CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Obnavljanje izgubljenih podataka

CCERT-PUBDOC-2009-04-261

+CERT.hr u suradnji s LSS

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada je i ovaj dokument, koji je nastao suradnjom CARNet CERT–a i LS&S–a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr

Nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.LSS.hr

Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Razvojem računala i računalnih mreža podaci igraju sve veću ulogu u poslovnom i osobnom pogledu. Vrijednost podataka ovisi o njihovoj važnosti vlasniku, dobitku koji donose te šteti koja nastaje njihovim gubitkom i/ili oštećenjem. Razni oblici podataka, od osobnih do poslovnih i financijskih, pohranjeni su u mnogobrojnim bazama podataka ili u nekom drugom obliku na poslužiteljima. Takve podatke potrebno je na odgovarajući način zaštititi od bilo kakvog oblika oštećenja.

Podaci pohranjeni na tvrdi disk računala ili neki drugi medij za pohranu mogu biti ugroženi ili fizičkim oštećenjem diska ili logičkim pogreškama datotečnog sustava i drugih komponenti. Nepravilno rukovanje podacima (što uključuje brisanje i prepisivanje datoteka) također donosi veliki dio gubitaka informacija. Zbog važnosti izgubljenih podataka razvijene su razne tehnike obnove podataka za svaki od navedenih tipova oštećenja. Većina tih tehnika ugrađena je u brojne programske alate koji omogućuju jednostavan povrat nestalih informacija (ako one nisu u potpunosti uništene).

Također, statistički podaci pokazuju velike novčane gubitke nastale kao posljedica izgubljenih podataka (oko 18 milijuna dolara). Zbog toga je puno bolja praksa odgovarajuća zaštita sustava, koju predstavlja izrada sigurnosnih kopija. Osim toga, korisnicima se pružaju mjere zaštite poput stvaranja slike diska s podacima, uporabe datotečnog sustava s dnevnikom ili RAID tehnologije.

2. Tipovi gubitaka podataka

Proces obnavljanja podataka je spašavanje podataka sa oštećenih, ugroženih ili pokvarenih medija za pohranu kojima nije moguće pristupiti. Obično se radi o medijima poput tvrdog diska, traka za pohranu, CD i DVD medija, RAID (eng. Redundant Array of Inexpensive Disks) tehnologija i sl. Potreba za obnavljanjem podataka može biti posljedica fizičkog oštećenja medija ili logičkog oštećenja datotečnog sustava.

Najčešći problem koji uzrokuje gubitak podataka uključuje pogrešku operacijskog sustava, a kao rješenje nameće se kopiranje podataka na drugi disk. Obično se to može postići pomoću *Live CD* (prijenosni medij koji sadrži operacijski sustav) tehnologije – tehnologije koja omogućuje upravljanje sustavom, stvaranje sigurnosnih kopija te kopiranje svih podataka u slučaju pogreške u osnovnom operacijskom sustavu na računalu. Nadalje, ovakvi slučajevi mogu biti ublaženi particioniranjem (podjela mjesta za pohranu tvrdog diska u posebna podatkovna područja zvana particije) diska i stalnim kopiranjem osjetljivih podataka u datoteke na particiju koja ne sadrži operacijski sustav.

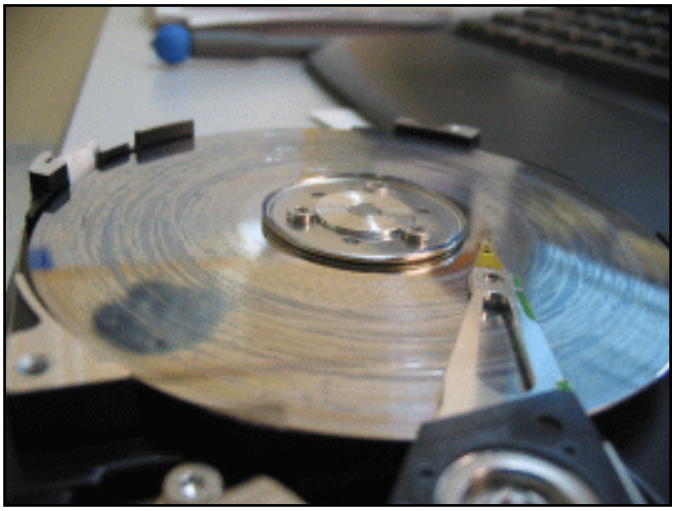
Drugi tip problema uključuje pogrešku na razini diska poput ugrožavanja datotečnog sustava, particije diska ili cijelog tvrdog diska, a posljedica je nemogućnost čitanja podataka. Ovisno o slučaju, rješavanje uključuje povratak ugroženih podataka, kao i zamjenu oštećenih dijelova sklopovlja.

Treći tip uključuje proces povratka podataka koji su obrisani s medija za pohranu.

2.1. Fizička oštećenja

Širok raspon pogrešaka može izazvati fizičko oštećenje medija za pohranu. CD/DVD mediji mogu imati izgrebenu podlogu, tvrdi disk može biti oštećen prilikom dodira glave za čitanje i pisanje (eng. head crash), a trake za pohranu mogu jednostavno puknuti.

Ipak, kao jedan od najčešćih problema u računalima javlja se oštećenje tvrdog diska glavom za čitanje/pisanje kako je prikazano na slici 1. Glava se obično kreće na tankom sloju (tj. „leti“ iznad njega) na površini diska. Gornji sloj diska je napravljen od materijala sličnog teflonu koji ima osobine maziva. Ispod navedenog sloja je sloj ugljika. Ovi slojevi štite magnetski sloj (područje za pohranu podataka) od čestih slučajnih dodira glave za čitanje/pisanje. Oštećenja glavom mogu biti inicirana sitnim česticama prašine koja uzrokuju poskakivanje glave na disku, tako uništavajući magnetsku zaštitu diska. Glava za čitanje/pisanje napravljena je tehnologijom koja uključuje materijal dovoljno čvrst da može oštetiti zaštitne slojeve. Ovakvo fizičko oštećenje može nastati i prilikom slučajnog ispuštanja uređaja pa moderni uređaji sve češće sadrže ii senzor pada u svrhu zaštite (u slučaju detekcije pada ili sličnih štetnih radnji, sustav automatski blokira glavu kako bi spriječio oštećenja ploča diska).



