TEHNIKA I INFORMATIKA U OBRAZOVANJU
4. Internacionalna Konferencija, Tehnički fakultet Čačak, 1–3. jun 2012.
TECHNICS AND INFORMATICS IN EDUCATION
4th International Conference, Technical Faculty Čačak, 1–3rd June 2012.

UDK: 004.42 Stručni rad

KORIŠĆENJE PROGRAMA R-STUDIO ZA REPARACIJU PODATAKA

Todor Anđić [1], Milenko Rončević [2], Branko Marković [3]

***Rezime**: Reparacija podataka je proces „spašavanja“ podataka sa oštećenih, pokvarenih, uništenih ili medija bez pristupa. Obično se podaci spašavaju sa medija poput internih i eksternih hard diskova, SSD diskova, USB fleš diskova, traka, CD, DVD, RAID diskova i sličnih medija. Reparacija je uslovljena fizičkim oštećenjem medija ili logičim oštećenjem fajl sistema koji sprečava upotrebu medija. Termin „Reparacija podataka“ se takođe koristi u kontekstu forenzičkih aplikacija i špijunaže, gde se restauriraju podaci koji su kriptirani ili sakriveni, umesto oštećenih. Softver R-Studio je jedan od alata kojim se mogu spašavati podaci.*

***Ključne reči:** Hard disk, USB fleš disk, restauracija, podaci, R-Studio.*

DATA RECOVERY WITH R-STUDIO SOFTWARE

***Summary**: Data recovery is the process of salvaging data from damaged, failed, corrupted, or inaccessible storage media when it cannot be accessed normally. Often the data are being salvaged from storage media such as internal or external hard disk drives, solid-state drives (SSD), USB flash drive, storage tapes, CDs, DVDs, RAID, and other electronics. Recovery may be required due to physical damage of the storage device or logical damage of the file system that prevents it from being mounted by the host operating system. The term "data recovery" is also used in the context of forensic applications or espionage, where data which has been encrypted or hidden, rather than damaged, is recovered. The software package R-Studio can be used to recover data.*

***Key words:** Hard disκ drive, USB flesh disκ, recovery, data, R-Studio.*

1. UVOD

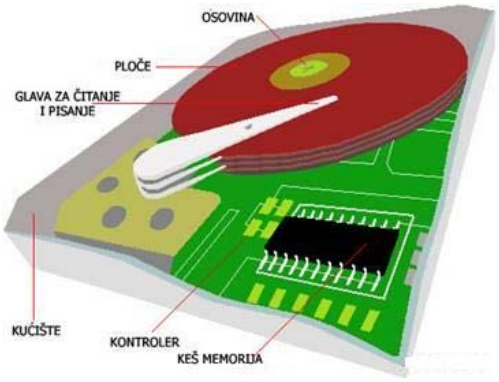
Kao spoljašnje memorije u kojima se čuvaju podaci i posle gašenja računara najčešće se koriste hrad diskovi (HDD), USB fleš diskovi (memorije), CD, DVD i drugi mediji.

[1] Todor Anđić, struk. ing. men, JU IKC, Gacko, Solunskih dobrovoljaca 2, E-mail: todorandjic@yahoo.com
[2] Milenko Rončević, ing. prim. rač, AD RiTe, Gračanica bb, Gacko, E-mail: milenko.roncevic@ritegacko-rs.ba
[3] Mr Branko Marković, VŠTSS, Svetog Save 65, Čačak, E-mail: branko333@open.telekom.rs

Naravno među njima dominantnu ulogu imaju hard diskovi koji sadrže operativne sisteme i aplikativne fajlove. Usled različitih uticaja često se dešava da fajlovi budu oštećeni, pa je funkcionisanje i pristup onemogućen. Zbog toga se koriste različiti metodi da se podaci rekonstruišu i sačuvaju. Jedan od takvih metoda je i primena softverskog paketa R-Studio[1] koji omogućava u određenim situacijama povraćaj izgubljenog saržaja.

