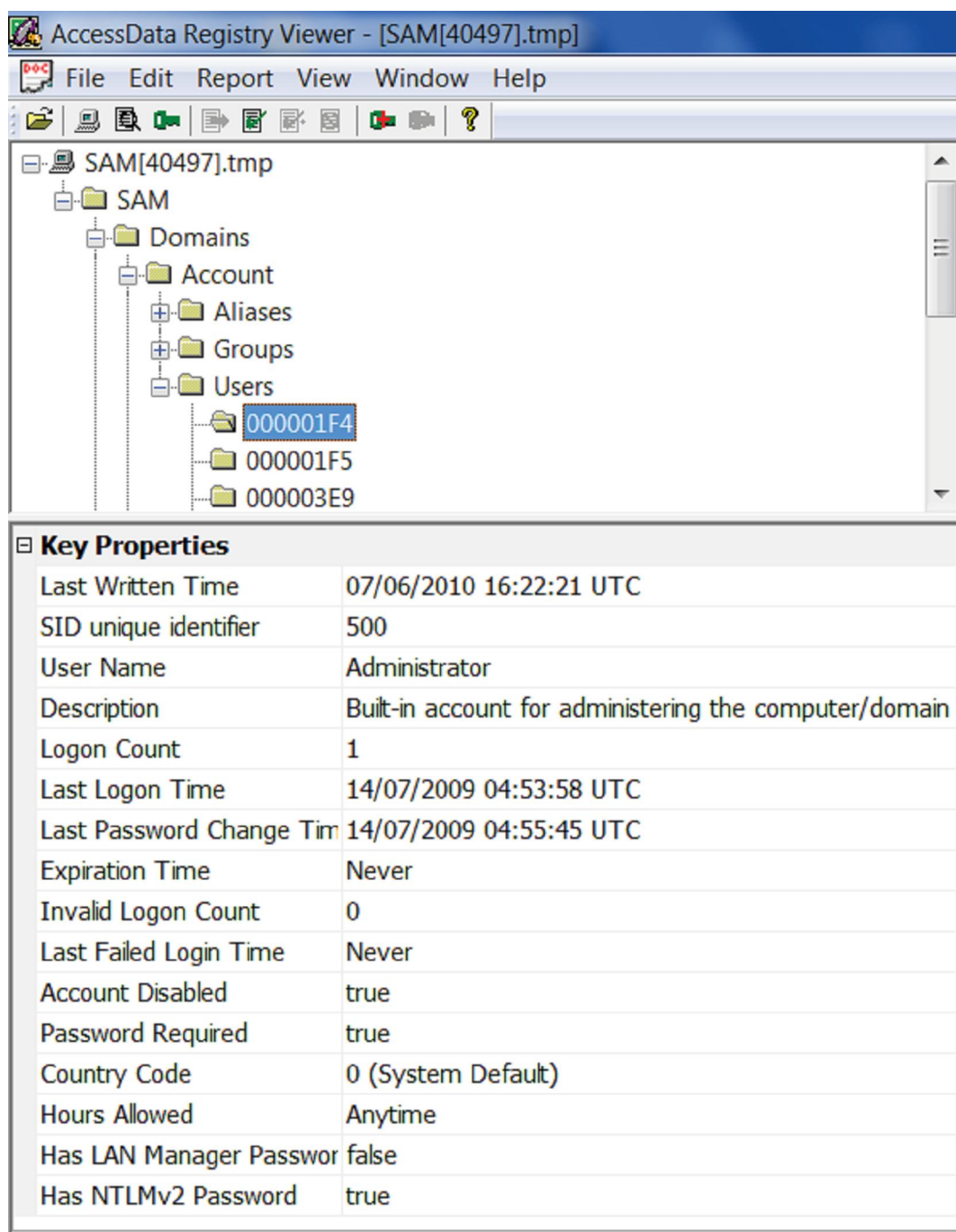


Slika 14 - Opis centralnog procesora unutar Windows Registry

Informacije o korisničkom nalogu se čuvaju u *Registry* bazi. Na primer lista korisničkih naloga, poslednje vreme kada se korisnik ulogovao na određeni nalog, da li on zahteva lozinku, da li je to neaktivan ili aktivan nalog i metod koji je korišćen da se šifruje lozinka korisničkog naloga. Sve ove informacije drže se u sledećem ključu Registra:

HKEY_LOCAL_MACHINE \SAM\Domains\Account\Users

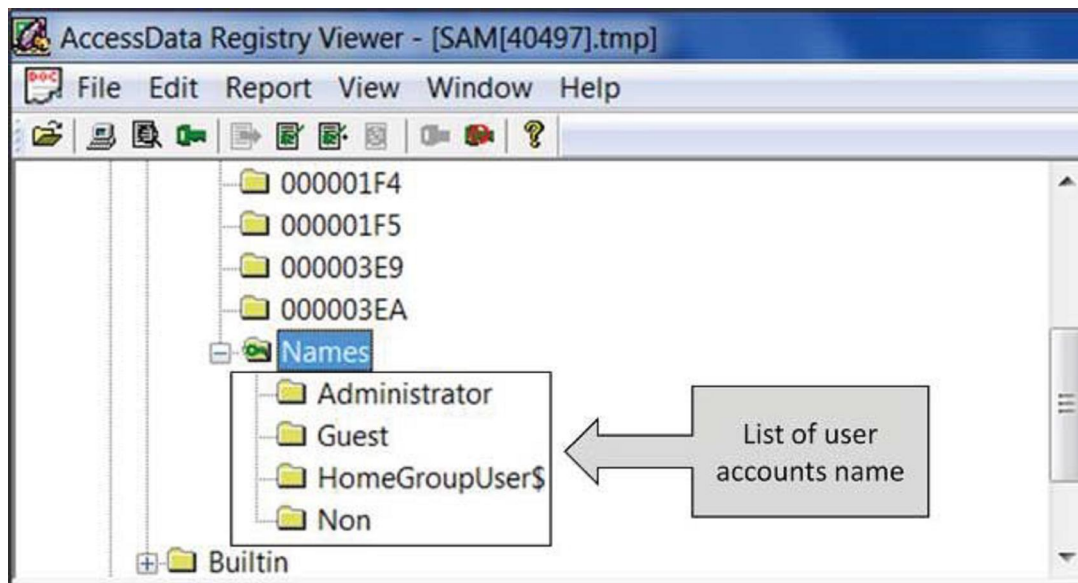
Slika 15 prikazuje pojedinosti korisničkog naloga kako se on vidi uz korišćenje programa *AccessData Windows Registry Viewer*



Slika 15 - Pojedinosti korisničkog naloga u Access Data Registry Viewer-u

Imena korisničkih naloga navedena su na listi u sledećem ključu registra:
HKEY_LOCAL_MACHINE\SAM\Domains\Account\Users\Names

Slika 16 pokazuje imena korisničkih naloga kako se ona vide uz korišćenje programa *AccessData Registry Viewer*-a.

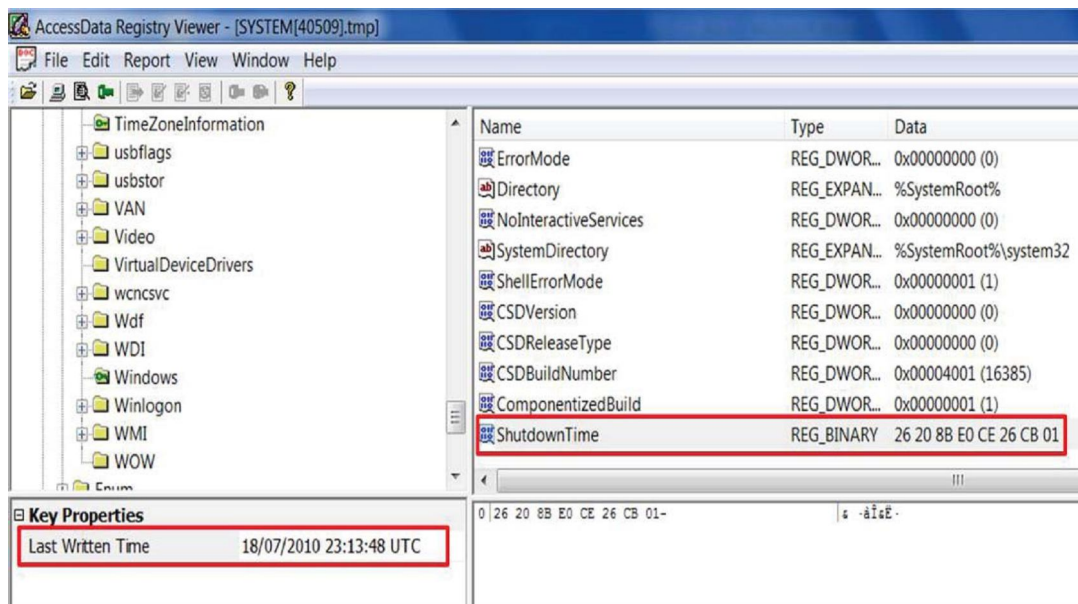


Slika 16 - Imena korisničkih naloga unutar Windows Registry

Sledeća, forenzičkom istražitelju, značajna informacija je vreme poslednjeg isključivanja sistema. Ova informacija je sačuvana u *ShutdownTime* vrednosti u sledećem ključu *Windows Registry* baze:

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Windows

Slika 17 pokazuje vrednost poslednjeg vremena gašenja računara (*ShutdownTime*) kako se ona vidi uz korišćenje *Access Data Windows Registry viewer*-a.



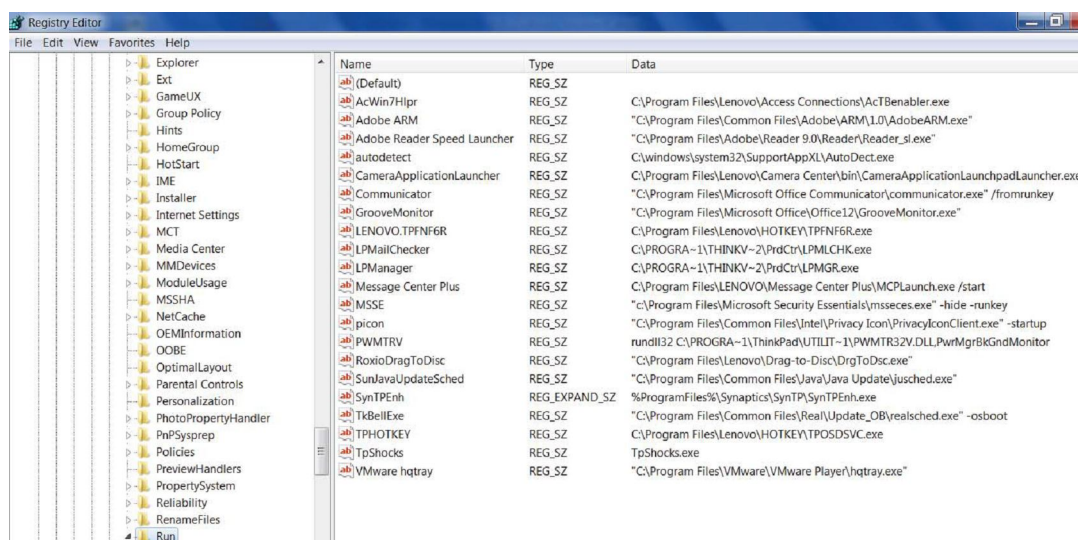
Slika 17 - Prikaz brojne vrednosti vremena isključivanja računara u binarnom obliku u Windows Registry bazi

3 - Analiza aplikacija

3.1 - Start up programi

Lista startup programa je prikazana na slici 18 i navedena na listi u sledećem ključu Windows registra:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

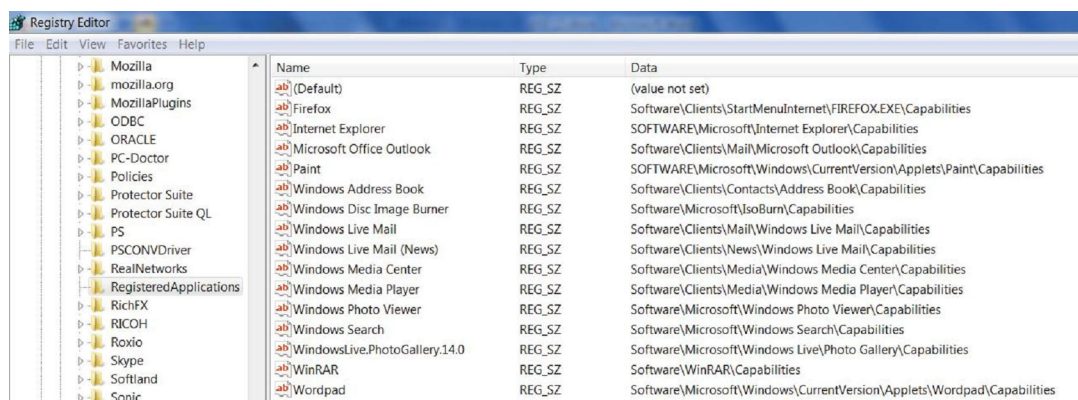


Name	Type	Data
(Default)	REG_SZ	
AcWin7Hlpr	REG_SZ	C:\Program Files\Lenovo\Access Connections\ActBEnabler.exe
Adobe ARM	REG_SZ	"C:\Program Files\Common Files\Adobe\ARM\1.0\AdobeARM.exe"
Adobe Reader Speed Launcher	REG_SZ	"C:\Program Files\Adobe\Reader 9.0\Reader\Reader_sl.exe"
autodetect	REG_SZ	C:\windows\system32\SupportApp\XLAutoDetect.exe
CameraApplicationLauncher	REG_SZ	C:\Program Files\Lenovo\Camera Center\bin\CameraApplicationLaunchpadLauncher.exe
Communicator	REG_SZ	"C:\Program Files\Microsoft Office Communicator\communicator.exe" /fromrunkey
GrooveMonitor	REG_SZ	"C:\Program Files\Microsoft Office\Office12\GrooveMonitor.exe"
LENOVO.TPFNF6R	REG_SZ	C:\Program Files\Lenovo\HOTKEY\TPFN6R.exe
LPMailChecker	REG_SZ	C:\PROGRA~1\THINKV~2\PrdCtr\LPMCHK.exe
LPManger	REG_SZ	C:\PROGRA~1\THINKV~2\PrdCtr\LPMGR.exe
Message Center Plus	REG_SZ	C:\Program Files\LENOVO\Message Center Plus\MCPLaunch.exe /start
MSSE	REG_SZ	"c:\Program Files\Microsoft Security Essentials\msseces.exe" -hide -runkey
picon	REG_SZ	"C:\Program Files\Common Files\Intel\Privacy Icon\PrivacyIconClient.exe" -startup
PWMTRV	REG_SZ	rundll32 C:\PROGRA~1\ThinkPad\UTILIT~1\PWMTR32V.DLL,PwrMgrBkGndMonitor
RoxioDragToDisc	REG_SZ	"C:\Program Files\Lenovo\Drag-to-Disc\DrToDisc.exe"
SunJavaUpdateSched	REG_SZ	"C:\Program Files\Common Files\Java\Java Update\jusched.exe"
SynTPEnh	REG_EXPAND_SZ	%ProgramFiles%\Synaptics\SynTP\SynTPEnh.exe
TkBellExe	REG_SZ	"C:\Program Files\Common Files\Real\Update_OB\yrealched.exe" -osboot
TPHOTKEY	REG_SZ	C:\Program Files\Lenovo\HOTKEY\TPOSD5VC.exe
TpShocks	REG_SZ	TpShocks.exe
VMware hqtray	REG_SZ	"C:\Program Files\VMware\VMware Player\hqtray.exe"

Slika - 18: Lista startup programa uz Windows Registry bazi

3.2 - Registrovane aplikacije

Lista registrovanih aplikacija je prikazana na slici 19, nalazi se na listi u ključu registra: HKEY_LOCAL_MACHINE\SOFTWARE\RegisteredApplications



Name	Type	Data
(Default)	REG_SZ	(value not set)
Firefox	REG_SZ	Software\Clients\StartMenuInternet\FIREFOX.EXE\Capabilities
Internet Explorer	REG_SZ	SOFTWARE\Microsoft\Internet Explorer\Capabilities
Microsoft Office Outlook	REG_SZ	Software\Clients\Mail\Microsoft Outlook\Capabilities
Paint	REG_SZ	SOFTWARE\Microsoft\Windows\CurrentVersion\Applets\Paint\Capabilities
Windows Address Book	REG_SZ	Software\Clients\Contacts\Address Book\Capabilities
Windows Disc Image Burner	REG_SZ	Software\Microsoft\IsoBurn\Capabilities
Windows Live Mail	REG_SZ	Software\Clients\Mail\Windows Live Mail\Capabilities
Windows Live Mail (News)	REG_SZ	Software\Clients\News\Windows Live Mail\Capabilities
Windows Media Center	REG_SZ	Software\Clients\Media\Windows Media Center\Capabilities
Windows Media Player	REG_SZ	Software\Clients\Media\Windows Media Player\Capabilities
Windows Photo Viewer	REG_SZ	Software\Microsoft\Windows Photo Viewer\Capabilities
Windows Search	REG_SZ	Software\Microsoft\Windows Search\Capabilities
WindowsLive.PhotoGallery.14.0	REG_SZ	Software\Microsoft\Windows Live\Photo Gallery\Capabilities
WinRAR	REG_SZ	Software\WinRAR\Capabilities
Wordpad	REG_SZ	Software\Microsoft\Windows\CurrentVersion\Applets\Wordpad\Capabilities