Slika 1. Fizičko oštećenje tvrdog diska

Fizičko oštećenje uvijek uzrokuje neki gubitak podataka, a u većini slučajeva ima za posljedicu i oštećenje datotečnog sustava. To dovodi do logičkih pogrešaka (stanja kod kojih dolazi do problema prilikom

pohrane podataka, izvođenja nekih operacija ili rušenja sustava) koje je potrebno otkloniti prije spašavanja podataka s ugroženog medija.

Krajnji korisnici najčešće ne mogu popraviti fizičko oštećenje računala jer nemaju odgovarajuće znanje i tehnologiju. Dakle, često obnavljanje podataka donosi velike troškove korisnicima. Postoje firme koje se bave tim postupcima, a obično koriste "Class 100" / ISO-5 objekte za zaštitu medija.

2.2. Logičke greške

Osnovni uzroci logičkih pogrešaka su:

- gubitak napajanja koji sprječava zapis struktura datotečnog sustava na medij,
- problemi sa sklopovljem i upravljačkim programima i
- rušenje sustava.

Rezultat bilo koje logičke pogreške je dovođenje sustava u nekonzistentno stanje što može uzrokovati razne probleme, poput:

- neočekivanog ponašanja (npr. upravljački programi prijavljuju negativnu vrijednost slobodnog prostora),
- rušenja sustava i
- gubitak podataka.

Postoje razni programi za ispravak spomenutih stanja, a svi operacijski sustavi sadrže barem osnovni alat za popravak datotečnog sustava. Primjeri uključeni u poznatije operacijske sustave su:

- „fsck“ korisnički program za „Linux“ platforme,
- „Disk Utility“ program namijenjen „Mac OS X“ okruženju i
- „chkdsk“ program za „Microsoft Windows“ platforme.

Dostupni su i dodatni alati poput programa „The Coroners Toolkit“ i „The Sleuth Kit“ koji ponekad mogu pružiti dobre rezultate čak i kada operacijski sustav ne prepoznaje disk. Osim navedenih, program „TestDisk“ se može koristiti za rekonstruiranje tzv. „ugroženih“ particija.

Neke logičke pogreške često se zabunom kategoriziraju u fizička oštećenja. Primjer je pritiskanje glave tvrdog diska, a moguće rješenje problema je ponovna izgradnja programa koji upravljaju elektroničkim uređajima.

Uporaba datotečnih sustava koji bilježe promjene u dnevniku, poput „NTFS“ inačice 5.0, „ext3“ i „XFS“ može smanjiti učestalost logičkih grešaka. Takvi sustavi u svakom trenutku mogu biti vraćeni u konzistentno stanje, a pri tome se gube samo podaci spremljeni u privremenoj memoriji diska u trenutku pojave greške. Ipak, regularno upravljanje sustavom treba uključivati uporabu programa za provjeru konzistentnosti. To osigurava zaštitu od pogrešaka u datotečnom sustavu i skrivenih nekompatibilnosti u dizajnu sklopovlja za pohranu podataka. Jedan primjer nekompatibilnosti je kada program za provjeru diska javlja da su strukture datotečnog sustava pohranjene na disk, a to se zapravo nije dogodilo. Često se takva situacija javlja ako upravljački program pohranjuje podatke u svoju privremenu memoriju, a tvrdi da ih je zapisao na disk. U slučaju gubitka napajanja moguće je stvaranje nekonzistentnog stanja (poput oštećenja ili nepotpunosti dnevnika). Jedno od rješenja je uporaba sklopovlja koje ne prijavljuje da su podaci zapisani dok se spremanje ne obavi. Drugo rješenje (češće korišteno u praksi) je uporaba programa za upravljanje diskom opremljenih s UPS (eng. uninterruptible power supply) tehnologijom. Primjena ovakve tehnologije cijelom sustavu omogućuje zadržavanje podataka i njihovo spremanje prije gašenja računala u slučaju prekida napajanja.

2.3. Obrisani podaci

Brisanje podataka je metoda prepisivanja podataka kojom se u potpunosti uklanjanju svi elektronički zapisi podataka na tvrdom disku ili drugom digitalnom mediju. Trajno brisanje podataka nije isto što i osnovno brisanje datoteka, koje uklanja samo pokazivače na sektor diska te ostavlja mogućnost obnove podataka putem osnovnih programskih alata. Postoje metode koje omogućuju potpuno uklanjanje podataka poput demagnetiziranja (eng. degaussing) i fizičkog uništavanja diska. Za razliku od njih, „obično" brisanje podataka uklanja sve informacije i ostavlja disk uporabljivim.

Postoje tri razine uklanjanja podataka:

1. čišćenje (eng. clearing) osjetljivih informacija – uklanjanje osjetljivih podataka s uređaja za pohranu na takav način da je korisnik siguran kako izbrisane podatke nije moguće rekonstruirati uporabom raznih funkcija sustava ili programa za obnovu podataka. Ipak, podatke je još uvijek moguće obnoviti uporabom nekih specijaliziranih laboratorijskih tehnologija. Obično se koristi kao administrativna zaštita protiv slučajnog otkrivanja podataka u organizacijama. Na primjer, prije ponove uporabe diska njegov sadržaj mora biti očišćen kako bi se spriječilo slučajno otkrivanje podataka slijedećem korisniku.
2. potpuno čišćenje (eng. purging, sanitizing) – uklanjanje osjetljivih podataka sa sustava ili uređaja za pohranu s namjerom da se ne mogu rekonstruirati nikakvim poznatim tehnikama. Obično se obavlja prije otpuštanja medija izvan kontrole firme, kao što je odbacivanje medija ili premještaj u drugo sigurnosno okruženje.
3. uništavanje (eng. destruction) – fizičko uništavanje medija (slika 2) spaljivanjem, taljenjem, mljevenjem, bušenjem ili na neki drugi način kako bi se spriječila obnova podataka.

Slika 2. Fizički uništen tvrdi disk

Jedna od metoda brisanja podataka je njihovo prepisivanje novim podacima (eng. wiping, shredding). Kod najjednostavnijeg oblika prepisivanja pohranjenih podataka zapisuju se neki podaci (obično uzorci nula) po svim sektorima diska, što pruža zaštitu od čitanja podataka s medija uporabom osnovnih funkcija sustava. Kako bi se izbrisali svi tragovi podataka te onemogućila uporaba tehnika obnove podataka, treba se koristiti neki složeniji uzorak (npr. uzorak nula i jedinica).