2. SNIMANJE SADRŽAJA I NJEGOVA OBNOVA POSLE OŠTEĆENJA

Hard disk se sastoji od nekoliko magnetnih ploča između kojih se nalazi glava za čitanje/pisanje (Slika 1). Podaci se upisuju u obliku koncentričnih krugova koji se nazivaju staze. Deo staze naziva se sektor, a više sektora zajedno čine klaster (cluster).



Slika 1: Unutrašnji izgled hard diska

Kada se kupi novi disk, pre upotrebe treba ga formatirati. Svrha toga je da se magnetni prostor podeli na sektore. Sektori se grupišu u klastere, a klaster je najmanja jedinica podataka kojom upravlja operativni sistem. Broj sektora u klasteru uvek je eksponent broja 2. Prvi sektor na disku je ključan za funkcionisanje samog uređaja. To je **Master Boot Record** (**MBR**). Kreira se automatski pri formiranju prve particije diska. MBR sadrži Tabelu particije (**Partition Table**) i malu količinu izvršnog koda. Funkcija ovog koda je pregled Tabele particije i pronalaženje sistemske particije i njene početne lokacije na disku. Postoji veliki broj virusa koji mogu oštetiti MBR i onemogućiti podizanje operativnog sistema. Ovakve viruse je teško detektovati iz operativnog sistema jer se pokreću pre samog sistema. Međutim postoje i alati kojima se može obnoviti sadržaj MBR-a (npr. **Microsoft Windows Resource Kits**).

Particije kod hard diska predstavljaju logičke celine koje se ponašaju kao odvojeni hard diskovi iako su na istom fizičkom disku. Obeležavaju se velikim slovima alfabeta (C:, D:, E: itd). Kod snimanja fajla na disk, podaci se zapisuju u klastere. Ako je veličina fajla manja od veličine klastera, ceo fajl će biti sačuvan unutar jednog klastera. Unutar jednog klastera ne mogu biti dva fajla, čak i kada je njihova ukupna veličina manja od veličine klastera. Ako je fajl veći od klastera, njegov sadržaj će se protezati kroz nekoliko klastera. Poželjno je da klasteri (za isti fajl) budu kontinuirani (nalaze se jedan iza drugog). U slučaju da nema dovoljno kontinuiranih klastera, fragmenti fajla se zapisuju u bilo koje slobodne klastere. Fragmentiranje podataka na ovaj način narušava performanse čitanja i zapisivanja podataka.

Podaci na spoljašnjim memorijama (hard disk, USB fleš disk i sl.) mogu biti oštećeni. Najbanalniji uzrok može biti nepažnja korisnika koji slučajno obriše fajl koji nije smeo obrisati. Štetu mogu izazvati virusi koji uništavaju podatke zapisane na MBR ili neki drugi deo diska. Uzrok gubitka podataka može biti i hardverski kvar, kao npr. nepovratno uništeni sektori na disku. U slučaju bilo kojeg od navedenih problema, sami podaci sačuvani na hard disk najčešće neće biti uništeni i biće ih moguće obnoviti.

Da bi se operativni sistem računara mogao podići moraju biti zadovoljeni sledeći uslovi:

- MBR mora postojati i mora biti ispravan,
- Tabela particije mora postojati i sadržati bar jednu aktivnu particiju

Izvršni kod iz MBR-a bira aktivnu (primarnu) particiju i sa te particije se učitavaju određeni fajlovi (COMMAND.COM, NTLDR ili neki drugi, u zavisnosti od operativnog sistema). U slučaju da ovih fajlova nema ili da nisu ispravni, operativni sistem se ne može pokrenuti. Tada se mora pokrenuti sistem sa nekog drugog uređaja (drugi hard disk, USB ili CD i sl.).