Slika 19 - Lista registrovanih aplikacija unutar Windows Registry

3.3 - Analiza aplikacije Windows Live Messenger

Microsoft Windows Live Messenger je veoma poznata aplikacija za četovanje (časkanje) koju koristi veliki broj ljudi. Unutar Windows registra se čuvaju informacije u vezi sa korišćenjem programa Microsoft Windows Live Messenger koje mogu biti od velikog značaja za forenzičara. Jednostavno rečeno, MSN objekat se koristi za čuvanje korisnikovih podešavanja, poput pozadine i prikazane slike. Ove informacija se čuvaju u vrednosti zvanoj UTL u sledećem ključu Registra:

HKEY_USERS\S-1-5-21-

[UserIdentifier]\Software\Microsoft\MSNMessenger\PerPassportSettings\[MSNMessengerAccountIdentifier]

Slika 20 pokazuje sadržaj UTL vrednosti.

```
<msnobj Creator="khawla@hotmail.com"
Size="1835" Type="3" Location="TFR1D.dat"
Friendly="5hAgAEEAbAAgAE0AYQBIAGEAIADmEA=="
SHA1D="rWoJZJy3Jofajyw4zriDiXTtn48="
SHA1C="NLUSWD+yEV94Oe+VmED5fTQjuVQ="/>
```

Slika 20 - Sadržaj UTL vrednosti

Ovo što sledi je opis svakog polja MSN objekta (MSN:P2P/Msnobj Description, 2009):

1. *Creator*: MSN messenger korisnički nalog
2. *Size*: veličina podataka koje objekat sadrži
3. *Type*: nekoliko identifikatora ovog polja je prikazano u tabeli 8

Tabela 8 - Opis polja type MSN objekta

Oznaka tipa	Opis
1	Unknown
2	Custom Emoticons
3	Static display picture
4	Shared File
5	Static Backgrounds
6	Unknown
7	Dynamic display pictures
8	Wink
9	Map File
10	Dynamic Backgrounds

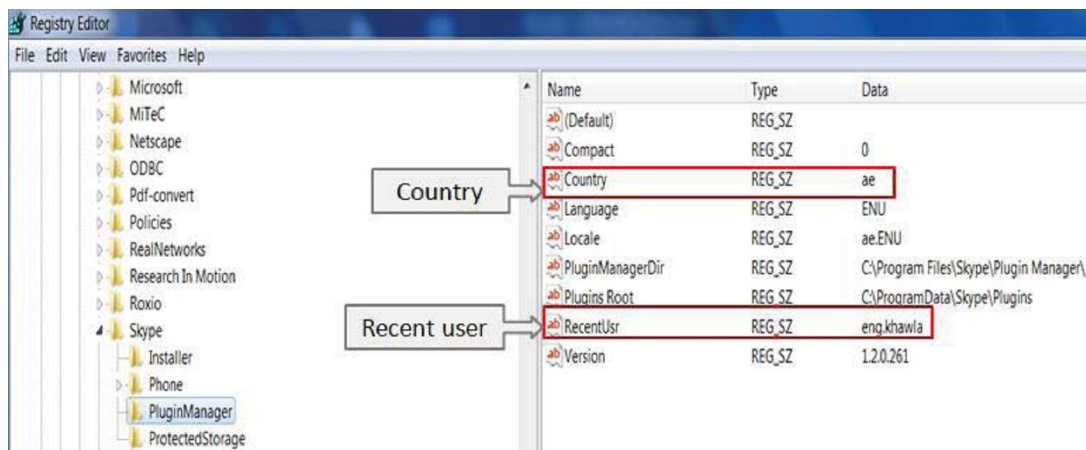
11	<i>Voice Clip</i>
12	<i>State</i>
13	<i>Roaming Objects</i>
14	<i>Signature Sound</i>
15	<i>Unknown</i>
16	<i>Scene</i>
17	<i>Web cam Dynamic Display Picture</i>

4. Location: ime fajla koji sadrži objekat
5. Friendly: šifrovano ime slike korišćenjem UTF-16
6. SHA1D: SHA1 heš pregled podataka
7. SHA1C: SHA1 heš pregled svih prethodnih polja MSN objekta ^[8].

3.4 - Analiza aplikacije Skype

Skype je još jedna dobro znana aplikacija koja dozvoljava korisniku da uputi govorni ili video poziv preko mreža zasnovanih na IP protokolu. Drugim rečima to je VoIP softver. Za forenzičkog istražitelja važno je da zna da li je i kako korisnik sistema koristio ovaj softver. Takodje je važno znati naziv Skype naloga koji koristi odgovarajući korisnik sistema. Ako je Skype aplikacija instalirana na sistemu, postojaće podključ u ključu HKEY_LOCAL_MACHINE i HKEY_USERS\S-1-5-21-[User Identifier]\. U ovom podključu forenzički istražitelj može pronaći korisnika koji je u najskorije vreme koristio ovu aplikaciju.

Ključ registra HKEY_USERS\S-1-5-21-[User Identifier]\Software\Skype\PluginManager koji sadrži vrednost za skorašnje korisnike i kod zemlje iz Skajp aplikacije prikazan je na slici 21 ^[8].



Slika 21 - Interesantne informacije Skajp aplikacije unutar Windows Registry

4 - Analiza mreže

4.1 - Mrežni adapteri

Registar sadrži listu svih mrežnih adaptera bilo da je adapter ugrađen ili je spoljni (eksterni). Kod većine laptop računara postoje dva tipa mrežnih adaptera: Ethernet mrežni adapter i Wi-Fi mrežni adapter. Sledeći ključ Registra sadrži listu mrežnih adaptera:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\NetworkCards
```

4.2 - Intranet mreže

Lista internih (*intranet*) mreža sa kojom je računar bio povezan sačuvana je unutar registra u sledećem ključu:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\NetworkList\Nla\Cache\Intranet
```

4.3 - Bežične mreže

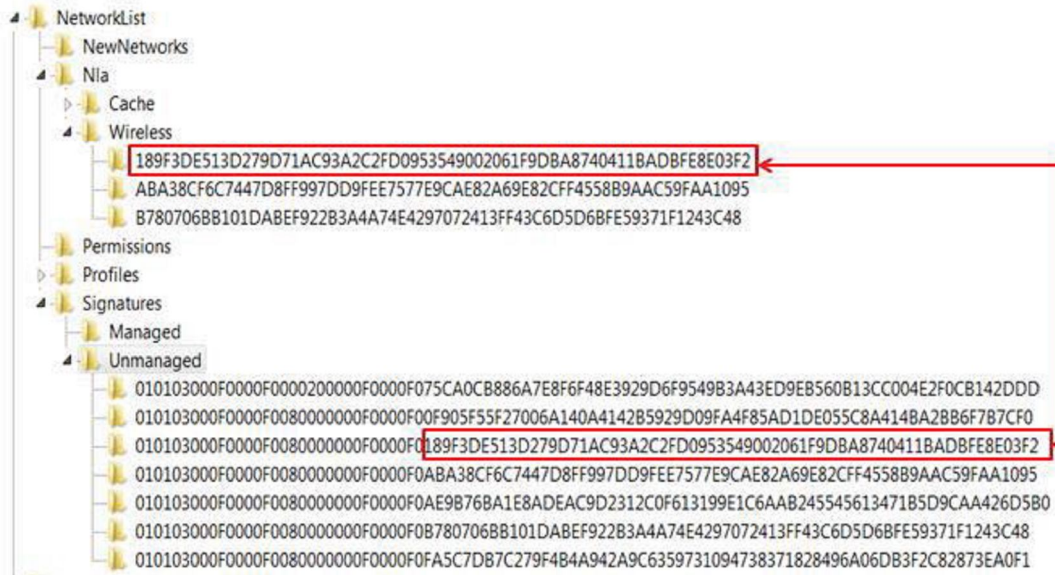
Identifikatori mreža sa kojima je sistem bio povezan, su sačuvani u sledećem ključu:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\  
CurrentVersion\NetworkList\Nla\Wireless
```

Ovaj ključ je samo lista identifikatora za svaku od bežičnih mreža sa kojima je računar bio povezan. Više informacija o svakoj od ovih bežičnih mreža poput MAC adrese, DNS sufiksa i SSID mogu se naći unutar registra. Ovo se može učiniti povezivanjem identifikatora iz prethodnog ključa sa ključem

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\NetworkList\Signatures\Unmanaged
```

u *Windows Registry* bazi kako je prikazano na slici 22. Ovaj ključ sadrži prilično mnogo informacija o mrežama uopšte, ne samo o bežičnim mrežama ^[8].

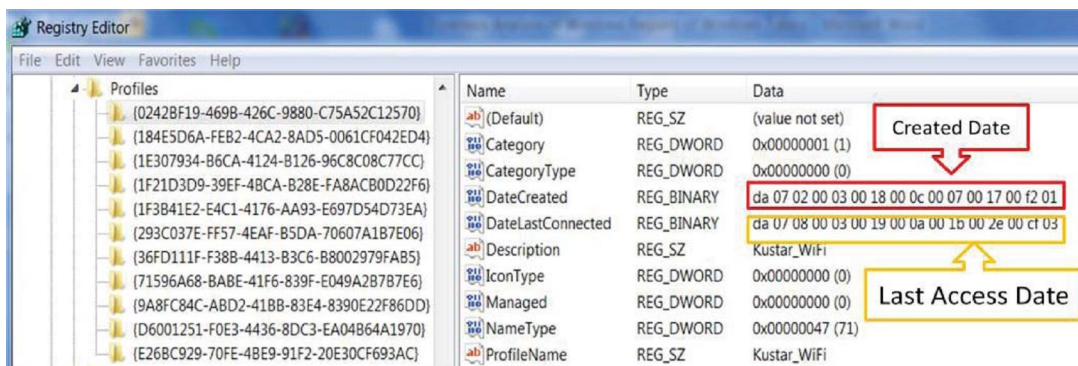


Slika 22 - Spajanje Identifikatora bežične mreže sa njemu odgovarajućim u okviru Windows Registry

Informacije o bežičnim mrežama uključuju datum prvog i datum poslednjeg uspostavljanja veze. One su sačuvane u sledećem podključu *Registry* baze:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\NetworkList\Profiles\{Wireless - Identifier}. Gde je {Wireless - Identifier} identifikator bežične mreže

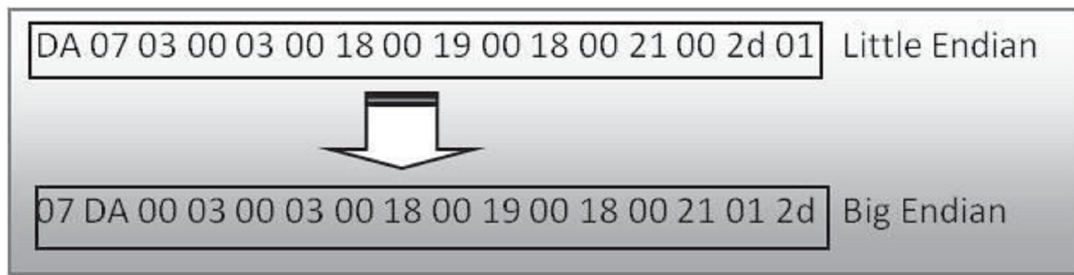
Vrednost DateCreated sadrži datum prvog uspostavljanja veze sa određenom bežičnom mrežom a vrednost DateLastConnected sadrži datum kada je računar poslednji put bio povezan na ovu bežičnu mrežu kako je prikazano na slici 23.



Slika 23 - Datum kada je veza prvi put uspostavljena i datum poslednjeg povezivanja na bežičnu mrežu

Tip ovih vrednosti je binarni tip podataka. Ovo što sledi je objašnjenje kako da se posmatraju ove vrednosti kao normalno vreme datuma dekodirajući `DateCreated` (vreme kad je nastao) i `DateLastConnected` (vreme kada je poslednji put konektovan) i `SSID` vrednosti:

1. Dužina podatka o vrednosti je 16 bajta
2. Uskladišten je uz korišćenje Little Endian, pa ga pretvramo (konvertujemo) u Big Endian pre dekodiranja podataka onako kako je prikazano na slici 24.



Slika 24 - Konverzija DateCreated vrednost iz Registra u format big endian

3. Vrednost godine = 07D = 2010
(Ignoriše se poslednja vrednost na šest decimala koja je [A] u prva dva bajta)
4. Mesec = 00 03 = March
(1= januar, 2= februar ...itd.)
5. Svaka dva bajta imaju odgovarajuću vrednost za godinu, mesec, datum, sat, minut i sekundu.
6. Dan u nedelji = 00 03 = sreda
(0 = nedelja, 1 = ponedeljak ...itd)
7. Datum= 00 18 = 18-ti
8. Čas = 00 19 = 19:00
9. Minuti = 00 18 = 18 minuta
10. Sekunda = 00 21= 21 sekundi

Shodno tome, dekodirani datum je 18. mart 2010 19:18:21 ^[8]

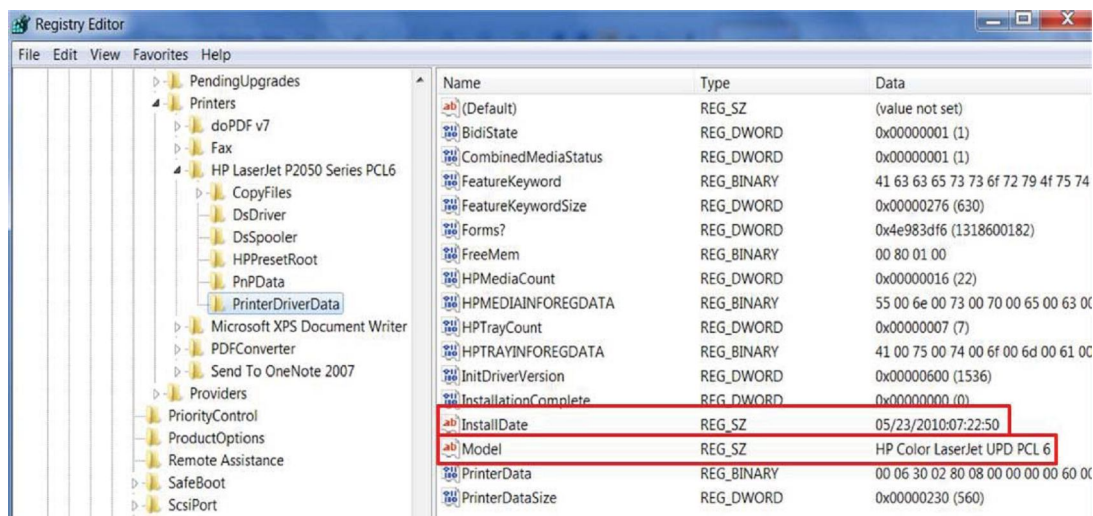
5 - Analiza priključnih uređaja

5.1. Štampači

Nekoliko ključeva unutar *Registry* baze sadrže informacije o štampačima u sistemu. Jedan od ovih ključeva je:

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Print\Printers

U ovom ključu se nalazi lista štampača koji postoje u sistemu. Istražitelj može dobiti više informacija o svakom štampaču ako pristupi PrinterDriverData podključu. Na primer, datum instaliranja i ime modela kako je prikazano na slici 25.



Slika 25 - Značajni podaci o štampačima unutar Windows Registry

5.2 - USB uredjaji

Kada kad se USB uredjaj priključi na sistem, informacije o USB uredjaju ostaju unutar baze registara. Ova informacija može jedinstveno identifikovati svaki USB uredjaj priključen na sistem. Operativni sistem Windows skladišti sledeće identifikacione podatke o USB uredjaju: naziv proizvođača, identifikaciju proizvoda, broj revizije i serijski broj za svaki priključeni USB uredjaj. Ova informacija može se naći u sledećem ključu registra:

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USBSTOR

Slika 26 pokazuje informaciju o USB uredjajima upisanu u prethodnom ključu.