Nedostatak prepisivanja je činjenica da neki dijelovi diska mogu biti nedostupni zbog oštećenja ili drugih pogrešaka uslijed čestog prepisivanja

2.4. Događaji koji vode do gubitka podataka

Rezultati ispitivanja pokazuju da su najčešći oblici gubitka podataka pogreške u sklopovlju ili ljudske pogreške. Zatim, najčešće zanemarivani uzroci gubitka podataka su prirodne nepogode. U nastavku su navedeni događaji koji mogu dovesti do gubitka podataka:

1. **Namjerne radnje:**
   - namjerno brisanje datoteka ili programa.
2. **Nenamjerne radnje:**
   - slučajno brisanje datoteka ili programa,
   - gubitak CD medija,
   - administratorske pogreške i
   - nemogućnost čitanja nepoznatih formata datoteka.
3. **Pogreške:**
   - gubitak napajanja – rezultira gubitkom podataka koji nisu spremljeni u trajnu memoriju,
   - pogreške u sklopovlju – nepravilan rad glave za čitanje/pisanje na tvrdom disku,
   - rušenje ili zastoj programa – rezultira nemogućnošću spremanja podataka,
   - nedostaci u programima – program ne potvrđuje naredbu spremanja datoteka i
   - nevaljani podaci u datotečnom sustavu ili bazi podataka.
4. **Nesreće:**
   - prirodne nepogode – potres, poplava, tornado,
   - požar.
5. **Zločini:**
   - krađa, sabotaže i sl.,
   - zlonamjerni programi – virusi, trojanski konji i sl.

3. Tehnike oporavka podataka

3.1. Oporavak od fizičkog oštećenja

Obnova podataka nakon fizičkog oštećenja može uključivati raznovrsne tehnike. Neka oštećenja mogu biti ispravljena zamjenom dijelova tvrdog diska. Iako ovaj postupak može omogućiti rad diska, ne isključuje postojanje logičkih pogrešaka. Posebna procedura zvana *disk-imaging* koristi se za obnovu svakog bita koji je moguće pročitati s površine diska. Jednom kada je slika dobivena i spremljena na medij, može biti detaljno analizirana kako bi se rekonstruirali izvorni podaci.

Primjeri procedura za oporavak od fizičkog oštećenja su:

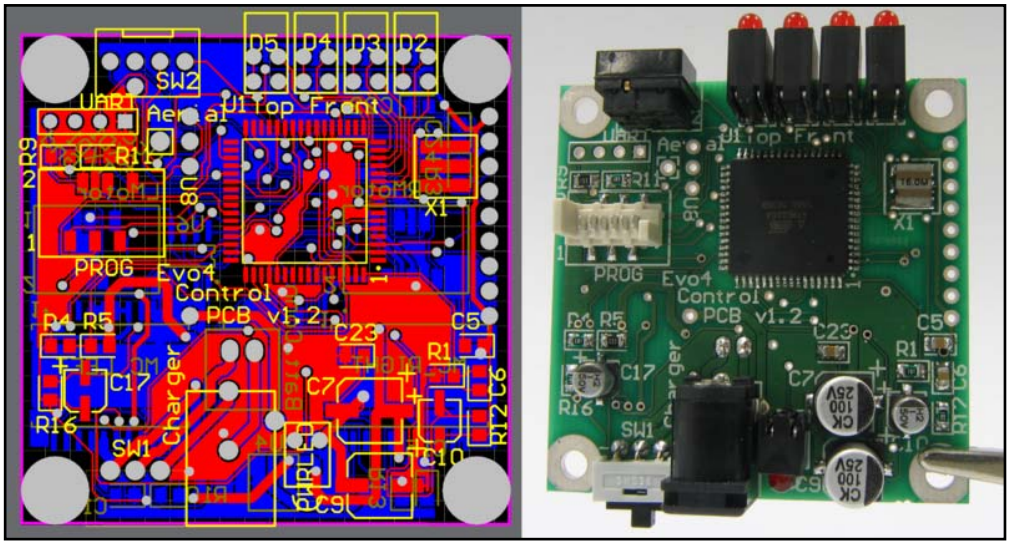
- Otklanjanje ugroženih PCB (eng. printed circuit board) komponenti te njihova zamjena s ispravnim dijelovima,
- Montiranje glave za pisanje/čitanje s obzirom na neoštećeni disk,
- Uklanjanje oštećenih dijelova diska i njihova zamjena novim.

Najčešće se koristi kombinacija svih navedenih procesa.

3.1.1. PCB komponente

PCB komponente spajaju elektroničke krugove kako je prikazano na slici 3, a vrlo su robusne, jeftine i pouzdane. Komponente su obično sačinjene od jednog ili više slojeva izolacijskog materijala. Vodljivi slojevi su izrađeni od tanke bakrene folije. Izolacijski slojevi su povezani zajedno s bakrenom folijom prevučenom termostabilnom smolom. Postoji nekoliko različitih materijala koje je moguće izabrati s obzirom na zahtjeve sklopa. Prema tome, izolacijski sloj je većinom načinjen od plastike, keramike, optički pojačane smole ili nekog drugog materijala.

U slučaju fizičkog oštećenja ovih komponenti jedino moguće rješenje je njihova zamjena s novim komponentama iste vrste. Nakon zamjene fizičke komponente moguće je primijeniti neki od postupaka obnavljanja podataka koji su izgubljeni zbog fizičke pogreške. To uključuje ispravljanje logičkih pogrešaka uporabom nekog programskog alata.