Obnova na osnovu različitih uzroka kvara ima i različite pristupe. Osnovni su sledeći:

1) MBR je oštećen

Ako je oštećen samo MBR, a Tabela particija je čitava, relativno je lako obnoviti izgubljene podatke. Sistem se može pokrenuti s nekog drugog uređaja. Nakon što se pokrene sistem, zahvaljujući sačuvanim Tabelama particija, sve particije su vidljive. Može im se pristupati na uobičajen način i kopirati sve podatke na neki drugi medij. Može se i obnoviti oštećeni MBR. Ako se koristi Microsoftov OS, najjednostavniji način obnove je korištenje Microsoft alata FDISK (komadom: **A:\>FDISK.EXE/MBR**).

Ova naredba će obnoviti sadržaj MBR-a na standardna Microsoft podešavanja. Obnova fizičkog diska na ovaj način nekad nije moguća, u slučaju da je sektor u kojem se nalazi MBR trajno oštećen. Tada je jedina opcija upotreba nekog od specijalizovanih alata za obnovu sadržaja diska i kopiranje sadržaja na neki drugi medij ili uređaj.

2) **Particija je obrisana ili je Tabela particija oštećena**

Podaci o particijama zapisani su u Tabeli particija. Tamo se može videti na kojoj fizičkoj lokaciji na disku počinje i završava se neka particija. Kod brisanja čitavih particija, sve što se zapravo obriše je zapis u Tabeli particija. Svi podaci koji su bili zapisani na obrisanoj particiji i dalje fizički ostaju zapisani na disku. Problem slučajnog brisanja particija ili oštećenih Tabela particija vrlo je sličan problemu slučajnog formatiranja particije. Tada se ima originalni zapis u Tabeli particija, ali su svi fajlovi obrisani. Obrisani fajlovi i dalje su fizički zapisani na disku i moguće ih je obnoviti specijalnim alatima.

Danas postoji veliki broj alata koji služe za obnovu sadržaja čitavih particija. Neki od njih su:

- Active@ Partition Recovery,
- Active@ UNERASER,
- R-Studio

3) Obnova pojedinih fajlova

Obnova izgubljenih fajlova može se kratko opisati kao skeniranje diska ili direktorijuma tražeći obrisane sadržaje, utvrđivanje lanca klastera u kojima je zapisan fajl koji se želi da obnovi i kopiranje sadržaja tih klastera u novi fajl (preporučuje se na neki drugi diski ili uređaj). Različiti fajl sistemi definišu različite logičke strukture koje se koriste za čuvanje podataka na disku. Ipak, gotovo svi fajl sistemi imaju sledeće delove:

- Listu ili katalog svih sačuvanih fajlova,
- Za svaki zapis u toj listi postoji lista klastera u kojima je fajl fizički zapisan.

Za razumevanje mehanizama obnove fajlova mora se objasniti sam postupak brisanja fajla. Kada se obriše fajl on u stvari nije fizički obrisan sa diska. Brisanjem, fajl je samo označen za brisanje u katalogu sačuvanih fajlova. Njegov zapis u katalogu, kao i sami podaci sačuvani u klasterima na disku i dalje ostaju fizički zapisani. Njihov sadržaj će se izgubiti tek kada na njihovo mesto dođu novi podaci. Dakle - sa diska se nikad ništa ne briše, već se samo označi kao obrisano i eventualno "pregazi" novim podacima.

3. SKENIRANJE DISKA I TRAŽENJE OBRISANIH ZAPISA

Skeniranje diska je proces čitanja i enumeracije svih zapisa u katalogu sačuvanih fajlova (Root Folders na FAT 12, FAT 16 i FAT 32 fajl sistemima ili Master File Table na NTFS i NTFS5 fajl sistemima). Cilj je pronaći obrisane zapise. Uprkos različitim strukturama načina zapisa fajla ili direktorijuma na različitim fajl sistemima, svi oni sadrže uglavnom iste atribute: ime, veličina, datum kreiranja, datum modifikacije, aktivno ili obrisano.