Slika 26 - Informacija o USB uredjajima unutar Windows Registry

6 - Ispitivanje baze registara

6.1 - Registar kao dnevnik (log)

Svi *Registry* ključevi sadrže vrednost koja se vezuje za njih, zvanu 'LastWrite' vreme, koja je veoma slična poslednjem vremenu modifikacije fajla. U odnosu na *Microsoft Knowledge Base*, *FILETIME* struktura predstavlja broj intervala od 100 nanosekundi od 1. januara 1601. *LastWrite* vreme se ažurira kada je *Registry* ključ stvoren, modifikovan, pristupi mu se ili je izbrisan. Na nesreću, samo *LastWrite* vreme ključa registra se može dobiti, dok *LastWrite* vreme za vrednost u registru ne može.

Harlan Karvi, autor dela "Windows forenzika" i "Oporavljanje od incidenata" upućuje na alat zvani Keytime.exe, koji dozvoljava ispitivaču da povрати (ponovo izvuče) *LastWrite* bilo kog specifičnog ključa.

To što zna *LastWrite* vreme ključa može dozvoliti forenzičkom analitičaru da zaključi približni datum ili vreme kada se događaj desio. I iako možete znati poslednje vreme kada je ključ u *Registry* bazi modifikovan, još uvek ostaje teško odrediti koja vrednost je stvarno promenjena. Korišćenje *Registry* baze kao dnevnika (log) je najviše od pomoći u korelaciji između *LastWrite* vremena *Registry* ključa i drugih izvora informacija, poput *MAC* (modifikovano, pristupljeno ili stvoreno) vremena nadjenih unutar fajl sistema. Ipak, sveobuhvatna diskusija tog procesa je van opsega ovog rada.

6.2 - Autorun lokacije

Autorun lokacije su ključevi *Registry* baze koji pokreću programe ili aplikacije u toku boot procesa (procesa koji pokreće operativni sistem kada korisnik uključi kompjuter).

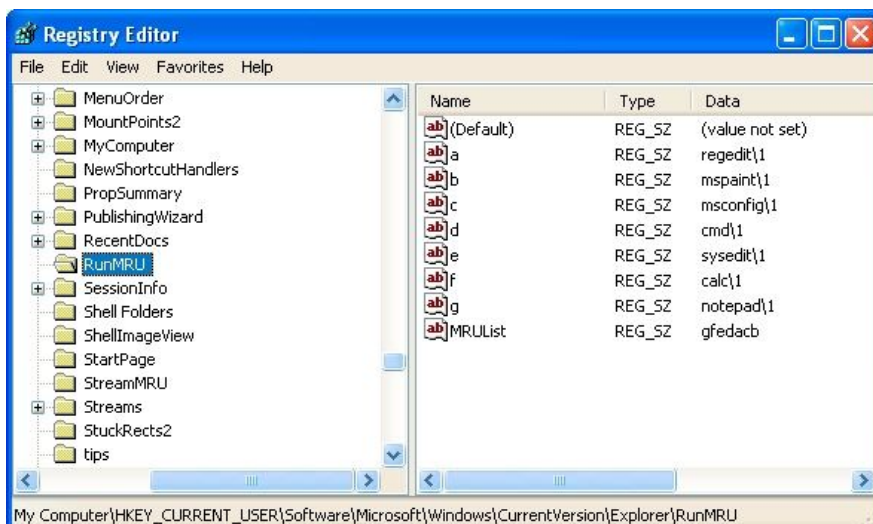
Lista uobičajenih autorun lokacija:

```
HKLM\Software\Microsoft\Windows\CurrentVersion\Runonce  
HKLM\Software\Microsoft\Windows\CurrentVersion\policies\Explorer\Run  
HKLM\Software\Microsoft\Windows\CurrentVersion\Run  
HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run  
HKCU\Software\Microsoft\Windows\CurrentVersion\Run  
HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce  
(ProfilePath)\Start Menu\Programs\Startup
```

6.3 - MRU liste

MRU, ili ‘najsكورije korišćen’ liste sadrže upise u listu načinjene usled akcija koje je izvršio korisnik. Postoje brojne MRU liste locirane posvud unutar različitih *Registry* ključeva. *Registry* održava ove liste pojedinačnih stvari za slučaj da im se korisnik vrati u budućnosti. To je u osnovi slično tome kako *history* i *cookies* deluju na *web browser*. Jedan primer MRU liste locirane u *Windows Registry* bazi je RunMRU ključ. Kada korisnik ukuca komandu u ‘Run’ dijalog boks preko Start menija, upis na listu se dodaje *Registry* ključu. Lokacija ovog ključa je HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU i njegov sadržaj se može videti na slici 27. Hronološki red aplikacija izvršenih preko ‘Run’ može se odrediti pogledavši u Data kolonu ‘MRUList’ vrednosti. Prvo slovo ovoga je ‘g’ što nam govori da je poslednja komanda otkucana u ‘Run’ prozoru bila da se pokrene (izvrši) notepad. Takođe, LastWrite vreme RunMRU ključa biće u korelaciji sa poslednjom aplikacijom izvršenom u ‘Run’, ili u ovom slučaju aplikacijom ‘g’^[8].

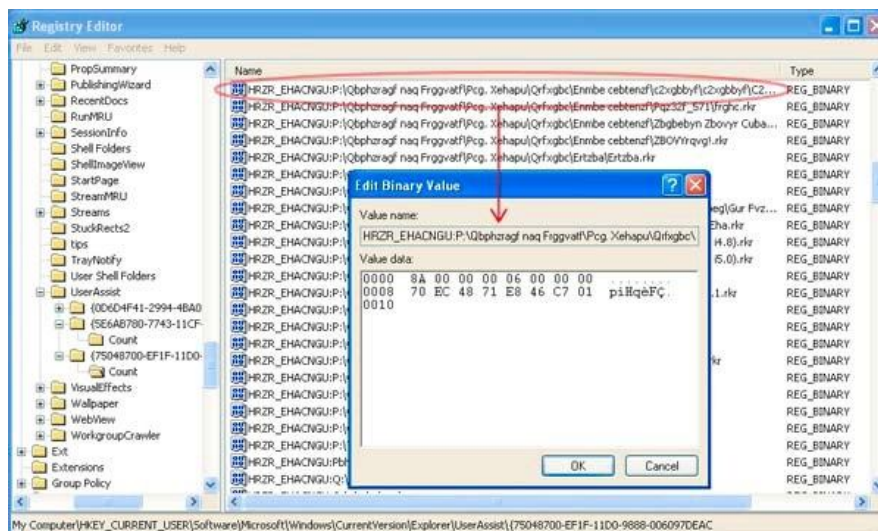
Sa informacijama obezbeđenim iz RunMRU ključa, ispitivač može doći do boljeg razumevanja korisnika koji je pod istragom i aplikacija koje se koriste. Sa slike 27, očigledno je da korisnik ima dovoljno znanje o Windows operativnom sistemu – zasnovano na aplikacijama koje su pokrenute (izvršene), poput msconfig, cmd, sysedit, and regedit.



Slika 27 - RunMRU ključ

6.4 - UserAssist

UserAssist ključ HCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist sadrži dva ili više podključeva koji imaju duga heksadecimalna (sa 6 decimala) imena koja se pojavljuju kao globalno jedinstveni identifikatori (GUIDs - *globally unique identifiers*). Svaki podključ beleži vrednosti koje se odnose na specifične stvari kojima je korisnik pristupio, poput apleta *Control Panel*, fajlova prečica, programa itd. Ove vrednosti su kodirane uz korišćenje ROT-13 algoritma za šifrovanje, ponekad znanog kao šifra Cezar. Ova posebna tehnika šifrovanja je laka za dešifrovanje, pošto se svaki znak zamenjuje znakom 13 mesta udaljenim od njega u ASCII tabeli. Mnogo brži i lakši metod za dešifrovanje ovog koda je korišćenjem ROT-13 dekodera [8].



Slika 28 - UserAssist ključ

Sa UserAssist ključem, forenzički istražitelj može doći do boljeg razumevanja toga kojim tipovima fajlova ili aplikacija je pristupano u određenom sistemu. Čak iako ovi podaci nisu definitivni, jer se ne mogu vezivati za specifičan datum i vreme, to bi moglo ipak ukazivati na specifično delanje korisnika.

Na primer, u primeru sa slike 28 dekodirana vrednost može ukazati na potencijalno veliku količinu informacija. Prvo, govori ime profila korisnika - 'Cpt. Krunch' - iz koga je .exe pokrenuto (izvršeno). Cpt. Krunch bi takodje moglo ukazivati na neku vrstu pseudonima. Drugo, pretraživanje 'p2ktools.exe', kazuje da je program korišćen za uređivanje (editing) i upravljanje Motorola mobilnim telefonima. Konačno, pokazuje da korisnik ima p2ktools folder u matičnom direktorijumu zvanom 'Razor programs', koji je lociran na njegovom/njenom desktopu. Ne samo da ovo daje lokaciju gde bi se mogli biti nalaziti slični programi, nego je i ime ovog direktorijuma dobar indikator da osumnjičeni ima mobilni telefon Motorola Razor. Ako je tako, njega bi takodje trebalo oduzeti za dalju analizu.

6.5 - Liste istorije

Liste istorije (*History*) ističu najskoriju aktivnost u sistemu. Na primer, nedavno posećivane web stranice ili skoro otvarane Word datoteke. Postoji nekoliko podključeva u registru koji pokazuju skorašnju aktivnost korisnika sistema. Tabela 9 prikazuje listu istorije sa odgovarajućim podključevima u *Windows Registry* bazi.

Tabela 9 - Liste istorije ^[8]

Lista istorije	Podključ koji se odnosi na listu istorije
Otkucani URL-ovi u Microsoft Internet Explorer-u	HKEY_USERS\S-1-5-21-[User Identifier] \Software\Microsoft\InternetExplorer\TypedURLs
Microsoft Word datoteke	HKEY_USERS\S-1-5-21-[User Identifier] \Software \Microsoft\Office\12.0\Word\File MRU
Microsoft Power Point datoteke	HKEY_USERS\S-1-5-21-[User Identifier] \Software\Microsoft \Office\12.0\PowerPoint\File MRU
Microsoft Excel datoteke	HKEY_USERS\S-1-5-21-[User Identifier] \Software \Microsoft \Office\12.0\Excel\File MRU
Acrobat Reader datoteke	HKEY_USERS\S-1-5-21-[User Identifier] \Software\Adobe\AcrobatReader\9.0\AVGeneral\cRecentFiles
WinRAR files	HKEY_USERS\S-1-5-21-[User Identifier] \Software \WinRAR \ArcHistory
Najskorije mapirana mreža	HKEY_USERS\S-1-5-21-[User Identifier] \Software \Microsoft \Windows\CurrentVersion\Explorer\Map Network Drive MRU
Najskorije korišćene pozadine za ekran desktopa	HKEY_USERS\S-1-5-21-[User Identifier] \Software \Microsoft
Najskorije otkucana komanda u RUN dijalogu	HKEY_USERS\S-1-5-21-[User Identifier] \Software \Microsoft \Windows\CurrentVersion\Explorer\RunMRU
.GIF datoteke (fajlovi)	HKEY_USERS\S-1-5-21-[User Identifier] \Software \Microsoft \Windows\CurrentVersion\Explorer\RecentDocs\gif
.jpg datoteke	HKEY_USERS\S-1-5-21-[User Identifier] \Software \Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\jpg
text datoteke	HKEY_USERS\S-1-5-21-[User Identifier] \Software \Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\txt
Folderi	HKEY_USERS\S-1-5-21-[User Identifier] \Software \Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\Folder
Zip fajlovi	HKEY_USERS\S-1-5-21-[User Identifier] \Software \Microsoft \Windows\CurrentVersion\Explorer\RecentDocs\zip

7 - Značaj forenzičke analize Windows baze registara

Analiza sistema obezbeđuje forenzičkom istražitelju vredne informacije o sistemu. Ona daje forenzičkom istražitelju sliku o sposobnostima obrade podataka mašine za koju se sumnja, poput imena procesora, brzine procesora, porodice (grupa srodnih sistema) sistema, imena sistema i verzije sistema. Sem toga, forenzički istražitelj će dobiti imena, identitet ili nadimke ljudi koji su koristili mašinu iz liste korisničkih naloga. Poslednje vreme isključivanja će pružiti forenzičkom istražitelju informaciju o tome kada je poslednji put korišćena mašina. Ovo bi moglo ukazati da ova mašina nije vezana za konkretan kriminalni akt.

Analiza aplikacija obezbeđuje forenzičkom istražitelju informacije o aplikacijama koje su bile instalirane na mašini. Forenzički istražitelj bi trebao da proveri *startup* programe, pošto bi tu mogao pronaći zlonamerne programe koji bi mogli kontrolisati sumnjivu mašinu, a sistem je mogao pokretati napadač, umesto legitimnog korisnika mašine. Na primer, ako je mašina bila korišćena da se izvrši aktivnost poput DoS napada, korisnik sistema možda nije bio taj koji je izvršio ovaj napad.

Istražitelj može otkriti programe koji su korišćeni da se izvrši kriminalni akt. Na primer, u slučaju piratskog kopiranja softvera, može se desiti da kriminalac koristi uređaje za narezivanje kompakt i DVD diskova i štampanje etiketa. Takodje, može se desiti da izvršilac nezakonitog dela koristi kodove za aktiviranje softvera i kodove za dupliranje softvera. Stoga, kad bi forenzički istražitelj našao bilo koji od gore navedenih programa, to se može smatrati za potencijalni digitalni dokaz. Povrh toga, forenzički istražitelj će biti zainteresovan da zna da li je korisnik mašine koristio aplikaciju za četovanje (ćaskanje) poput *Microsoft Windows Live Messenger*-a i *Skype*-a. Takodje je važno da sazna naziv naloga za čet koji je korisnik sumnjive mašine koristio. Na primer, u slučajevima koji uključuju zlostavljanje dece, može se desiti da kriminalac komunicira sa detetom koristeći *Microsoft Windows Live Messenger* ili/i *Skype*. Naziv naloga saznajemo sa detetove liste kontakata i onda tražimo nalog kriminalca kao skorašnjeg korisnika. Ovo se smatra potencijalnim digitalnim dokazom ^[8].

Analiza mreže pružice forenzičkom istražitelju pregled aktivnosti povezivanja (umrežavanja). Sa liste kartica mreže, forenzički istražitelj može identifikovati sve kartice koje je sistem koristio, bilo da su bile ugrađene u sistem ili spolja povezane na sistem. Takodje, on će pronaći listu internih mreža na koje je bila povezana konkretna mašina. Isto važi i za bežične mreže na koje se sistem povezivao, uključujući imena bežičnih mreža, datum konekcije i datum poslednjeg povezivanja na mrežu.

Analiza priključenih uređaja daće forenzičkom istražitelju informacije o uređajima koji su bili povezani na sistem. Ona uključuje dve kategorije priključenih uređaja, štampače i USB uređaje. Lista štampača i njihove informacije kao ime modela i datum instaliranja su vredne informacije forenzičkom istražitelju i mogle bi se smatrati kao potencijalni digitalni dokaz. Na primer u zločinu falsifikovanja, kriminalac će normalno koristiti štampače visokog kvaliteta da proizvede kreditnu karticu koja izgleda kao original. Za forenzičkog istražitelja važno je da zna koji USB uređaji su priključeni na sistem i podatke kao što su identifikacija proizvoda i serijski broj, posebno u slučaju krađe podataka iz kompjutera ^[8].

Lista istorije obezbeđuje forenzičkom istražitelju najskorije aktivnosti svakog korisnika u sistemu, poput otkucanih URL-ova u *Microsoft Internet Explorer*-u i u najskorije vreme korišćenih *Microsoft Word* fajlova.

Pregled lista otvaranih .jpg i .GIF fajlova mogu obezbediti forenzičkom istražitelju digitalne dokaze o otvaranim slikama.