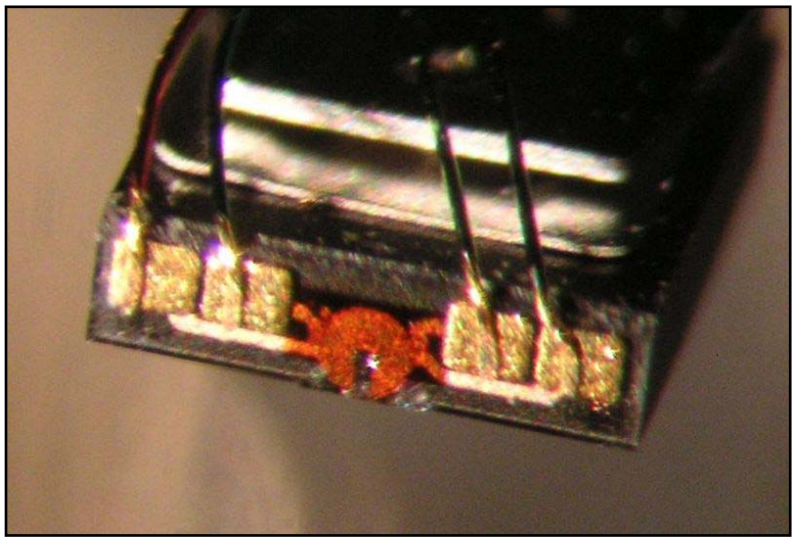
Slika 3. PCB komponente

3.1.2. Glava za pisanje/čitanje

Glava za pisanje/čitanje omogućuje čitanje ili zapisivanje podataka na tvrdi disk. Ona „leti“ iznad diska na udaljenosti od 3 nm. Navedena udaljenost se razvojem tehnologije neprekidno smanjuje kako bi se omogućila veća površinska gustoća (količina podataka koja se može pohraniti u dani prostor tvrdog diska). Da bi se zadržala konstantna udaljenost glave od diska u gotovim uređajima uvodi se tzv. zračni ležaj (eng. air-bearing) pričvršćen na sučelje. Njegova uloga je sprječavanje fizičkog oštećenja diska koje može nastati kada glava dotakne površinu. Uvećan izgled glave za čitanje/pisanje prikazan je na slici 4.

Budući da većina modernih uređaja ima brzinu okretanja diska između 5 400 i 15 000 o/min (okretaja po minuti), popravak fizičkog oštećenja magnetske površine može biti vrlo skupo. Stariji diskovi obično se kreću mnogo sporije i imaju udaljenije glave od površine diska. Pri brzini od 7.200 o/min rub diska putuje preko 74 milja po satu (120 km/h) pa se dodirivanjem glave s diskom ona može pregrijati. Tada dijelovi diska ili cijeli disk mogu postati neuporabljivi dok se glava ne ohladi. Također se javlja mogućnost pojave dodatnih oštećenja diska prilikom dodira glave.

Ispravnost glave za čitanje ključna je u zaštiti sustava od fizičkog oštećenja diska pa i gubitka podataka. U slučaju kvara glave za pisanje/čitanje potrebno je izvršiti zamjenu oštećenog dijela ispravnim komponentama s neoštećenog uređaja. Kod prijenosnih računala ugrađene su dodatne mjere zaštite od oštećenja uslijed čestog pomicanja računala.



Slika 4. Glava za čitanje/pisanje

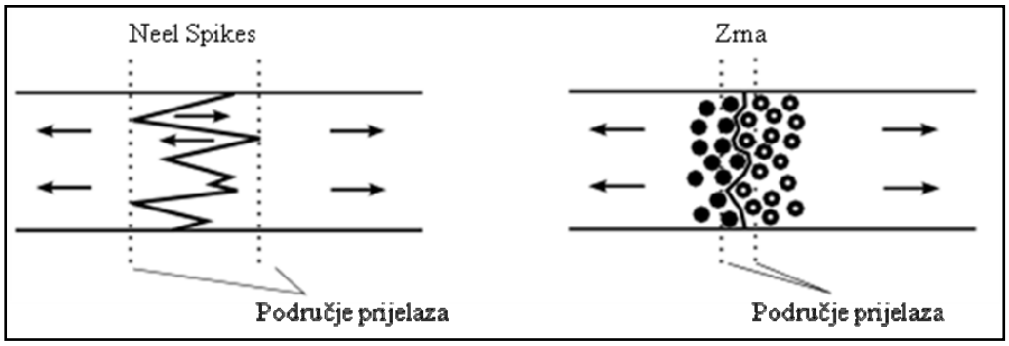
3.1.3. Uklanjanje oštećenih dijelova diska

Magnetska površina diska podijeljena je u male magnetske regije mikrometarskih veličina, od kojih svaka predstavlja jednu binarnu jedinicu podataka (nula ili jedan). Tipična magnetska regija na tvrdom disku je oko 200 do 250 nm široka i 25 do 30 nm duboka. To odgovara veličini od oko 100 bilijuna bitova (100 gigabita) po četvornom inču površine diska. U današnjim tvrdim diskovima svako magnetsko područje je sačinjeno od nekoliko stotina magnetskih zrna, koja su osnovni materijal za stvaranje magnetskih regija.

Jedan od razloga korištenja magnetskih zrna, kao suprotnost kontinuiranom magnetskom mediju, je smanjivanje prostora koji je potreban za jednu magnetsku regiju. U kontinuiranim magnetskim materijalima, pojavljuju se formacije zvane „Neel Spikes“. One sadrže suprotan magnetizam i uzrokuju usmjeravanje magneta u suprotnim smjerovima. To dovodi do problema jer se poništava djelovanje magnetskih polja. Na granicama regija, prijelaz s jednog magnetizma na drugi događa se preko cijele površine te formacije i naziva se širina prijelaza.

Uporaba zrna pomaže riješiti problem jer svako zrno predstavlja jedinstvenu magnetsku domenu. To znači da magnetske domene ne mogu rasti i oformiti područja zvana „Neel spikes“ pa su i područja prijelaza manja. Usporedba opisanih tehnologija prikazana je na slici 5. Kod oštećenja

diska potrebno je zamijeniti ovako oštećena područja te tako omogućiti povratak izgubljenih podataka nekom od tehnika oporavka od logičkih pogrešaka.



Slika 5. Područja prijelaza

3.2. Oporavak od logičke pogreške

Dvije osnovne tehnike obnove podataka nakon logičkih pogrešaka su:

1. provjera konzistentnosti i
2. „data carving" postupak.

Dok većina logičkih oštećenja može biti popravljena uporabom ovih tehnika, programi za obnovu podataka ne mogu garantirati da neće doći do gubitka podataka. Na primjer, u datotečnom sustavu „FAT", kada dvije datoteke dijele istu jedinicu za dodjelu memorije, gubitak podataka jedne od datoteka je garantiran.