Obrisani zapisi se takođe označavaju na različite načine, u zavisnosti od fajl sistema. Tako npr. na FAT fajl sistemu obrisan zapis označava se sa 0xE5 na prvom bajtu. To je razlog zbog kog se u MS-DOS-u koristeći program „undelete.exe“ mora navesti prvo slovo obrisanog fajla. Na NTFS fajl sistemu zapisi imaju poseban atribut koji se nalazi u zaglavlju fajla i koji govori da li je fajl obrisan ili ne. Da bi se ustanovilo koji klasteri čine lanac klastera za fajl koji se želi obnoviti moraju se skenirati redom svi klasteri (ili samo slobodni ako se radi o FAT fajl sistemu). Za svaki pročitani klaster odmah se utvrđuje da li pripada traženom fajlu (ili kom fajlu pripada – u slučaju da se žele obnoviti svi obrisani fajlovi). Skeniranje traje sve dok veličina pronađenih klastera ne dostigne veličinu traženog fajla. Ako je skeniran ceo disk, a nije dostignuta puna veličina traženog fajla, to znači da se traženi fajl ne može obnoviti bez oštećenja. Ovo se događa u slučaju da neki drugi fajl "pregazi" klastere obrisanog fajla.

Fizička lokacija klastera kao i način utvrđivanja kom fajlu pripadaju zavisi od fajl sistema. Npr. kod NTFS fajl sistema svaki fajl ima _DATA_ atribut. On sadrži zapise za svaki deo (fragment) određenog fajla. Svaki od tih zapisa sadrži adresu početnog klastera i ukupan broj klastera tog fragmenta. Nakon što se pronađu svi klasteri koji pripadaju traženom, obrisanom zapisu, sve što se treba uraditi je kopirati fajl na neku drugu lokaciju.

Kao što je već navedeno u dosadašnjem tekstu, obrisani sadržaji se nikada zapravo ne obrišu. Klasteri u kojima se nalaze, označe se kao obrisani, dok njihov sadržaj ostaje nepromenjen. Obrisani zapisi ostaju na disku sve dok se na njihovo mesto ne sačuvaju novi zapisi. To znači da nije moguće obnoviti baš svaki fajl koji je bio sačuvan na disku. S toga, nameće se pitanje - kada i koje fajlove je moguće obnoviti? Nije moguće sa sigurnosti definisati kada će biti moguće obnoviti neki fajl, a kada ne. Mogućnost obnove zapisa zavisi od velikog broja parametara. Na neke od tih parametara uopšte se ne može uticati, tako da se može samo govoriti o verovatnoći obnove pojedinog zapisa.

Ovo su glavni parametri od kojih zavisi mogućnost obnove zapisa:

- koliko je vremena prošlo od gubitka zapisa,
- koliko je novih podataka zapisano na disk u međuvremenu,
- veličina izgubljenog zapisa,
- fizička pozicija fajla na disku i
- fajl sistem.

Pravovremenom i ispravnom reakcijom može se u velikoj meri povećati mogućnost obnove izgubljenog zapisa. U trenutku kada se ustanovi gubitak važnog fajla, trebalo bi se pridržavati sledećih saveta:

- **Ništa ne zapisivati na disk na kome su izgubljeni podaci**
- **Ne snimati obnovljeni zapis na isti uređaj s kojeg se obnavlja zapis**