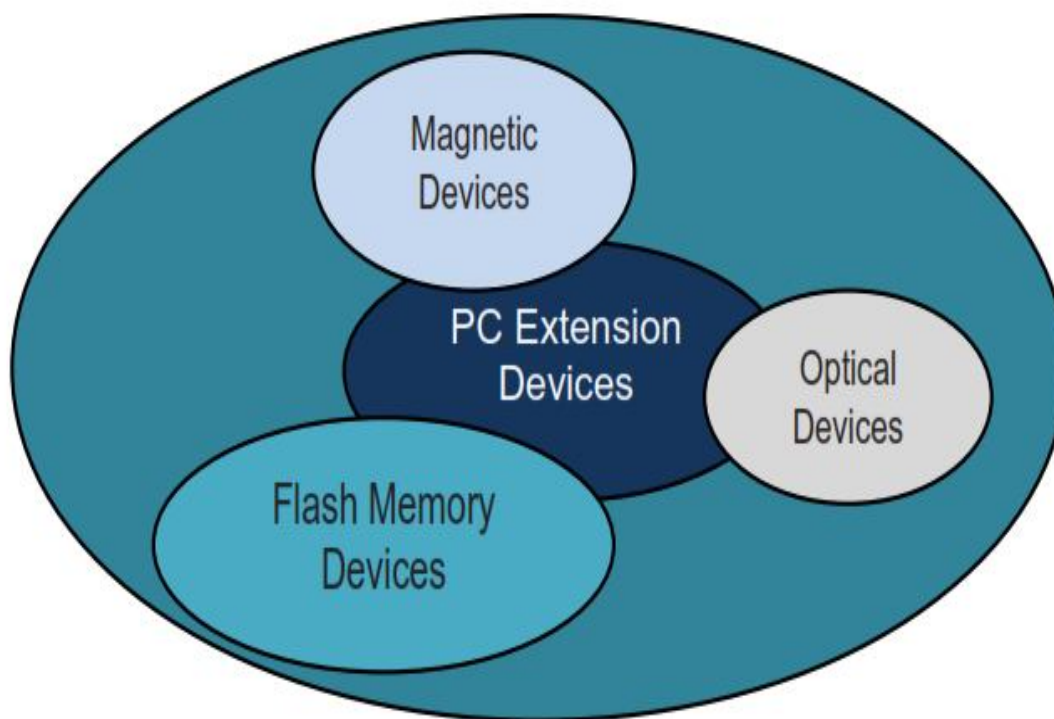
IV – Forenzička analiza USB uređaja za skladištenje podataka

1 - Opis i karakteristike USB uređaja za skladištenje podataka

USB uređaji za skladištenje podataka, tzv. fleš diskovi, su postali veoma čest, može se reći standardan uređaj za skladištenje različitih kategorija podataka u digitalnom obliku. Malih su dimenzija i samim tim pogodni za nošenje u tašni, džepu ili kao privezak za ključeve. Posmatrano sa drugog aspekta, lako ih je sakriti. Iz navedenog se može zaključiti da su ovi uređaji veoma pogodni kako za legalnu tako i ilegalnu upotrebu.

Kao posledica prave poplave na tržištu, USB uređaji za skladištenje podataka su dostupni svakome. U pojedinim državama broj prodatih USB uređaja za skladištenje podataka je veći od broja stanovnika. Iz navedenog se može zaključiti da ovi uređaji zauzimaju prvo mesto po potencijalu koji imaju kao predmet digitalnih forenzičkih istraga.

Slika 29 prikazuje udeo koji USB uređaji za skladištenje podataka imaju u digitalnim forenzičkim istragama u odnosu na druge tipove uređaja za memorisanje podataka.



Slika 29 – Udeo koji USB uređaji za skladištenje podataka imaju u digitalnim forenzičkim istragama u odnosu na druge tipove uređaja za memorisanje podataka^[13]

Kapacitet skladištenja podataka ovih uređaja omogućava skladištenje velike količine informacija tako da poznavanje načina funkcionisanja predstavlja imperativ u oblasti digitalne forenzike.

Prenosivi USB uređaji za skladištenje podataka, za razliku od ostalih uređaja za skladištenje podataka, koriste poluprovodničku tehnologiju – čipove za čuvanje podataka. Imaju malu potrošnju energije i napajaju se preko USB priključka na računar. Ova vrsta memorijkih čipova se naziva fleš (*flash*) memorijom. Otuda se za ovu vrstu uređaja odomaćio naziv - USB fleš.

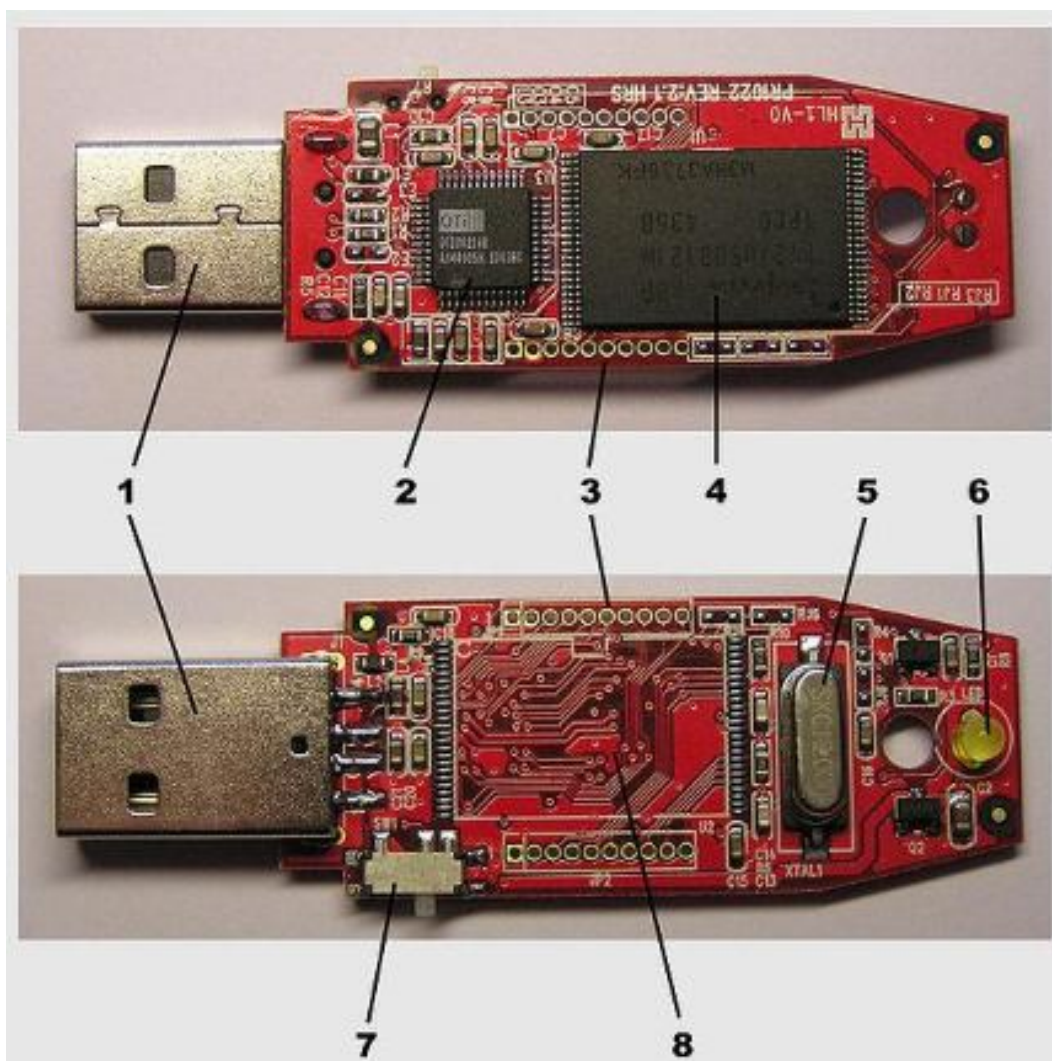
Fleš memoriji nije potrebno električno napajanje da bi se sačuvali podaci. U idealnim uslovima trajnost upisa podataka je oko 10 godina.

Ovi uređaji su se pojavili 2003 godine, početni kapacitet im je bio 16 megabajta i koristili su USB 1,0/1,1 interfejs. Od 2004 godine ovi uređaji koriste USB 2.0 interfejs koji ima maksimalnu brzinu čitanja od 100 Mb/s. Do današnjih dana kapacitet im je drastično porastao, do više desetina gigabajta.

Veliki kapacitet, male dimenzije, velika brzina čitanja i pisanja su učinili ovu vrstu uređaja veoma popularnom, što ih čini veoma interesantnim u oblasti digitalne forenzike.

Posebno treba naglasiti da je način upisivanja, čitanja i brisanja podataka na fizičkom nivou značajno različit odnosu na magnetne čvrste diskove i RAM memoriju. Memorijske ćelije koje se nalaze u ovim uređajima mogu podneti ograničen broj upisivanja podataka, tipično između 10.000 i 1.000.000 puta, pre nego što postanu nestabilne.

Na slici 30 je prikazan izgled unutrašnjosti USB uređaja za skladištenje podataka.



Slika 30 - Izgled unutrašnjosti USB uređaja za skladištenje podataka

Na slici 30 vide se sledeći elementi USB uređaja za skladištenje podataka:

1. USB konektor
2. Kontroler memorijskog čipa
3. Štampana pločica
4. Memorijski čip
5. Kristal generatora takta
6. LED pokazivač statusa uređaja
7. Mikroprekidač za *read only* režim rada

Memorija u ovim uređajima može biti:

1. NOR fleš memorija koja dozvoljava i podržava brzo čitanje i upisivanje podataka ali po visokoj ceni.
2. NAND fleš memorija novijeg je datuma. Njena prednost je u tome što se po niskoj ceni može postići veliki kapacitet skladištenja podataka, a mana joj je manja brzina čitanja u upisivanja veće količine podataka.

Brisanje podataka sa ovih uređaja se obavlja na potpuno različit način u odnosu na sve ostale vrste memorijskih uređaja. Na novom uređaju celokupna memorija ima vrednost 1. Tokom procesa upisivanja podataka pojedini se bitovi postavljaju na vrednost 0. Jedini način da se podaci u memoriji prepisu drugim podacima je da se, kao prvo, memorijske ćelije operacijom brisanja vrata na vrednost 1 a zatim upišu novi podaci.^[13]

Zavisno od tipa memorije operacija brisanja sadržaja memorijskih ćelija se obavlja na sledeći način:

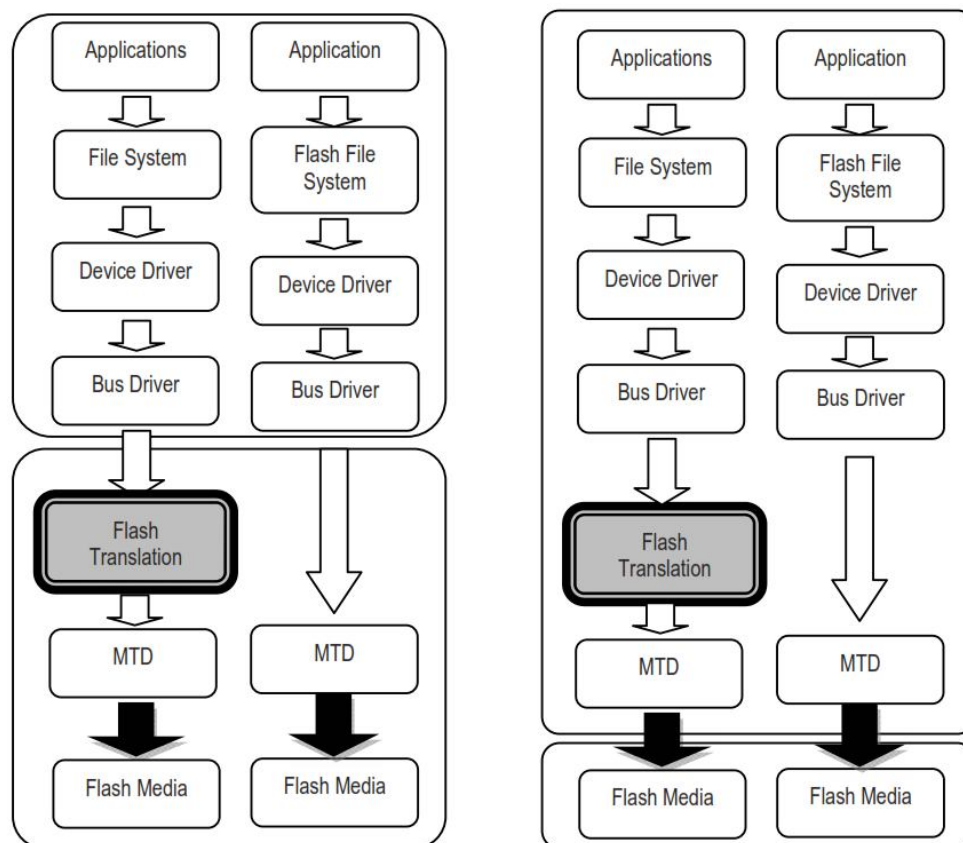
1. NOR memoriju je moguće brisati bit po bit
2. NAND memorija je podeljena na blokove. Svaki blok sadrži predefinisani broj stanica fiksne veličine. Svaka stranica je podeljena na regione u kojima se skladište podaci. Jedan region u okviru stranice je rezervisan za čuvanje statusa ostalih regiona sa podacima. Pri svakoj izmeni postojećih podataka novi podaci se upisuju na neku drugu dostupnu lokaciju (stranicu) a prethodna lokacija se označava kao nedefinisana i u tom stanju čeka sledeću operaciju brisanja. Posle izvesnog vremena akumulira se broj ovakvih stranica koje se potom brišu i ponovo postaju dostupne za nove podatke. Ova operacija se u slengu naziva „sakupljanje đubreta“ (*garbage collection*). Pošto svaki memorijski blok ima ograničen broj brisanja ono se obavlja po posebnoj strategiji kako bi se vek trajanja memorijskog uređaja maksimalno produžio.

Da bi se USB memorijski uređaj koristio na personalnom računaru moramo instalirati drajvere koji će fizičku strukturu memorije ovog uređaja predstaviti na način koji je poznat računaru i operativnom sistemu koji se nalazi na tom računaru. Ovi drajveri predstavljaju memorijski uređaj računaru kao *block device* što po tipu odgovara hard disku.

Na slici 31 prikazan je način funkcionisanja ovih drajvera za dva tipa memorijskih uređaja.

Značenja skraćenica sa slike su:

FTL – Flash Translation Layer
MTD – Memory Tehnology Device



Slika 31 – Prikaz funkcionisanja FTL i MTD drajvera za dva tipa memorijskih uređaja^[13]

Pomenuti drajveri mapiraju fizičku strukturu flash memorije u logičku strukturu koja je poznata operativnom sistemu računara.

Vidjeno sa strane operativnog sistema, memorijski uređaj ovog tipa se vidi kao hard disk te se može formatirati istim fajl sistemom kao i svaki (magentni) hard disk. Do skoro je to najčešće bio FAT fajl sistem. Međutim, kako FAT fajl sistem ima brojna ograničenja u pogledu veličine i broja fajlova i poddirektorijuma, a kapacitet za skladištenje podataka eksponencijalno raste, u novije vreme sve češće nailazimo na USB uređaje za skladištenje podataka formatirane nekim naprednijim fajl sistemom kao što je *Windows NTFS* fajl system. Novije verzije Windows operativnog sistema podržavaju formatiranje NTFS fajl sistemom, što u starijim verzijama ovog operativnog sistema nije bio slučaj, već se za tako nešto morao koristiti poseban alat kao što je recimo *HP Tool*.

Kako detalji funkcionisanja USB memorijskih uređaja na fizičkom nivou nisu predmet istraživanja u ovom radu oni neće dalje biti razmatrani.

2 - USB uređaji za skladištenje podataka u Windows okruženju

2.1 - Prvo priključivanje USB uređaja za skladištenje podataka na računar sa Windows operativnim sistemom

Pri prvom priključivanju memorijskog USB uređaja za skladištenje podataka na računar pod Windows operativnim sistemom zapravo pokrećemo čitav niz procesa u cilju automatskog prepoznavanja i konfiguracije priključenog uređaja.

Operativni sistemi kompanije *Microsoft* pri uključivanju uređaja u USB port najpre pozivaju informacije uskladištene u USB *hub* drajveru iz kojeg dobija informaciju o tipu povezanog uređaja. Nakon detekcije tipa uređaja, Windows traži drajvere za sam uređaj, a za sve to potrebno je da ima sve informacije o uređaju. Tom prilikom operativni sistem pravi jedinstveni profil USB uređaja. Nakon formiranja profila Windows traži potrebne instrukcije za rad u *usbstor.inf* fajlu, a zatim i preko *Windows Update* servisa (ako je računar povezan na internet i ako je korisnik to dozvolio ranijim podešavanjima). Ako ne pronade drajver za konkretan uređaj, pokreće se generički drajver - *generic mass storage device*.

Sve informacije o prepoznatom uređaju Windows upisuje u svoju bazu registara tako da pri sledećem priključivanju uređaja može odmah pokrenuti prethodno priključivan uređaj a da pri tome ne pokreće postupak prepoznavanja i konfigurisanja uređaja. U prethodnom poglavlju koje se bavi forenzičkom analizom *Windows registry* baze prikazano je gde i kako Windows operativni sistem upisuje i čuva ove informacije. Jednom upisane, ove informacije ostaju trajno upisane u bazu registara. Sam operativni system ih neće brisati. Naravno, ove informacije se mogu izmeniti ili obrisati izmenom sadržaja ili brisanjem pojedinih ključeva u bazi registara.

Informacije na osnovu kojih se vrši pretraživanje u *usbstor.inf* nalaze se u samom hardveru.

Na Windows sistemima identifikator uređaja formira se u formatu `USB\VID_v(4)&PID_d(4)&REV_r(4)`.