3.2.1. Provjera konzistentnosti

Provjera konzistentnosti uključuje skeniranje i provjeru logičke strukture diska kako bi se provjerila konzistentnost u skladu sa specifikacijom. Na primjer, u većini datotečnih sustava direktoriji moraju imati barem zapise:

- točka (.) – pokazuje na njih same,
- točka-točka (..) – pokazuje na roditeljski direktorij.

Program za ispravljanje pogreške datotečnog sustava može čitati svaki direktorij i osigurati da ovi zapisi postoje i pokazuju na ispravne direktorije. Ako otkrije nepravilnosti, takav program pruža ispis poruke o pogreški kako bi se problem mogao ispraviti. Na opisani način funkcioniraju i programi „chkdsk" i „fsck".

Ipak, postupak ima i neke nedostatke. Jedan od njih javlja se u slučaju kada je datotečni sustav ozbiljno oštećen, a dovodi do potpunog neuspjeha provjere konzistentnosti. U tom slučaju, prilikom rukovanja s oštećenim ulaznim podacima, može doći do rušenja programa za ispravak pogrešaka (koji zatim nije u mogućnosti ispraviti oštećenje). Također, postoje situacije kada program za ispravak pogrešaka ne detektira postojanje datotečnog sustava. Drugi od nedostataka je nebriga za podatkovne datoteke. Primjer je situacija kada program „chkdsk" pronađe nerazumljive podatkovne datoteke (ili izvan namijenjenog prostora), on bi mogao ukloniti datoteku bez upozorenja o radnji. Prednost ove funkcionalnosti je lakši rad, ali obrisane datoteke mogu korisnicima predstavljati važne podatke. Sličan problem javlja se i prilikom uporabe diskova za obnovu (obično ih pružaju sustavi tvrtki Dell i Compaq), koji obnavljaju operacijski sustav uklanjanjem prijašnje instalacije. Ovaj problem moguće je izbjeći instaliranjem operacijskog sustava na odvojenu particiju od korisničkih podataka.

3.2.2. Metoda „Data Carving“

Metoda „Data Carving“ je tehnika obnavljanja podataka koja omogućuje identificiranje i izdvajanje dijelova koji pripadaju podacima bez informacija o dodijeljenom memorijskom prostoru. Tehnika obično pretražuje područja diska tražeći željene potpise datoteka. Činjenica da ne postoje informacije o dodjeli memorije znači da je potrebno specificirati veličinu podataka prilikom traženja podudarajućeg potpisa datoteke. Ovo donosi mogućnost pogrešne detekcije ovisno o složenosti potpisa datoteke. Također, postoje zahtjevi za pohranom obnovljenih podataka u slijedna područja (a ne fragmentirano). Metoda „Data Carving“ donosi uštedu na vremenu i resursima.

Metoda je u nastavku opisana na nekoliko osnovnih formata datoteka:

- Zip datoteka podijeljena je u specifične dijelove koje je moguće identificirati preko posebnih potpisa. Osnovni oblik datoteke je arhiva individualnih sažetih datoteka, lokalnih datoteka sa zaglavljem koje ima oznaku „50 4B 03 04“, podacima i opisnikom „50 4B 07 08“. Veličina svake lokalne datoteke zapisana je u zaglavlju ili opisniku te u središnjem zapisniku kojeg je moguće identificirati putem potpisa „50 4B 01 02“. Kraj tog zapisnika označava potpis „50 4B 05 06“, a omogućuje očitavanje veličine zapisa i pomak lokacije od zaglavlja prve datoteke. Pozicioniranjem na potpis završetka središnjeg zapisnika i pomakom ispravnog broja okteta podataka (veličina zapisnika + pomak) moguće je doći do početka prve lokalne datoteke u arhivi.

  Ako se pri procesu pomaka otkrije da je početak prve lokalne datoteke više udaljen nego je izračunato, radi se o fragmentiranom bloku. Tada je potrebno otkriti koji fragmenti ne pripadaju arhivi pregledom opisnika ili središnjeg zapisnika. Veličina sažetih datoteka (uključujući i zaglavlja) smještena je na pomaku 0x14 od središnjeg zapisnika svake lokalne datoteke (koji počinje potpisom „50 4B 01 02“). Krećući od zaglavlja prve datoteke i pomakom za veličinu sažete datoteke treba doći na početak zaglavlja sljedeće datoteke. Ako se pri pomaku ne dođe na početak sljedeće datoteke, zaključuje se da ta datoteka sadrži fragmente. Nakon identificiranja svih datoteka koje sadrže fragmente iste se uklanjaju (te datoteke su onda trajno izgubljene, ali su se „spasile“ sve ostale).

- Složene datoteke dokumenata dijele se u tokove koji se zatim dijele u sektore koji sadrže upravljačke podatke ili korisničke podatke. Cijela datoteka se sastoji od zaglavlja i liste sektora koji slijede zaglavlje. Fiksnu veličinu sektora moguće je postaviti u zaglavlju. Početak pretrage započinje traženjem složenog zaglavlja dokumenta „D0 CF E0 A1 B1 1A E1“. Na pomaku 0x1E od početka zaglavlja nalazi se vrijednost koja označava veličinu sektora (obično 512 okteta). Zatim, na pomaku 0x2C nalazi se znak „#“ koji koristi SAT (eng. Sector Allocation Table), a na 0x30 početni broj sektora. Također je moguće pronaći SSAT (eng. Short- Sector Allocation Table) na pomaku 0x3C (ali ne kod svih vrsta dokumenata). Sljedeći parametar je MSAT (eng. Master Sector Allocation Table) na pomaku 0x44 iza kojeg dolaze podaci (436 okteta). SSAT i MSAT označavaju podatkovne strukture koje sadrže određene informacije o pohranjenim podacima.