Snimanje obnovljenog podatka na isti uređaj može narušiti proces obnove, ako se podaci obnovljenog zapisa snime preko zapisa koji se obnavlja dok se proces obnove još nije završio. Puno je sigurnije obnovljeni zapis čuvati na nekom drugom uređaju ili mediju (drugi hard disk, CD, DVD, USB). Obnova izgubljenih sadržaja (Data Recovery) hard diskova može biti jako korisna. U slučaju raznih grešaka i kvarova hard diskova ili neželjenog brisanja važnih podataka, raznim tehnikama obnove podataka može se uštediti puno vremena i truda koje bi trebali uložiti da bi se ti podaci rekonstruisali na druge načine. Šteta koja nekad nastane zbog gubitka podataka zna biti neprocenjiva. Sve to ukazuje samo na pozitivne strane obnove podataka. Treba sagledati i sigurnosne aspekte obnove podataka, koji na čitavu temu bacaju potpuno drugačije svetlo. Pošto fajlovi nisu trajno uništeni na diskovima postoji opasnost curenja i zloupotrebe tajnih, poslovnih ili privatnih podataka. Zbog toga se prilikom odstranjivanja starih kompjutera (a time i njhovih diskova) pristupa procesu potpunog uništenja podataka. Uništavanje podataka (**disк sanitization)** je potpuna suprotnost obnovi podataka (**data recovery**). To je postupak kojim se nepovratno uništavaju podaci zapisani na tvrdom disku. Podaci uništeni na ovaj način neće se moći obnoviti alatima i tehnikama navedenim u ovom tekstu.

Postoji veliki broj softverskih i hardverskih rešenja za uništavanje podataka. Na slici 2 dati su primerci uređaja predviđenih za ovu namenu hardverskog tipa[2]. Zahtevniji korisnici upravo pribegavaju ovim rešenjima.

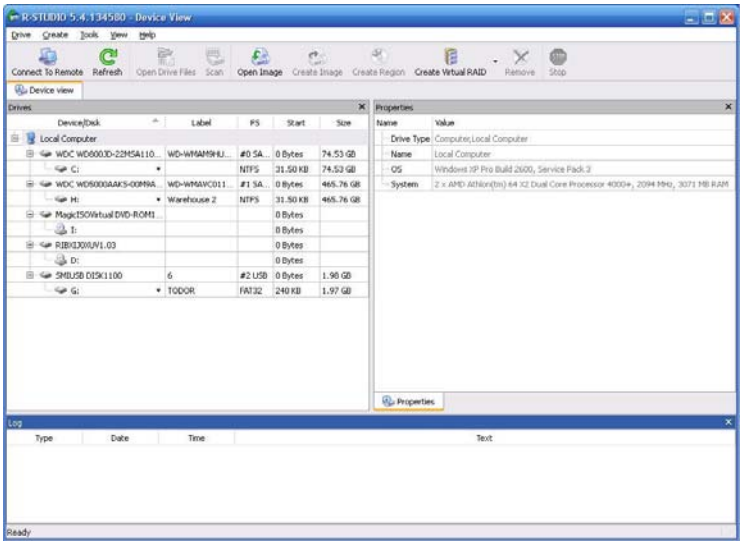
WipeMASSter

V660 HDD Evo Manual Degausser

Slika 2: Uređaji za uništavanje podataka

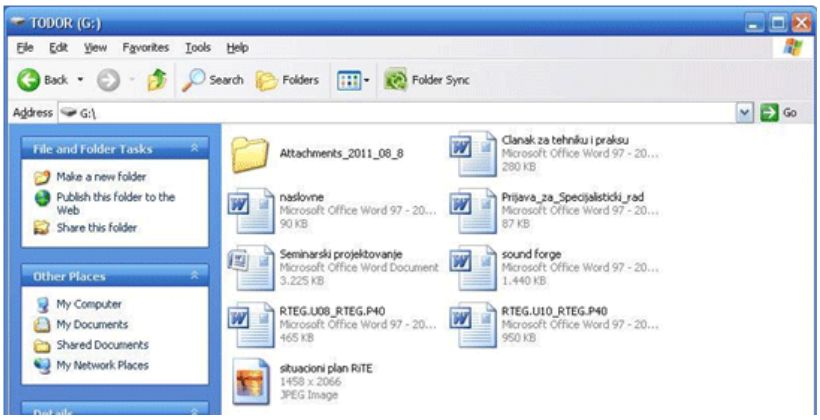
4. SPASAVANJA PODATAKA KORIŠĆENJEM R-STUDIO PROGRAMA

Primer korišćenja programa R-Studio 5.4 softverske firme R-Tools Technology Inc. dat je u nastavku. Primenjen je na spasavanje fajlova koji se nalaze na formatiranom USB fleš disku, na kojem su već upisivani novi fajlovi posle formatiranja. Isti princip primenjiv je i na hard diskove. Na slici 3 dat je interfejs ovog programa.