Po informacijama kompanije Microsoft

v(4) je četvorocifreni broj proizvođača, dodeljen od strane nadležnih komisija,
d(4) – broj koji proizvođač dodeljuje uređaju, a
r(4) je revizija koda.

Ilustrovano na konkretnom uređaju u device manager-u
`USB\VID_08EC&PID_0008\0CD02851333229`, gde je:

08EC kod proizvođača,
0008 kod proizvoda, a
0CD0 je revizioni kod.

Svi indetifikatori su jedinstveni i predstavljaju ID uređaja (*Device Instance ID*).

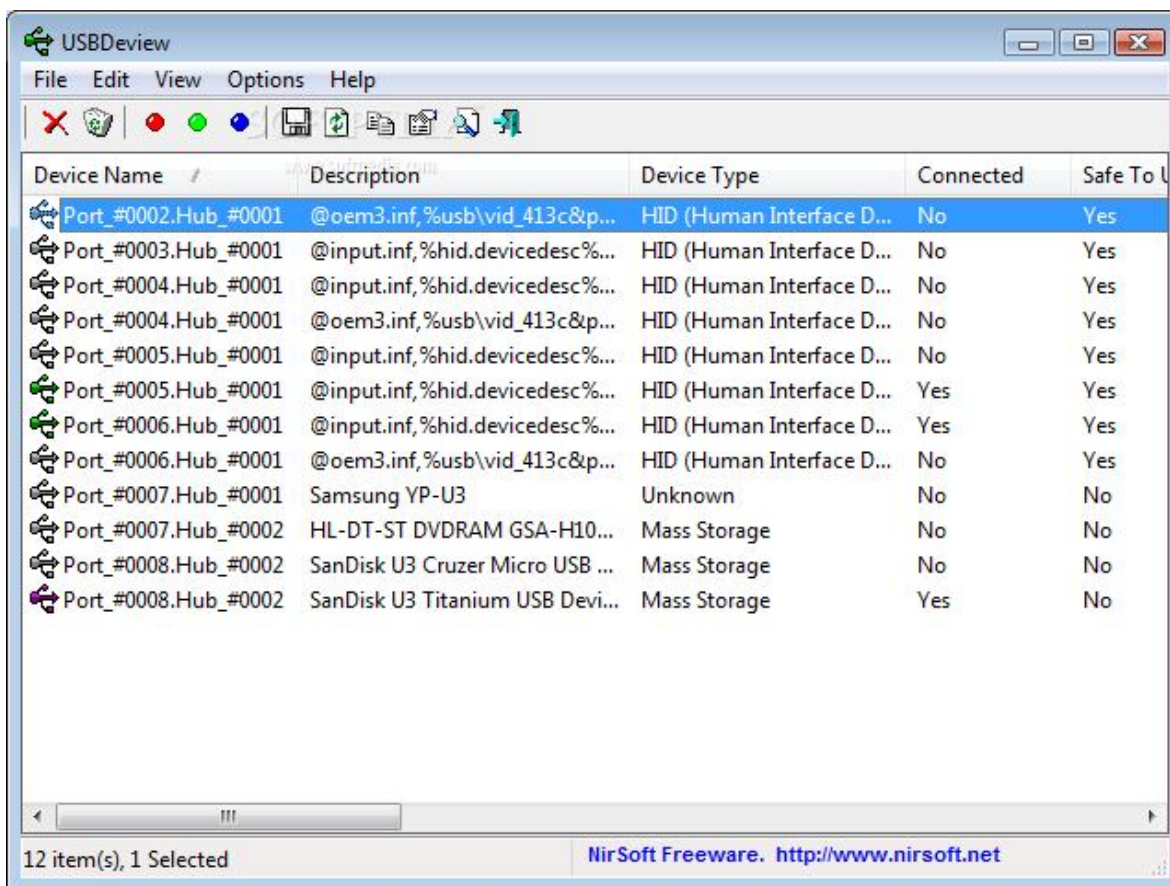
Iako svi ovi identifikatori postoje u sistemu, u današnje vreme se ne mogu okarakterisati kao pouzdani i neporecivi u procesu prikupljanja digitalnih dokaza. Razlog tome, osim

uništavanja dokaza jeste i to što danas postoji veliki broj NO NAME proizvođača, koji pri proizvodnji ne upisuju sve potrebne podatke u sam uređaj tj. pre proizvodnje ne kontaktiraju “USB Implementers Forum”- fondaciju postojećih proizvođača kako bi pribavili i registrovali odgovarajuće kodove proizvođača i proizvoda.

2.2 - Program *USBDeview*

Osim metode pretraživanja registry baze, podatke o USB uređajima je moguće prikazati ili odrisati. Postoje brojni softverski alati koji pouzdano i sortirano prikazuju sve informacije o USB uređajima iz registry baze. Među njima najviše se izdvojio *USBDeview*, alat kompanije NirSoft, koji se osim za pregled dokaza može koristiti i za njihovo uništavanje.

Na slici 32 vidi se aktivan program *USBDeview* koji prikazuje podatke o USB uređajima na sistemu.



The screenshot shows the USBDeview application window. It has a menu bar (File, Edit, View, Options, Help) and a toolbar with various icons. The main area is a table with the following columns: Device Name, Description, Device Type, Connected, and Safe To U. The table lists 12 items, with the first item selected. The status bar at the bottom indicates '12 item(s), 1 Selected' and provides the NirSoft Freeware website URL.

Device Name	Description	Device Type	Connected	Safe To U
Port_#0002.Hub_#0001	@oem3.inf,%usb\vid_413c&p...	HID (Human Interface D...	No	Yes
Port_#0003.Hub_#0001	@input.inf,%hid.device-desc%	HID (Human Interface D...	No	Yes
Port_#0004.Hub_#0001	@input.inf,%hid.device-desc%	HID (Human Interface D...	No	Yes
Port_#0004.Hub_#0001	@oem3.inf,%usb\vid_413c&p...	HID (Human Interface D...	No	Yes
Port_#0005.Hub_#0001	@input.inf,%hid.device-desc%	HID (Human Interface D...	No	Yes
Port_#0005.Hub_#0001	@input.inf,%hid.device-desc%	HID (Human Interface D...	Yes	Yes
Port_#0006.Hub_#0001	@input.inf,%hid.device-desc%	HID (Human Interface D...	Yes	Yes
Port_#0006.Hub_#0001	@oem3.inf,%usb\vid_413c&p...	HID (Human Interface D...	No	Yes
Port_#0007.Hub_#0001	Samsung YP-U3	Unknown	No	No
Port_#0007.Hub_#0002	HL-DT-ST DVD-RAM GSA-H10...	Mass Storage	No	No
Port_#0008.Hub_#0002	SanDisk U3 Cruzer Micro USB ...	Mass Storage	No	No
Port_#0008.Hub_#0002	SanDisk U3 Titanium USB Devi...	Mass Storage	Yes	No

Slika 32 - Program *USBDeview*, prikaz podataka o USB uređajima na sistemu

Program USBDeview pronalazi i prikazuje sve podatke o USB uređajima koji se mogu pronaći u *Windows Registry* bazi, pa čak i potrošnju električne energije svakog uređaja. Sa druge tačke gledišta, onoliko koliko je dobar u prikazivanju, filtriranju i sortiranju podataka toliko je dobar i u postupku uklanjanja podataka o USB uređajima sa sistema.

U praksi, ovakvi programi se često koriste za pouzdano uklanjanje digitalnih dokaza, što digitalnom foranzičaru u mnogome otežava, a u pojedinim slučajevima i onemogućava pronalaženje digitalnih dokaza.

3 - Program za trajno brisanje podataka sa memorijskih uređaja *Active KillDisk*.

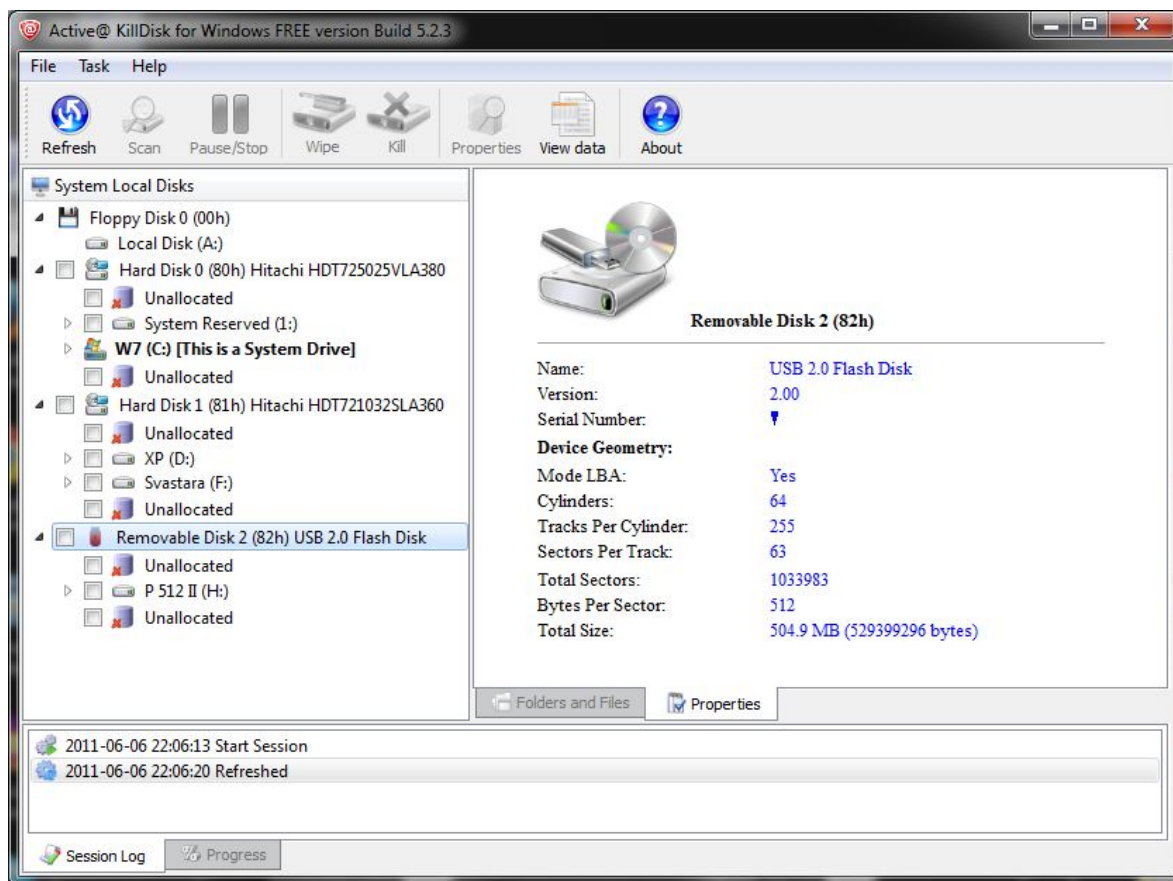
Active KillDisk jedan je od najpoznatijih programa za trajno brisanje (*wipe*) celokupnog sadržaja svih vrsta diskova, samim tim i za brisanje sadržaja USB fleš diskova. Potpuno i nepovratno uništava celokupan sadržaj upisan na disku, uključujući podatke o particijama.

Posle brisanja podataka nije moguće podatke oporaviti.

Pri testiranju na USB fleš disku program je bio toliko temeljan u uklanjanju podataka da je, posle brisanja, formatiranje diska bilo neuspešno u više pokušaja. Windows 7 je uspeo da formatira fleš disk obrisano ovim programom tek posle nekoliko pokušaja, dok je Windows XP u tome bio uspešan iz prvog pokušaja.

Ni jedan, od tri programa za oporavak podataka koji su testirani nije uspeo da povрати bilo kakav podatak sa fleš diska obrisano *Active KillDisk* programom.

Izgled programa *Active KillDisk* prikazan je na slici 33.



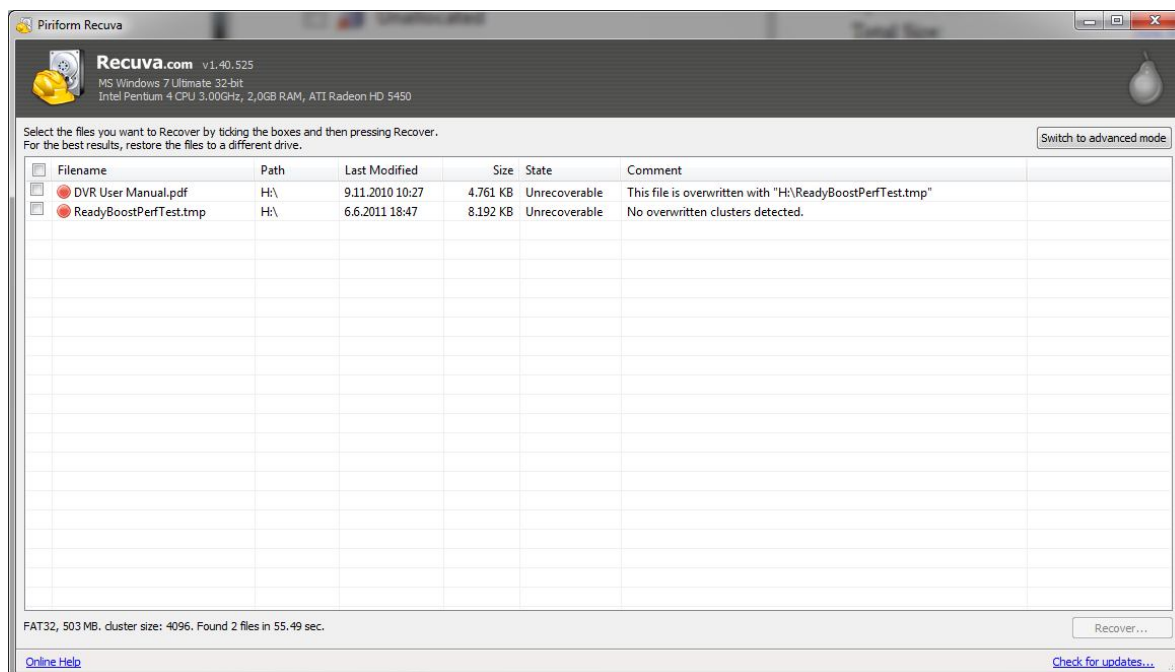
Slika 33 - Izgled programa Active KillDisk

4 - Programi za oporavak obrisanih fajlova sa memorijskih USB uređaja

4.1 - Recuva

Recuva je jedan od najpoznatijih programa za oporavak obrisanih fajlova, prvenstveno sa medija koji koriste poluprovodničku memoriju. Tek u novije vreme se nalazi na forenzičkim distribucijama iako odavno pokazuje dobre rezultate pri oporavku podataka. Program u suštini nije namenjen forenzičarima već običnim korisnicima. Ima intuitivan interfejs i besplatan je.

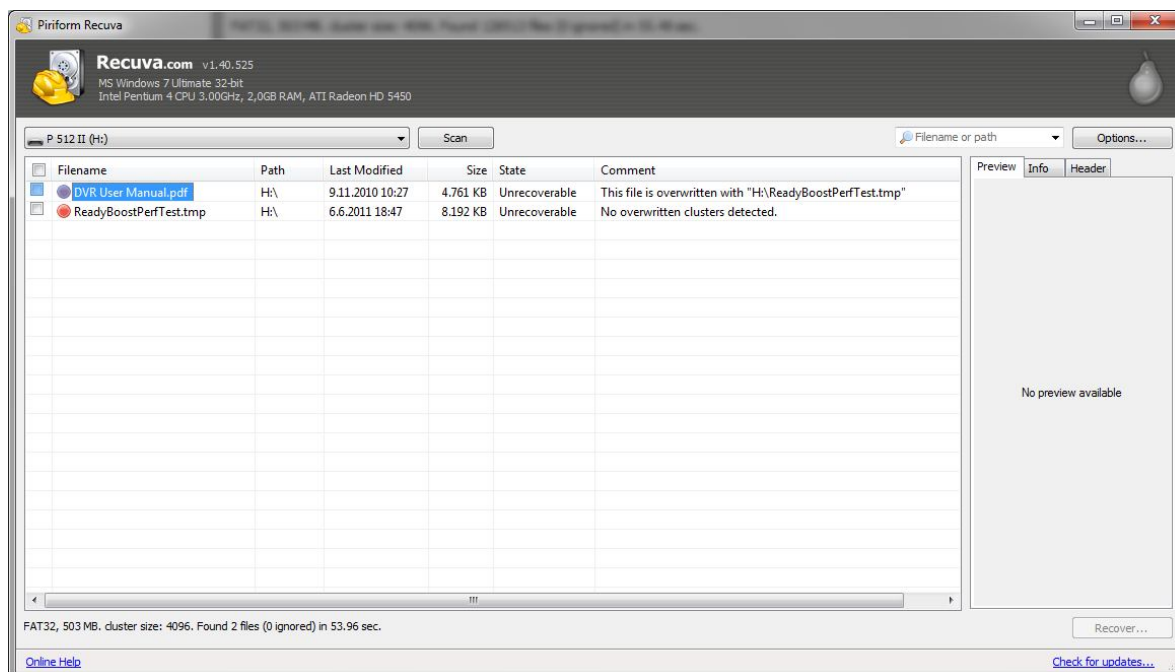
Izgled programa *Recuva* prikazan je na slici 34.