  Koristeći prvi sektor MSAT parametra i uspoređujući ga s vrijednošću s početka dokumenta moguće je otkriti da li ima fragmentiranih blokova ispred MSAT dijela. Zatim je potrebno potražiti početak zapisnika (potpis „52 00 6F 00 74 00 20 00 45 00 6E 00 74 00 72 00 79 00“) krećući od zaglavlja dokumenta. Pronađenu vrijednost u zapisniku potrebno je usporediti s vrijednošću na pomaku 0x30. Ako nema razlike, ne postoje fragmenti između početka datoteke i zapisnika, a ako razlika postoji tada ima nekih fragmenata koji ne pripadaju dokumentu. Najveći objekt u složenom dokumentu je najvjerojatnije traženi dokument (npr. Word dokument ili Workbook objekt), a fragmenti se najčešće upravo tu javljaju.

3.3. Oporavak obrisanih podataka

Što se tiče obnove obrisanih podataka, svaki operacijski sustav sadrži neki oblik zaštite od slučajnog brisanja datoteka. Obrisane datoteke je tako moguće lako povratiti ako je to potrebno. Jedan od primjera je komponenta „Recycle Bin" kod operacijskog sustava „Microsoft Windows".

Također, postoje razni specijalizirani programi koji omogućuju obnavljanje određenog oblika datoteka (slikovnih datoteka, dokumenata, glazbenih datoteka, poruka elektroničke pošte i dr.).

U slučaju brisanja podataka njihovim prepisivanjem drugim podacima oporavak nije tako jednostavan. Zapravo, mnogi stručnjaci tvrde da ne postoji način na koji je moguće obnoviti prepisane podatke. Peter Gutmann istraživao je obnavljanje podataka s prepisanih medija sredinom 90-ih godina. Predložio je postupak obnove zvan MFM (eng. magnetic force microscopy) te razvio posebne uzorke za razne tehnologije koji su kasnije postali poznati kao Gutmann-ova metoda. Još uvijek nije praktično dokazano niti da je moguće niti da nije moguće izvesti obnovu podataka koji su prepisani drugim podacima.

4. Specijalizirani programski alati

U nastavku dokumenta opisano je nekoliko alata kategoriziranih u pet skupina prema funkcionalnosti za koju su napravljeni. Popis ostalih alata koji služe za provjeru stanja sustava ili obnovu podataka moguće je pronaći na slijedećoj poveznici:

http://www.dmoz.org/Computers/Hardware/Storage/Data_Recovery//

4.1. Alati s ugrađenim operacijskim sustavom

Obnova podataka ne može uvijek biti obavljena dok je radni operacijski sustav kojeg korisnik upotrebljava pokrenut. Kao rješenje tog problema izrađeni su *boot* diskovi (prijenosni medij kojeg je moguće učitati i pokrenuti na računalu), Live CD i USB (eng. Universal Serial Bus) tehnologije, kao i Live Distro tehnologije, koje sadrže „mali operacijski sustav" i skupinu alata za ispravak.

Neki od alata takvog tipa su:

- **"Knoppix"**

  Operacijski sustav temeljen na „Debian" platformi kojeg je moguće pokrenuti sa CD ili DVD diska. Razvio ga je Klaus Knopper, savjetnik za „Linux" platforme. Postoje dvije inačice programa:

  - tradicionalna CD inačica (700 MB) i
  - DVD Maxi inačica (4,7 GB).

  Može se koristiti za jednostavnu obnovu podataka s tvrdog diska koji sadrži operacijski sustav kojem nije moguće pristupiti. Također ga je moguće koristiti kao dodatni operacijski sustav umjesto instaliranja novog.

  Program „Knoppix" (slika 6) radi na mnogo osobnih i prijenosnih računala, ali ne na svima jer ne podržava automatsko otkrivanje svih vrsta sklopovlja.

Slika 6. Program „Knoppix“

- **“Ubuntu Rescue Remix”**

  „GNU/Linux“ sustav koji se pokreće sa CD ili USB uređaja, a uključuje program za obnovu podataka otvorenog programskog koda, kao i druge forenzičke alate. Krajnji korisnici imaju pravo uporabe, izmjene i poboljšanja programa te distribucije modificirane ili nemodificirane inačice.

  Program ne koristi grafičko već tekstualno sučelje tj. konzolu za naredbe. Trenutna inačica je 8.10, a sadrži i alat „GNU ddrescue“ inačice 1.9 (program za obnovu podataka koji kopira datoteke s jednog uređaja na drugi prilikom pogrešaka čitanja).

- **“SystemRescueCD”**

  Operacijski sustav koji se pokreće s Live CD ili USB prijenosnog medija za pohranu podataka, a omogućuje obnovu podataka nakon rušenja sustava. Razvio ga je tim pod vodstvom Francois Dupoux-a, a temelji se na distribuciji „Gentoo Linux“. Upotrebljava platformu „Linux“ s jezgrom inačice 2.6.27.17 i ima opcije poput spajanja na Internet mrežu putem ADSL modema te grafičke web preglednike (kao što je „Mozilla Firefox“).

  Alat posjeduje podršku za većinu datotečnih sustava: „NTFS“, „FAT32“ i „Mac OS HFS“. Također, omogućen je rad na „Windows“, „FreeDOS“, „PowerPC“ i „Macs“ sustavima.

- **“NeroBackItUp ImageTool”**

  Okruženje koje omogućuje obnovu slike stvorene pomoću „NeroBackItUp“ i/ili „NeroBackItUp ImageTool“ alata. Služi za vraćanje sustava u konzistentno stanje u slučaju pogreške. “. Radi se o komercijalnom programu koji je dostupan na mnogim jezicima koji sadrži podršku za rad na operacijskim sustavima „Windows“ XP, 2003 i „Vista.

- **“Selkie Rescue Data Recovery”**

  Alat s ugrađenim operacijskim sustavom koji služi za obnovu podataka na drugo računalo uporabom direktne veze među dva računala ili putem lokalne računalne mreže. Omogućen je rad na svim inačicama operacijskog sustava „Microsoft Windows“ (Win95 /98 /98 SE /Me /2000 /NT /XP /2003 /). Sadrži jednostavno korisničko sučelje, i dostupan je na engleskom jeziku.