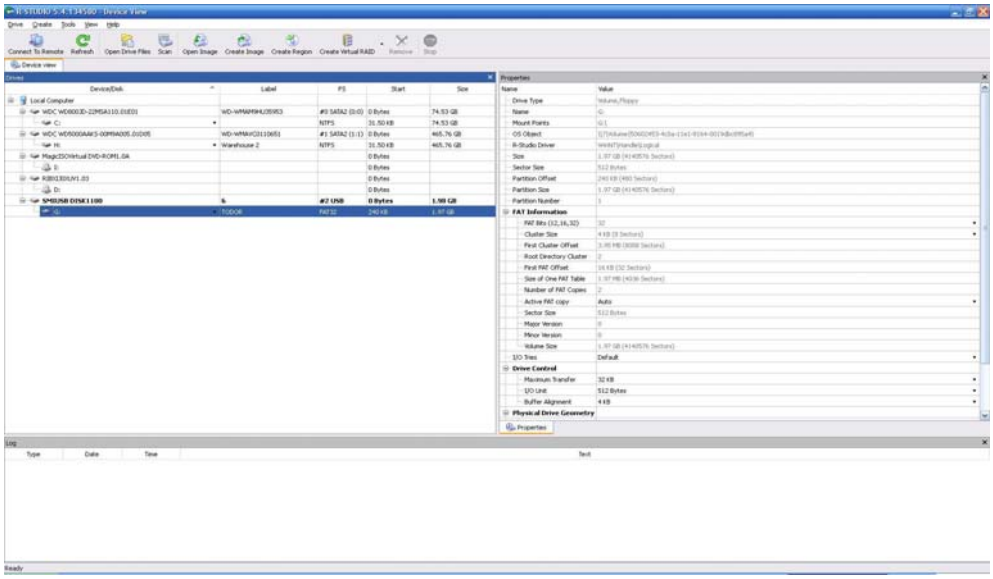
Slika 3: Interfejs programa R-Studio

Prikazana je lista diskova koji su priključeni na računar. U ovom primeru USB fleš disk je disk G: sa koga se spasavaju podaci. Slika 4 prikazuje fajlove koji su nasnimljeni na disk posle formatiranja.

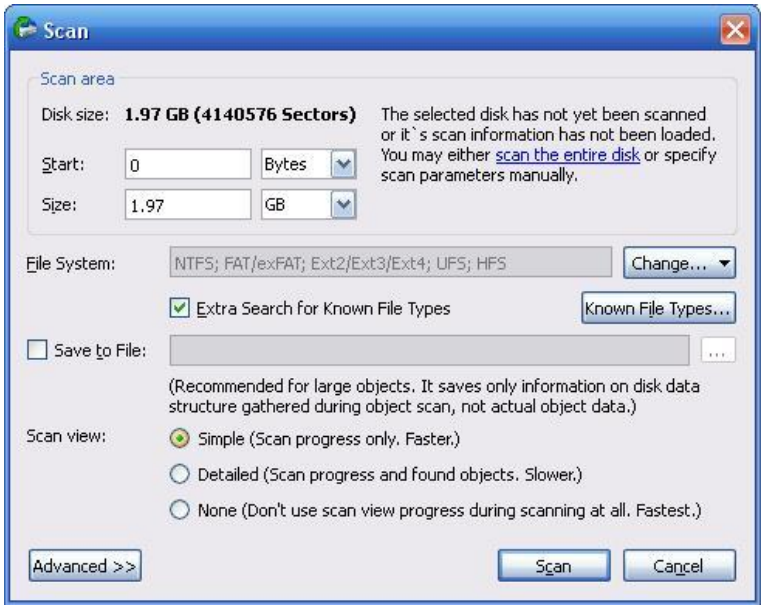


Slika 4: Fajlovi na disku G:

U programu se bira disk G: pa opcija „Scan“, da bi izvršilo skeniranje diska za fajlovima.