Slika 34 - Izgled programa Recuva

Pri testiranju, program *Recuva* pokazao je dobre rezultate ali tek sa uključenom opcijom *DeepScan*. Ovakav način rada donekle vremenski produžava proces oporavka fajlova zbog toga što se na današnjim fleš diskovima nalazi velika količina podataka.

Izgled programa Recuva u Advaced modu prikazan je na slici 35.



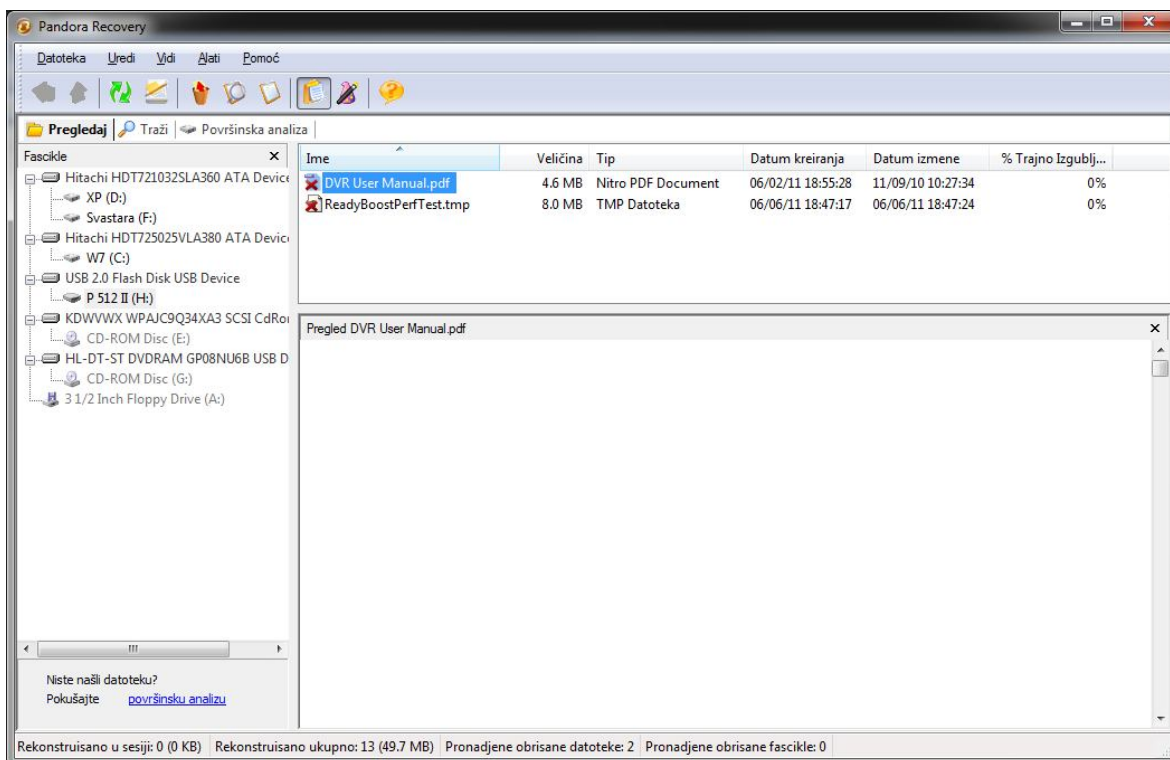
Slika 35 - Izgled programa Recuva u Advaced modu

4.2 - Pandora Recovery

Pandora Recovery, takođe, je jedan od besplatnih programa za oporavak obrisanih fajlova, prvenstveno sa medija koji koriste poluprovodničku memoriju.

Pri testiranju je bio dobar u pronalaženju obrisanih fajlova, međutim, nije uspeo da prepozna koje fajlove je moguće oporaviti. Svaki pronađeni fajl će “oporaviti” ali po “oporavku” oštećeni fajlovi, naravno, neće biti čitljivi. Pretraživanje DeepScan opcijom daje daleko bolje rezultate.

Izgled programa *Pandora Recovery* prikazan je na slici 36.



Slika 36 - Izgled programa Pandora Recovery

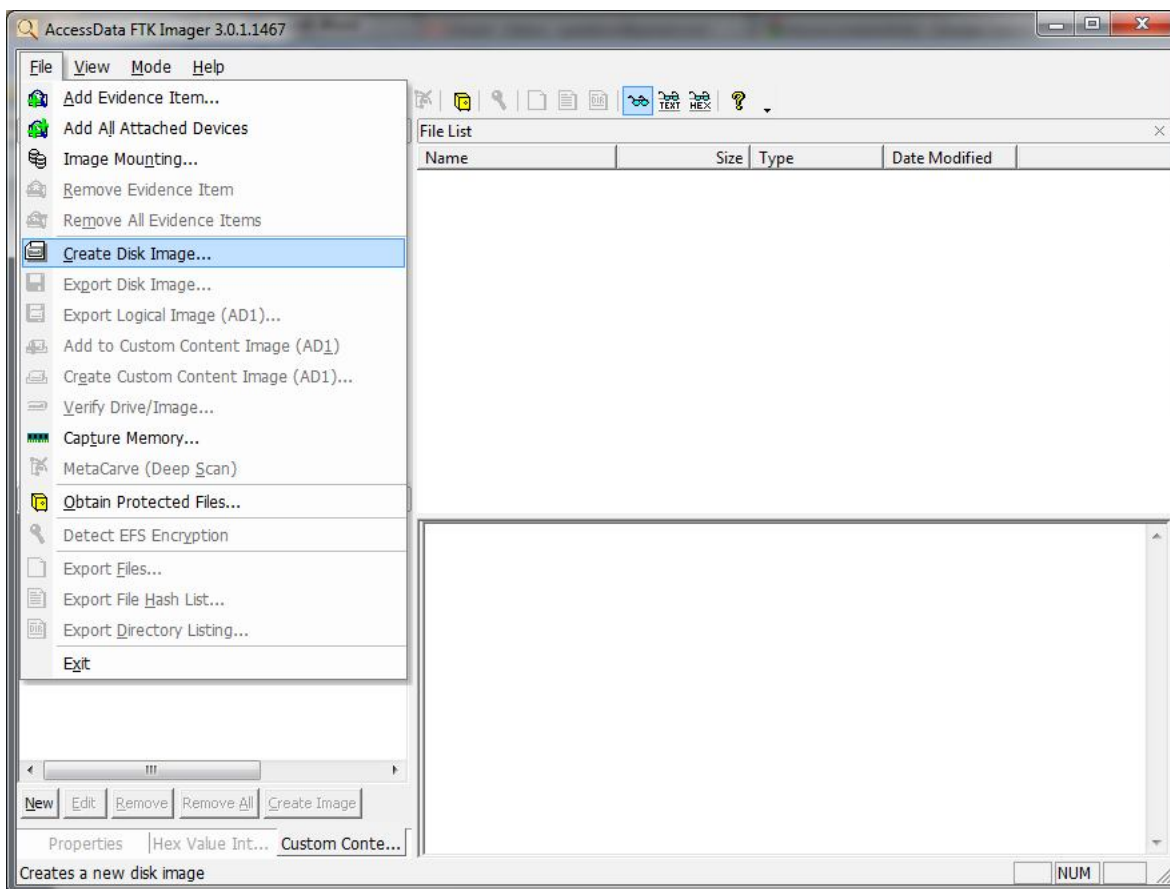
5 - Javno dostupni (besplatni) softverski alati za forenzičku istragu

5.1 - AccessData FTK Imager

AccessData FTK Imager je standardan forenzički alat koji pouzdano pravi forenzičke kopije svih media za skladištenje podataka. Osim pouzdanosti u radu velika prednost u ovoj oblasti je i činjenica da je besplatan.

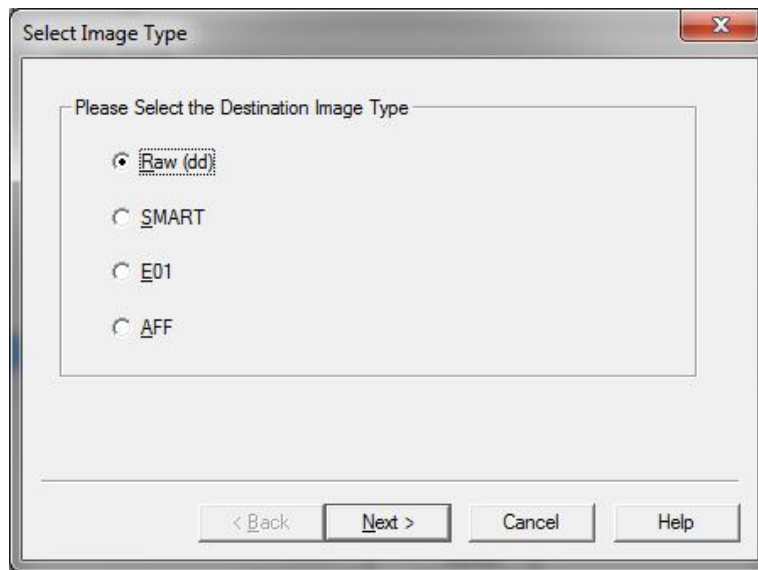
Program osim izrade sudski validnih kopija medija za skladištenje podataka ima i druge funkcije.

Na slici 37 se vidi izgled programa *AccessData FTK imager* sa opcijama glavnog menija koje su nam na raspolaganju.



Slika 37 – Program AccessData FTK imager

Program AccessData FTK imager pravi forenzičke kopije medija u više standardnih formata, što se vidi na slici 38. Ova osobina programa AccessData FTK imager nam daje mogućnost da kopije medija za skladištenje podataka možemo analizirati drugim alatima.



Slika 38 – Formati forenzičkih kopija koje pravi program AccessData FTK imager

AccessData FTK imager je prilično rasprostranjen, može se reći standardan, forenzički alat, prvenstveno zbog svoje pouzdanosti u radu.

5.2 - Forenzički softverski paket *OSForensics*

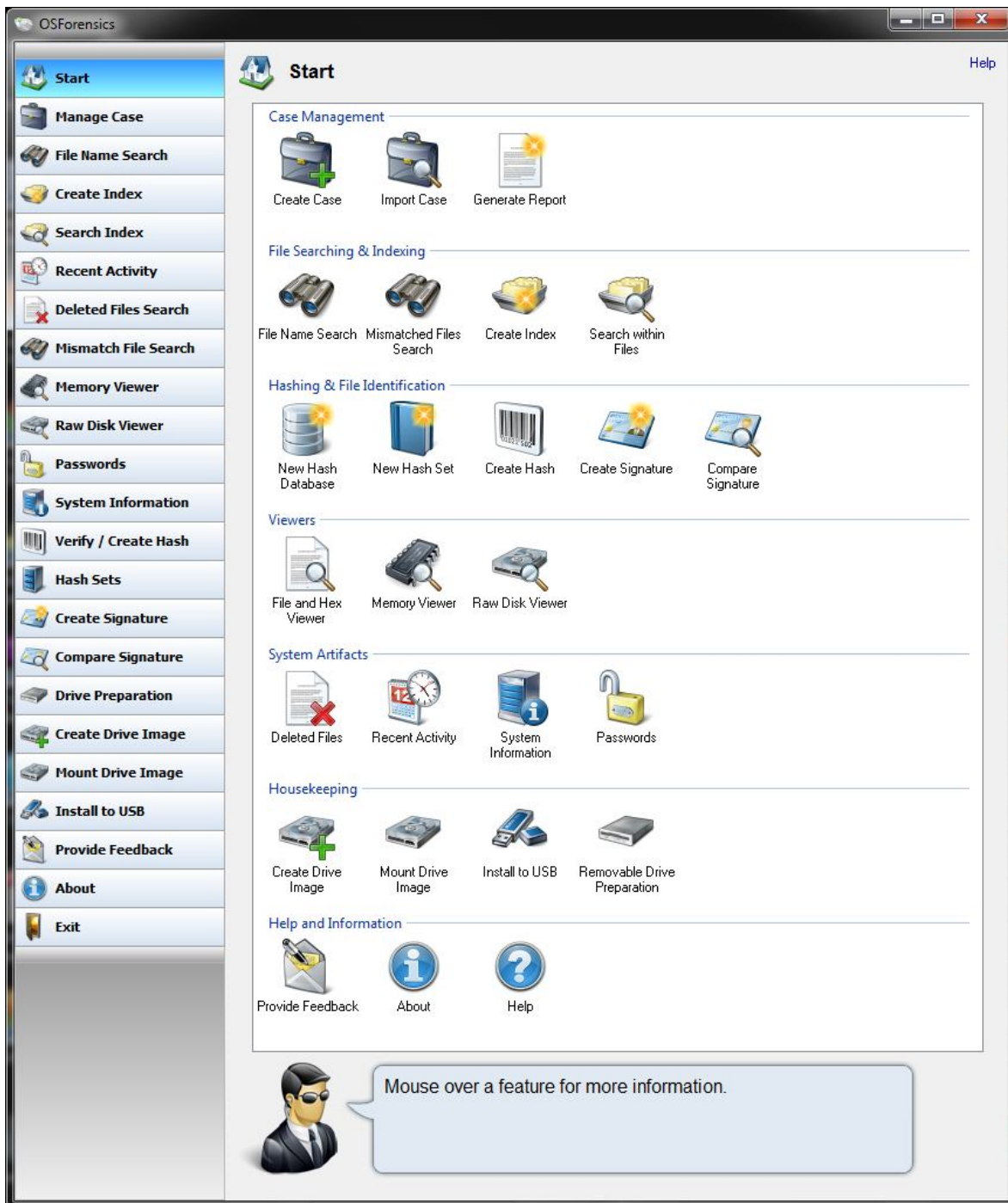
OSForensics je softverski paket namenjen digitalnim forenzičarima. Novijeg je datuma i, za sada, besplatan. Trenutno se putem interneta distribuira finalna beta verzija.

U budućnosti paket neće u potpunosti biti besplatan, iako proizvođač tvrdi da će uvek postojati neka vrsta besplatnog paketa.

Pri otvaranju programa uočavamo mnoštvo funkcija koje su ugrađene u paket. Izgled programa odmah po otvaranju se vidi na slici 39.

Po ponuđenim opcijama možemo pretpostaviti da ovaj paket predstavlja ozbiljan skup forenzičkih alata.

Uz pomoć ovog softveskog paketa ćemo sprovesti analizu memorijskog USB uređaja za skladištenje podataka (*USB flash disk*). Uz sprovođenje forenzičke analize pomenutog uređaja ćemo ujedno opisati neke od funkcija i testirati pouzdanost ovog forenzičkog paketa.