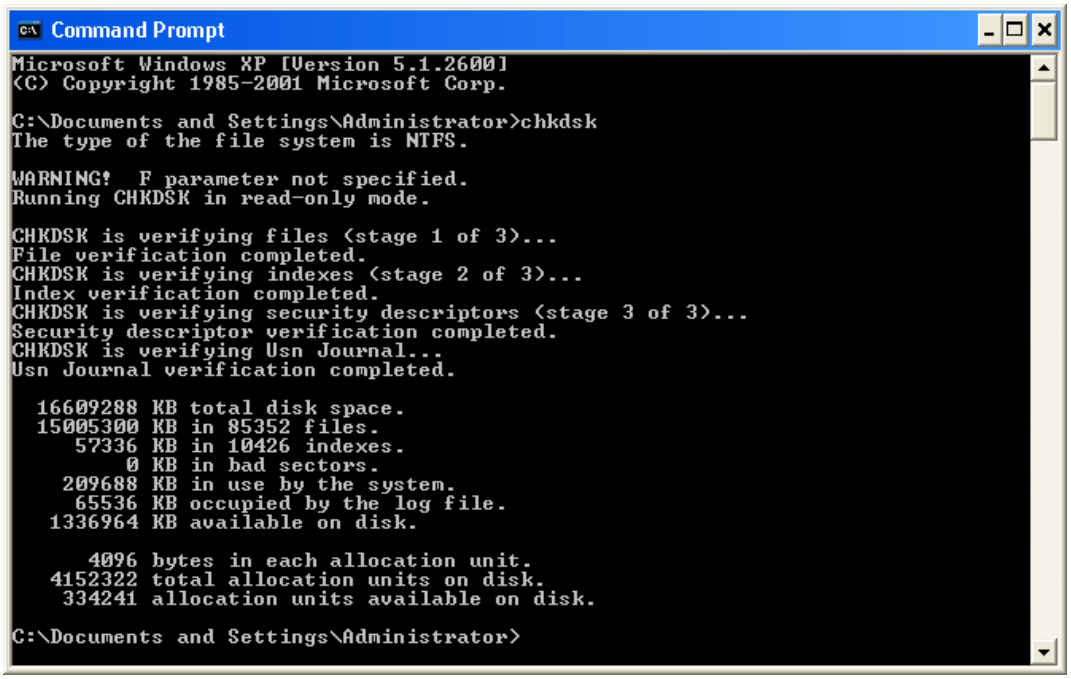
4.2. Alati za provjeru konzistentnosti

Neki od alata koji omogućuju provjeru konzistentnosti sustava su:

- **„CHKDSK“ (eng. Checkdisk)**

  Naredba na računalima s operacijskim sustavima „DOS“, „OS/2“ i „Microsoft Windows“ koja prikazuje status datotečnih sustava na tvrdom disku. Ima mogućnost ispravka logičkih pogreška datoteka, a slična je naredbi „fsck“ kod platformi „Unix/Linux“. Na računalima na kojima je pokrenuta inačica operacijskog sustava „Windows NT“, „CHKDSK“ ima mogućnost provjere i sučelja diska u svrhu otkrivanja fizičke pogreške ili uništenih područja na disku. Neke inačice naredbe mogu obnoviti podatke koje je moguće pročitati u slučaju otkrivanja fizičke pogreške.

  Jedan od glavnih nedostataka ovog alata je nemogućnost rada s uključenim /f (ispravljanje pogrešaka na određenom području) ili /r (otkrivanje oštećenih sektora i obnavljanje čitljivih informacija) opcijama jer neke aplikacije (anti-virus, anti-spyware ili vatrozid programi) sprječavaju pristup particijama. Osim toga, inačica namijenjena „MS-DOS“ 5.0 platformi može dovesti do ugrožavanja podataka. Opisani programski alat prikazuje slika 7.



Slika 7. Naredba „CHKDSK“

- **“Disk First Aid”**

  Besplatan program koji je razvila tvrtka „Apple Inc.“, a namijenjen je operacijskim sustavima „Mac OS“. Navedeni alat služi za provjeru i ispravak problema strukture direktorija kod HFS (eng. Hierarchical File System) ili HFS Plus tvrdih diskova. Moguće ga je koristiti za provjeru sustava prilikom:

  - čestih rušenja sustava,
  - nestajanja datoteka,
  - promjene veličine datoteka,
  - nemogućnosti kopiranja datoteka,
  - pojave poruka o pogreškama kriptiranja i
  - nemogućnosti spremanja datoteka.

- **“Disk Utility”**

  Uslužni program koji je razvila tvrtka Apple za uporabu na „Mac OS X“ platformama. Omogućuje funkcije poput:

- stvaranja, sažimanja i kriptiranja slika diska (objašnjenje pojma nalazi se u poglavlju „Izrada slike diska“),
- omogućavanja ili onemogućavanja dnevnika,
- provjere integriteta diska te ispravka pogrešaka,
- provjere i ispravka korisničkih ovlasti nad pojedinim datotekama,
- brisanja, formatiranja i particioniranja diska,
- osiguravanja brisanja podataka,
- stvaranja, uklanjanja i ispravka RAID skupina te
- kopiranja slika diska na CD, DVD uređaje.

➢ **„fsck“** („file system check" ili „file system consistency check")

Alat koji služi za provjeru konzistentnosti kod „Unix/Linux“ i sličnih operacijskih sustava. Općenito, „fsck“ se pokreće automatski kada sustav otkrije da je datotečni sustav u nekonzistentnom stanju (uključujući i gašenje uzrokovano rušenjem ili nestankom napajanja). Obično pruža operacije za:

- ispravak oštećenog datotečnog sustava (s tim da korisnik mora odlučiti kako popraviti pojedini problem),
- automatsko odlučivanje ispravka pogrešaka (korisnik ne mora donositi odluku svaki put kad se pojavi problem) i
- pregleda problema koji se trebaju ukloniti bez ispravka istih.

Administrator sustava ima mogućnost ručnog pokretanja alata, ali mora biti svjestan činjenice da može doći do gubitka ili ugrožavanja podataka.