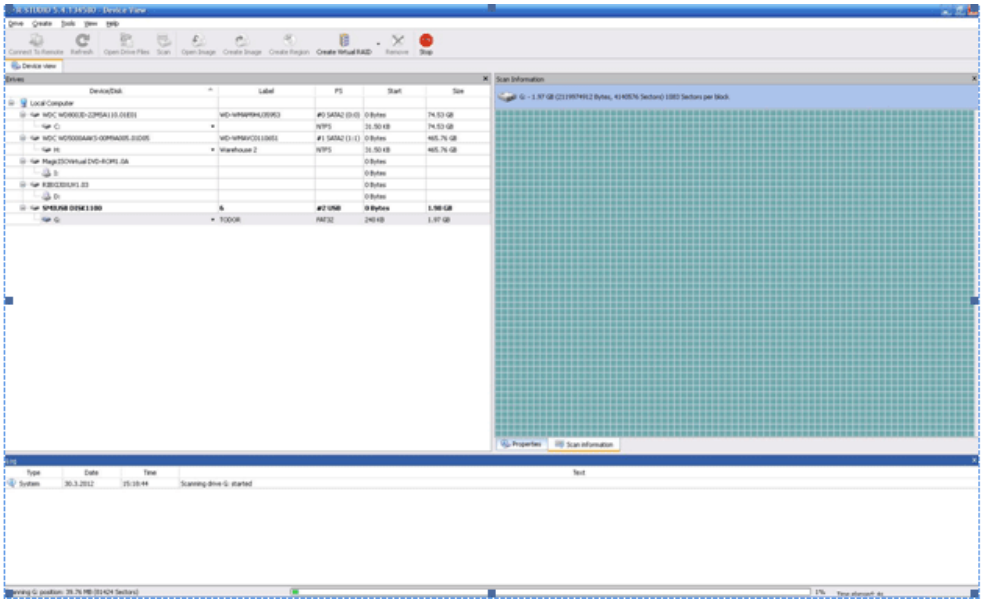


Slika 5: Dijaloški prozor za izbor diska



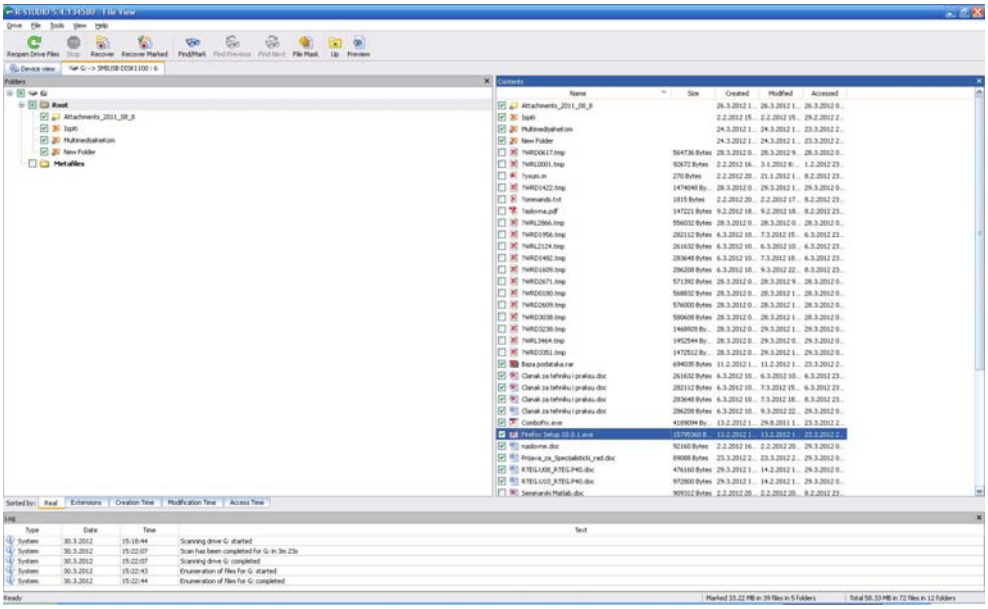
Slika 6: Dijaloški prozor sa opcijama skeniranja