Slika 39 - Izgled programa OSForensics odmah po otvaranju

6 - Primer forenzičke analize USB fleš uređaja

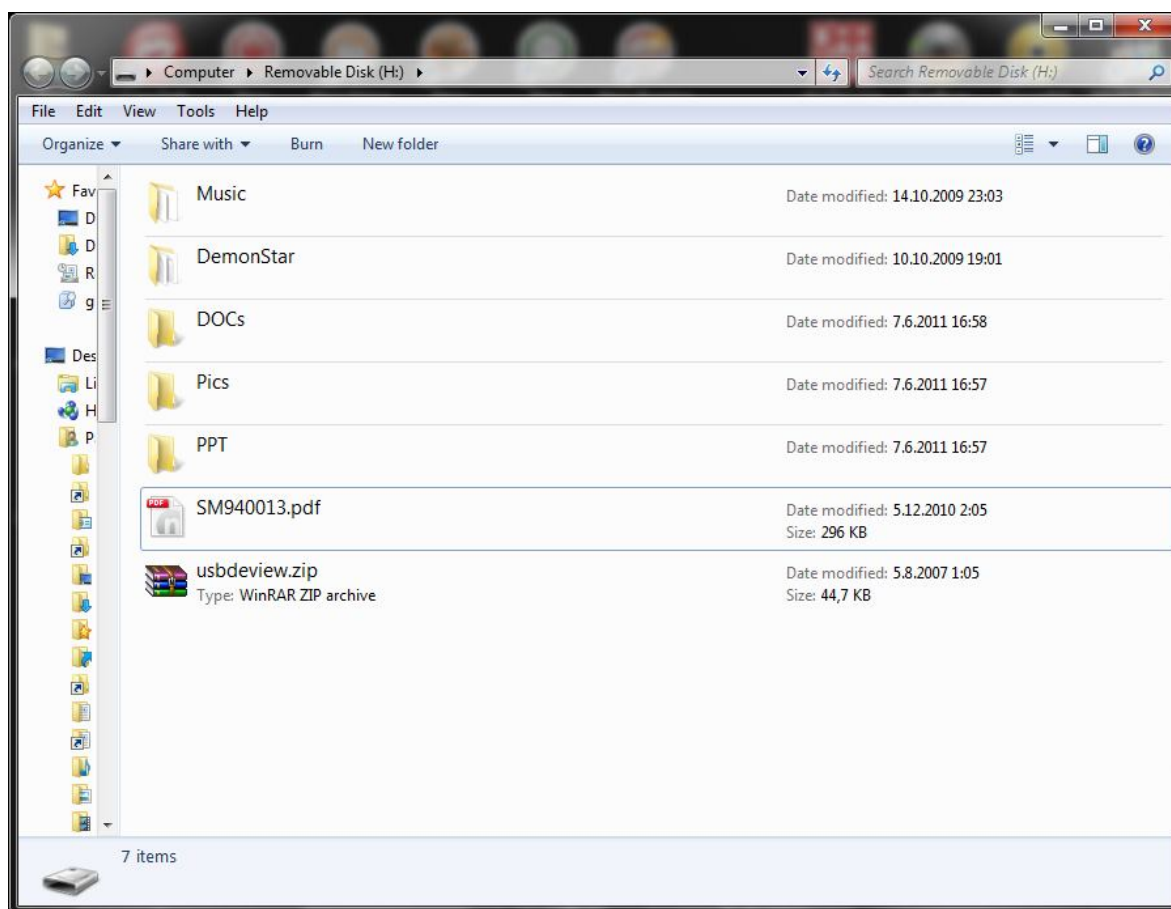
6.1 - Priprema USB fleš uređaja

U cilju spovođenja postupka forenzičke istrage USB fleš uređaja izvršena je priprema jednog USB fleš diska kapaciteta 512 Mb.

USB disk je prvo obrisao programom *Active KillDisk*. Potom je formatiran FAT fajl sistemom, opcija *Quick format*. Zatim je izvršena provera uz pomoć prethodno opisanih programa za oporavak obrisanih fajlova, ni jedan od opisanih programa nije uspeo da pronađe bilo šta što bi se moglo oporaviti.

Na prazan disk, u različite foldere je snimljeno nekoliko tipova fajlova koji se često mogu naći na personalnim računarima. Većina fajlova je sa čvrstog diska kopirana u osnovni (*root*) folder USB diska a zatim premeštena u druge foldere na istom disku.

Kopirani fajlovi i folderi prikazani su na slici 40.



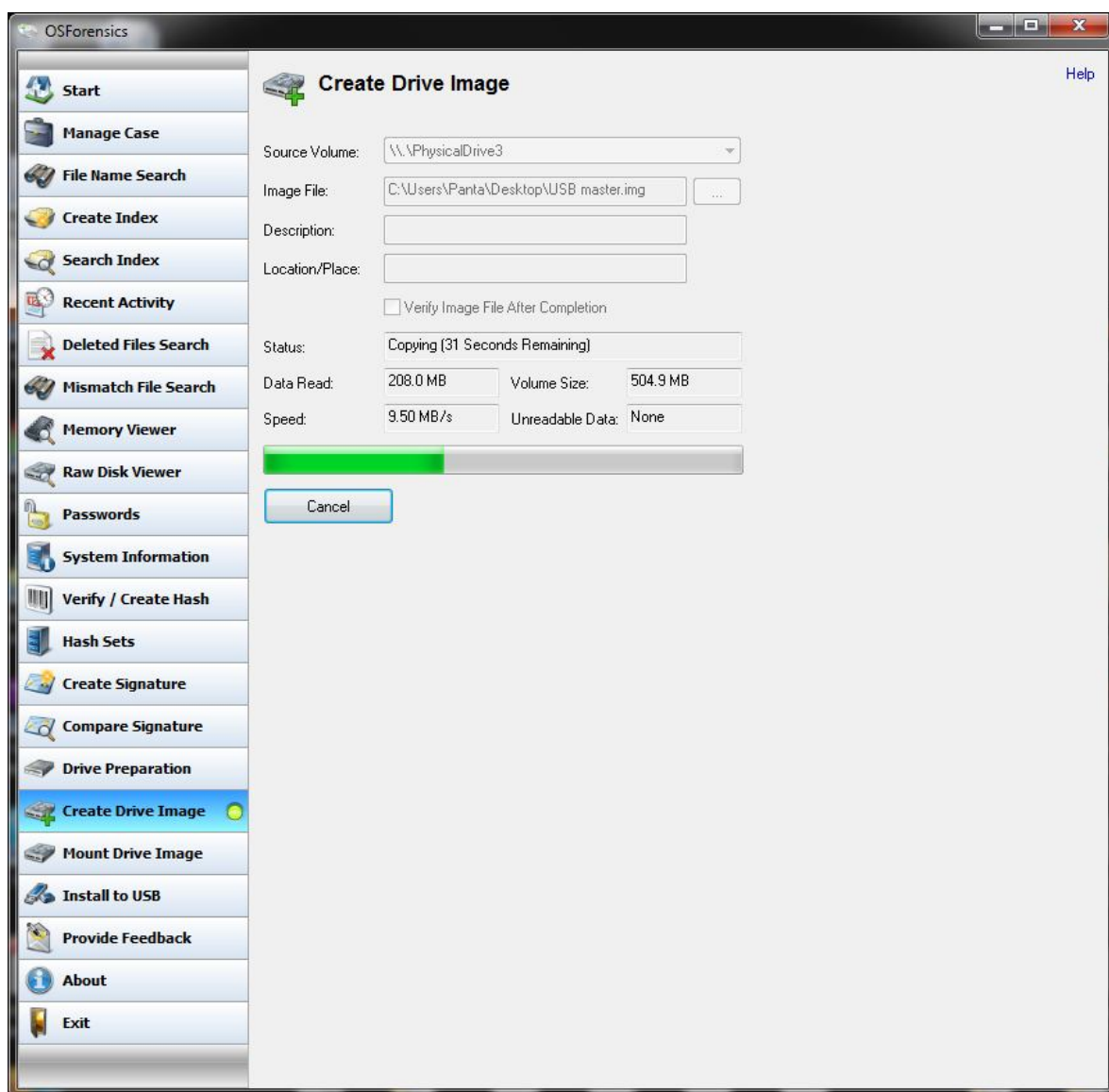
Slika 40 - Kopirani fajlovi i folderi na USB fleš disku

Posle kopiranja i premeštanja pojedini fajlovi su obrisani, najmanje po jedan iz svakog fodera.

6.2 - Izrada forenzičke kopije USB fleš uređaja

Pokrenut je programski paket OSForensics i napravljena je forenzička kopija USB fleš diska.

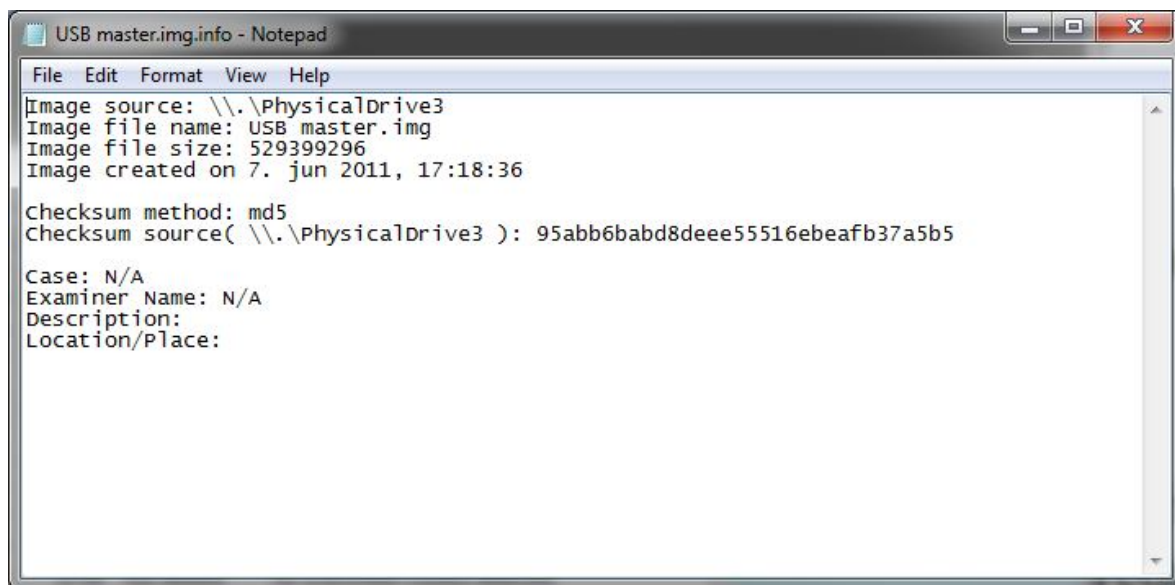
Na slici 41 se vidi program OSForensics u toku izrade kopije USB diska.



Slika 41 - Program OSForensics u toku izrade kopije USB diska

Po okončanju procesa izrade forenzičke kopije USB diska program *OSForensics* generiše fajl sa podacima o generisanoj kopiji diska. Između ostalog, u tom fajlu se nalazi i heš vrednost generisane kopije.

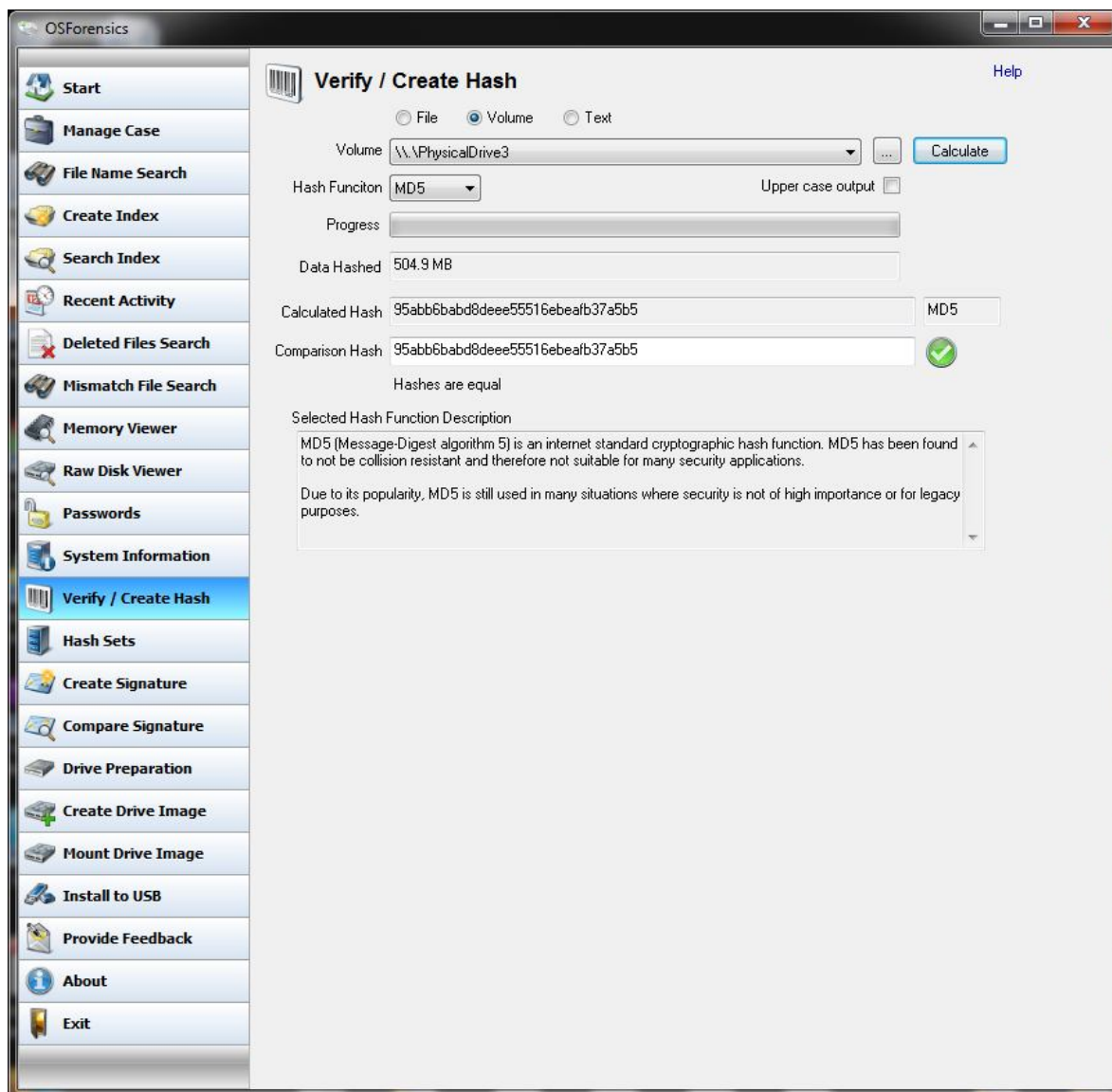
Na slici 42 je prikazan sadržaj fajla koji se generiše pri izradi forenzičke kopije diska.



Slika 42 - Sadržaj fajla koji se generiše pri izradi forenzičke kopije diska

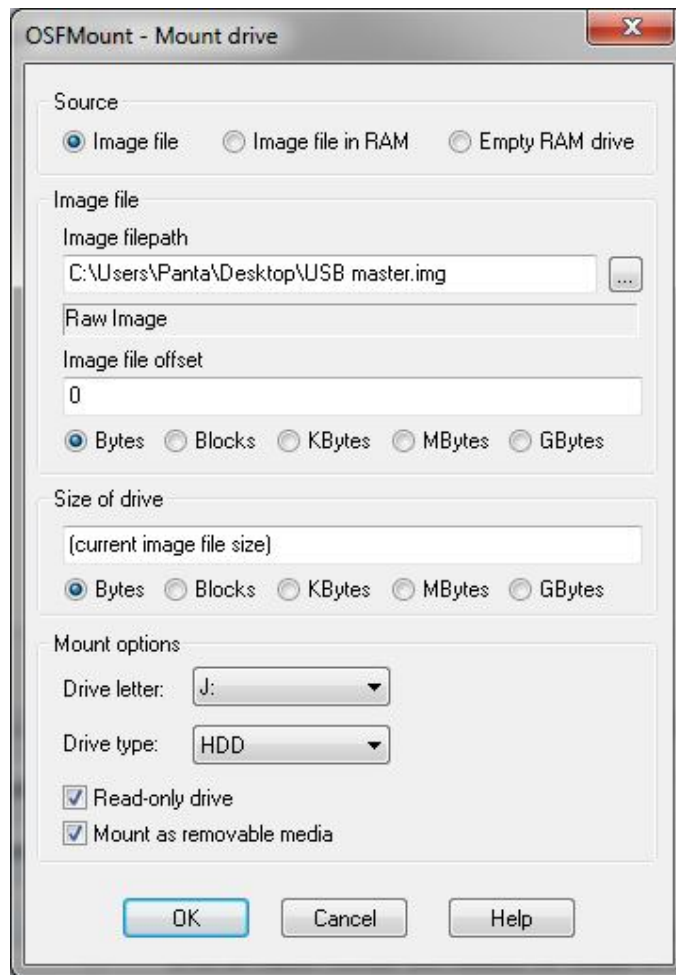
Kreirane *hash* vrednosti za USB disk i Forenzičku kopiju diska, su zatim upoređene.

Poređenje *hash* vrednosti se vidi na slici 43.



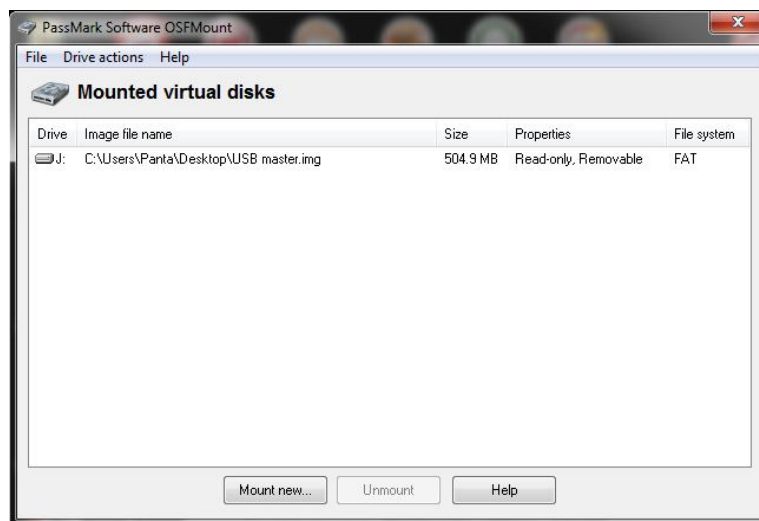
Slika 43 - Poređenje hash vrednosti USB diska i hash vrednosti njegove forenzičke kopije

Pošto je potvrđeno da su *hash* vrednosti identične pristupljeno je *mount*-ovanju kopije diska na sistem. Opcije koje su pri tome korišćene se vide na slici 44.



Slika 44 - Opcije za mount-ovanje kopije diska na sistem

Na slici 45 se vidi kopija diska kao virtualni disk na sistemu.



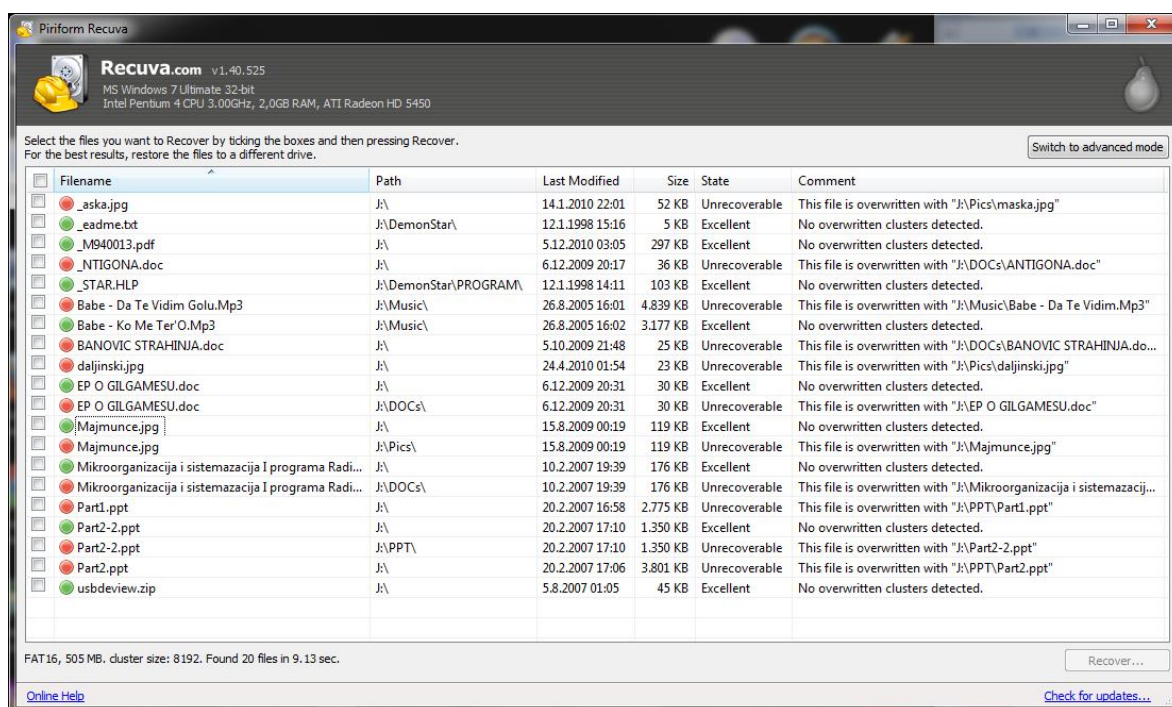
Slika 45 - Kopija USB diska postavljena kao virtualni disk na sistemu

6.3 - Oporavak obrisanih fajlova

Sledeći korak je oporavak obrisanih fajlova. Operacija oporavka je vršena na forenzičkoj kopiji USB diska koja je *mount*-ovana na sistem.

Alat za oporavak koji se nalazi u paketu *OSForensics* je dao jako loše rezultate pa je u tu svrhu korišćen program *Recuva*.

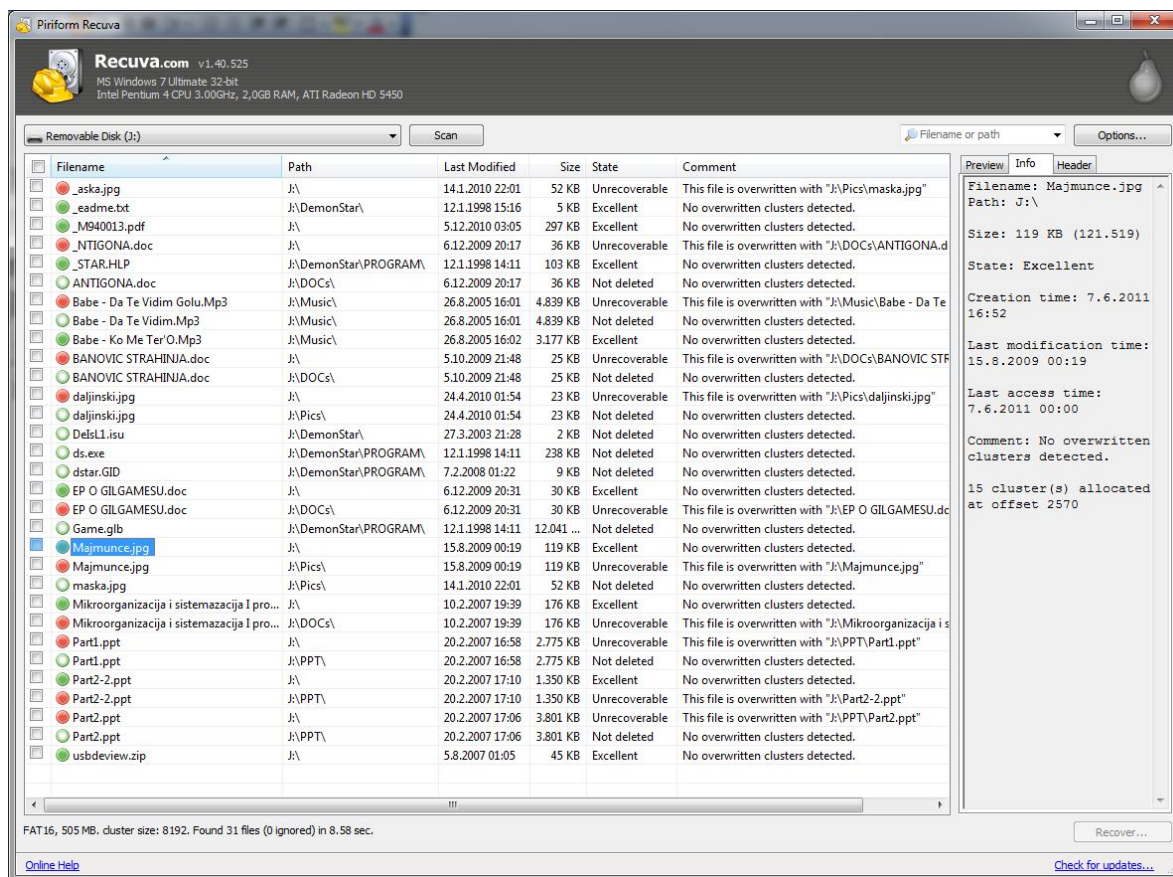
Rezultat pretrage USB diska programom *Recuva* se vidi na slici 46.



Slika 46 - Rezultat pretrage USB diska programom Recuva

Pošto je poznato kako je formiran sadržaj diska na kome je vršena pretraga, može se dati komentar na rad ovog programa. Sa prethodne slike (46) se vidi da se nazivi pojedinih fajlova pojavljuju dva puta, razlog tome je premeštanje fajlova sa početne lokacije iz *root* foldera u druge foldere. Jedan od fajlova je preimenovan, na slici 46 se vidi da je prepisan istim fajlom sa novim nazivom (novi naziv je kraći za jednu, poslednju, reč).

Sve navedeno se može bolje sagledati ako pretraživanje diska izvršimo u *advanced* modu kao što je prikazano na slici 47. U ovom modu program u listu uvrštava i fajlove koji nisu obrisani pa se lakše može doći do zaključka šta se desavalo sa fajlovima. Može se uočiti koji su fajlovi stvarno obrisani a koji su premešteni u druge foldere.



Slika 47 - Rezultati pretraživanja kopije USB diska programom Recuva u advanced modu

Po okončanju pretrage izvršen je oporavak fajlova. Program je oporavljene fajlove upisao na izabranu lokaciju na čvrstom disku računara.

Svi fajlovi za koje je program postavio status „Excellent“ oporavljeni su bez greške.

6.4 - Smernice za dalji rad na forenzičkoj istazi USB fleš diska

Dalji rad na istrazi bi se sastojao od obrade svakog pojedinačnog fajla kroz analizu vremena kreiranja (ako je fajl kopiran ili preuzet sa interneta onda ova vrednost predstavlja vreme kada je kopiran ili učitao sa interneta), vremena poslednje izmene sadržaja fajla i vremena poslednjeg pristupa fajlu. Od ovih vremena, do kojih se relativno lako dolazi, najrelevantnije u mnogim istragama može biti vreme poslednje izmene jer jedino ono nije podložno izmeni u slučaju kopiranja ili premeštanja fajla.

Zavisno od tipa fajla, postoje i mnogi drugi podaci koji se nalaze u samom fajlu.

U slučaju fajlova kreiranih programima iz Microsoft Office paketa možemo videti naziv naloga korisnika koji je kreirao fajl, koliko izmena je vršeno, koliko je trajao rad na samom fajlu i još mnogo toga.

Kada se radi o fotografijama u fajlu postoje podaci o vremenu snimanja, uslovima snimanja, modelu i proizvođaču uređaja kojim je izvršeno snimanje. U slučaju fotografija preuzetih sa interneta često nedostaju mnogi od ovih podataka.

Ukoliko se fajlovi nalaze na USB disku formatiranom NTFS fajl sistemom, što je još uvek redak slučaj, možemo se poslužiti i drugim tehnikama pronalaženja podataka i informacija o fajlovima. Na primer, višestruki tokovi podata (*NTFS Multiple Data Streams* ili *Alternate Data Streams*) često sadrže podatke o poreklu fajla i vremenu preuzimanja.

Metodologija forenzičke istrage USB memorijskih uređaja još uvek nije jasno definisana te se moramo osloniti na metodologije koje se koriste u istragama magnetnih medija.

Ne postoje alati koji su namenjeni sprovođenju istraga za ovu vrstu uređaja te od konkretnog slučaja zavisi kakvu ćemo strategiju osmisлити i primeniti.

Za istrage koje se obavljaju na nivou sadržaja memorijskih ćelija se koristi poseban hardver i softver. Ali čak ni u ovoj oblasti ne postoje standardizovane metode rada. U nekim slučajevima se ide i do toga da se memorijski čipovi vade iz USB uređaja i postavljaju u poseban uređaj za čitanje.

Ono što se uvek mora uraditi je sledeće:

1. Izrada kopije celog USB diska
2. Verifikacija kopije diska uz pomoć heš vrednosti
3. Oporavak obrisanih fajlova

Zavisno od rezultata postupka oporavka obrisanih fajlova i potreba istrage možemo se odlučiti za analizu sadržaja kopije USB diska na niskom nivou (bajt po bajt) u nekom alatu koji prikazuje i pretražuje disk nezavisno od fajl sistema i operativnog sistema.

Sve ostale akcije zavise od toga šta pronađemo u prethodnim analizama i pri tome se moramo osloniti na vlastito znanje i iskustvo u radu sa drugim vrstama medija za skladištenje podataka.

V – ZAKLJUČAK

Analizom fajl sistema se dolazi do većine dokaza u savremenim forenzičkim istragama. U ovom radu su prikazani elementi NTFS fajl sistema koji mogu biti od velikog značaja prilikom izvođenja dokaza u toku forenzičke analize.

U toku forenzičke analize, zavisno od metode koja se primenjuje, mogu se izvesti mnogobrojni dokazi.

Ciljanim pretraživanjem fajl sistema na osnovu zadatog naziva i ekstenzije fajla mogu se otkriti podaci kao što su datum i vreme kreiranja fajla i korisnik koji je vlasnik fajla.

NTFS fajl sistem nam nudi mogućnost oporavka obrisanih fajlova i podataka koji oni sadrže.

Pretraživanje slobodnog prostora na disku nam u mnogim slučajevima može dati vredne dokaze jer se u njemu mogu naći skriveni podaci.

Pronalaženjem i isčitavanjem sadržaja višestrukih tokova podataka može se otkriti mnoštvo podataka od toga da li je i odakle sa interneta preuzet određeni fajl pa do podataka o tome koji korisnik je kojim programom i kada kreirao ili menjao fajl.

Takodje, u velikom broju slučajeva, analizom *slack* prostora koji predstavlja razliku između stvarnog prostora koji fajl zauzima na disku i prostora koji zauzima u samom fajl sistemu (nepopunjen poslednji klaster koji pripada fajlu) mogu se pronaći zlonamerno skriveni podaci.

Iz navedenog se može zaključiti da se pronalaženjem i čitanjem podataka koji se podrazumevano nalaze u NTFS fajl sistemu može prikupiti i izvesti mnoštvo forenzičkih dokaza.

Windows Registry je baza podataka koja je implementirana u Microsoft Windows operativni sistem i sadrži podešavanja i konfiguraciju sistemskog hardvera, aplikacija i profila korisnika. *Windows Registry* sadrži nekoliko potencijalno značajnih elemenata koji bi mogli biti od vrednosti forenzičkim istražiteljima.

Identifikacija i dobijanje dokaza sa medija za čuvanje (skladištenje) podataka čija veličina se stalno povećava je proces koji troši vreme. Mnoštvo elemenata koji mogu biti od velikog značaja forenzičkim istražiteljima sadržani su unutar *Windows Registry* baze, i to može pomoći da se smanji vreme trajanja istrage. Jednom kada je istražitelj pronašao relevantnu informaciju, ona može pomoći kao smernica za dalji rad kako bi se na taj način obezbedile informacije koje nisu bile dostupne iz drugih izvora. Kao posledica toga, proces istrage bi mogao biti jednostavniji i trajao bi znatno kraće.

Iako digitalna forenzika postoji kao nauka već desetak godina, naučnih istraživanja u oblasti USB fleš diskova ima vrlo malo. Razvoj alata za akviziciju digitalnih dokaza sa USB fleš diskova nedovoljno prati rastuće potrebe u pogledu prezentacije i neporecivosti prikupljenih dokaza pred sudom. Postojeći forenzički alati imaju velikih teškoća u prikupljanju esencijanih podataka koji bi služili kao digitalni dokaz u toku sudskog procesa.

Potrebno je sprovesti naučna istraživanja u oblasti mehanizama čitanja fleš memorija i ugraditi ih u sledeću generaciju alata za forenzičku akviziciju podataka.

Neophodno je bolje istražiti specifičan način brisanja podataka u blokovima koja je ujedno povezana sa strategijom održanja veka trajanja ovih uređaja i ta saznanja primeniti na poboljšanje procesa oporavka i analize podataka. Jasno je da bi nova saznanja u oblasti stvarnog brisanja podataka u blokovima doprinela boljem oporavku podataka nego metoda pristupa oporavku obrisanih fajlova na nivou fajl sistema.

Ovakva naučna istraživanja bi doprinela povećanju efikasnosti rada u oblasti forenzičkih ispitivanja USB fleš uređaja od strane prosečno osposobljenih IT stručnjaka.

VI – LITERATURA

- [1] Honeycutt, Jerry, 2005, Microsoft Windows Registry Guide. 2nd., Redmond, WA: Microsoft Press
- [2] Doc. Dr Gojko Grubor, mr Igor Franc, 2010, Forenzička analiza Windows 7 registry
- [3] Wong, Lih Wern, Forensic Analysis of the Windows Registry, Forensic Focus, 1 Feb 2007.
- [4] Harlan Karvey, 2007, Windows forensic analysis, Syngress.
- [5] Chad Steel, 2006, Windows Forensics: The Field Guide for Corporate Computer Investigations, John Wiley & Sons ©.
- [6] Milan Milosavljević, Gojko Grubor, 2009, Istraga kompjuterskog kriminala - metodološko tehnološke osnove, Singidunum.
- [7] Davies, Peter, Forensic Analysis of the Windows Registry, Peter Davies, 2006. 3 Feb 2007.
- [8] Khawla Abdulla Alghafli, Andrew Jones, Thomas Anthony Martin, Forensic Analysis of the Windows 7 Registry, Khalifa University of Science, Technology and Research, 2010
- [9] Microsoft press, Description of the Microsoft Windows Registry, Help and Support, 27 Jan 2007. Microsoft Corp. 8 Apr 2007.
- [10] Microsoft tech net, How NTFS works
<http://technet.microsoft.com/en-us/library/cc781134%28WS.10%29.aspx>
- [11] ntfs.com, NTFS file types <http://www.ntfs.com/ntfs-files-types.htm>
- [12] Data Hiding in the NTFS File System, Ewa Huebner, University of Western Sydney Australia, 2007
- [13] A forensics overview and analysis of USB flash memory devices, Krishnun Sansurooah Security Research Centre, School of Computer and Security Science, Edith Cowan University