Pojavljuje se dijaloški prozor „Scan“ (Slika 6) sa više opcija (složenost skeniranja, sektori diska koji će se skenirati, fajl sistem kao i tip fajlova). Ovde se koristi standardno podešavanje, skeniranje celog diska, za sve poznate tipove fajlova, metodom „Simple“. Samo skeniranje može da potraje od par minuta pa do više sati, u zavisnosti od veličine diska koji se skenira (Slika 7).



Slika 7: Skeniranje diska u toku

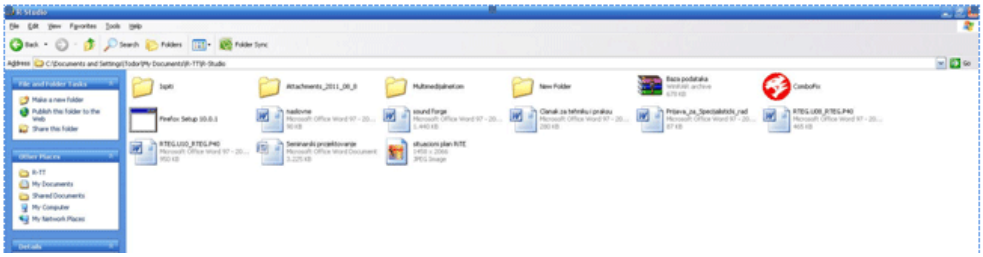
Po završetku skeniranja dobiće se lista fajlova koje je program pronašao na disku.



Slika 8: Izbor fajlova za spasavanje

Može ce izvršiti obeležavanje fajlova koje ce žele sačuvati, i zatim se bira opciju „Recover Marked“, da bi pokrenuo proces spasavanja fajlova.

Program fajlove standardno snima u folder „C:\Documents and Settings\Todor\My Documents\R-TT\R-Studio“. Na slici 9 ce može primetiti da se u direktorijumu nalaze i fajlovi koji su bili na disku pre formatiranja, kao i fajlovi koji su nasnimljeni na disk posle formatiranja. Navednim postupkom se može izvršiti spasavanje izgubljenih fajlova sa diskova raznih veličina i fajl sistema. Jedini preduslov je da disk fizički bude ispravan.



Slika 9: Sadržaj odredišnog foldera posle spašavanja fajlova

5. ZAKLJUČAK

Osnove čuvanja podataka kao i mediji su uglavnom isti i univerzalni, dok su metode reparacije različite. Postoji širok spektar softverskih paketa koji se koriste u ove svrhe: od onih koji su namenjeni korisnicima sa nižim nivoom znanja i koji imaju manje opcija, do visoko profesionalnih koji zahtevaju ozbiljan nivo znanja i detaljno podešavanje prilikom korištenja. U skladu sa složenosti softvera i znanjem korisnika variraju i rezultati reparacije podataka. Ovo je veoma široka oblast za analizu, a kroz primer korišćenja programa R-Studio dat je primer kako se može tretirati ova problematika.

6. LITERATURA

[1] http://www.data-recovery-software.net/
[2] http://www.storageheaven.com/products/degausser_manual_v660.asp
[3] http://www.recovermyfiles.com/file-recovery.php
[4] http://www.hddrecovery.com.au/HDD_Press_2.htm
[5] http://www.storagesearch.com/disksanitizers.html
[6] http://www.csoonline.com/article/218000/PC_Disposal_Hard_Disk_Risk/2
[7] http://www.partitionrecovery.net/