4.3. Alati za obnovu datoteka

U nastavku su opisana dva programa koja služe za obnovu datoteka:

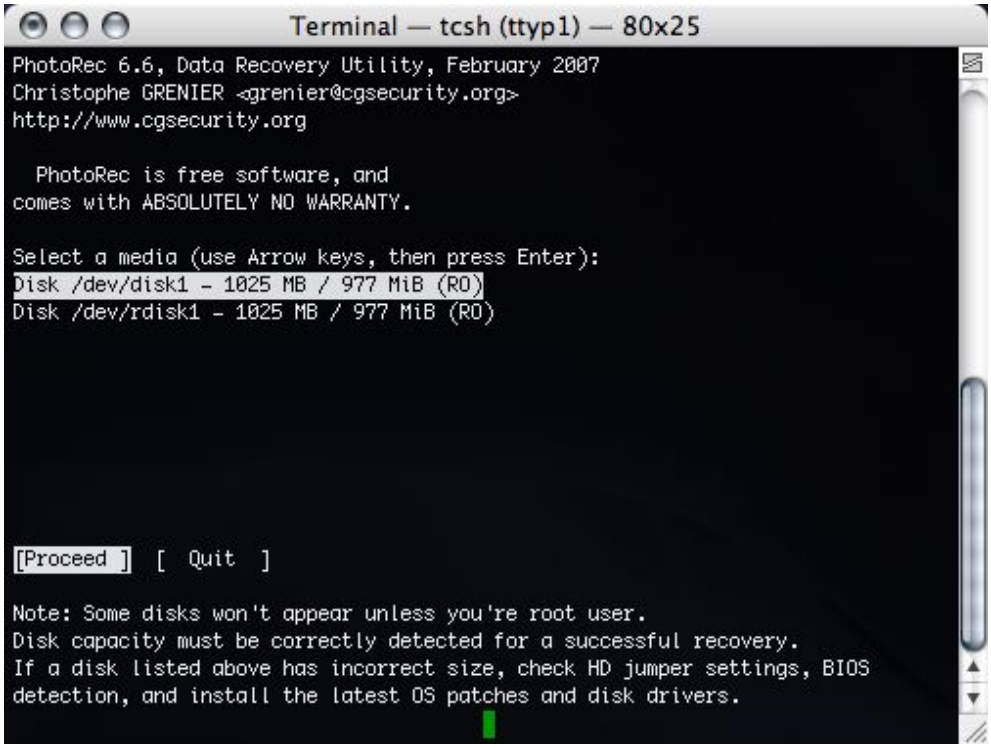
➢ **„PhotoRec“**

Program za obnovu podataka dizajniran za obnovu datoteka s memorije digitalnih kamera (CompactFlash, Memory Stick, SecureDigital, SmartMedia, Microdrive, MMC, USB Memory Drives i sl.), tvrdog diska i CD/DVD prijenosnih medija. Omogućuje obnovu:

- osnovnih slikovnih formata (uključujući JPEG),
- audio datoteka (npr. MP3, WAV),
- formata za dokumente (kao što su Microsoft Office, PDF i HTML) te
- formata za arhive (primjerice .zip).

Prilikom čitanja oštećenih podataka program „PhotoRec“ *ispravljene* datoteke zapisuje u direktorij u kojem je pokrenut ili neki drugi po korisnikovom izboru (a ne u oštećeni direktorij iz kojeg čita podatke). Rad alata prikazuje slika 8.

Sadrži podršku za sljedeće operacijske sustave: „DOS“, „Microsoft Windows“, „Linux“, „FreeBSD“, „NetBSD“, „OpenBSD“, „SunOS“ i „Mac OS X“.



Slika 8. Program „PhotoRec"

- **"SanDisk RescuePRO"**

  Program "RescuePro" izvorno je dizajniran za obnovu podataka kao što su slučajno obrisane ili izgubljene slikovne datoteke, sa memorijskih kartica proizvođača SanDisk. ResucePro omogućuje i obnovu:

  - slikovnih dokumenata,
  - poruka elektroničke pošte,
  - video zapisa i
  - glazbe.

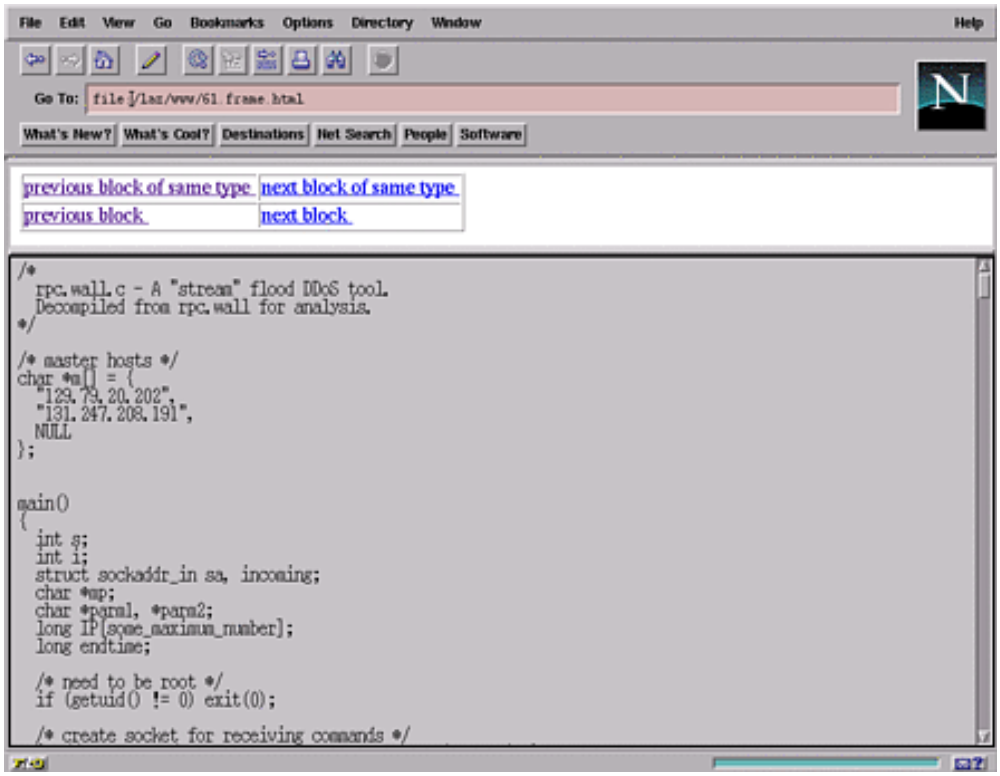
  Sadrži podršku za rad u većini USB, FireWire ili FlashPath tehnologija, a može spasiti podatke sa Palm Pilots, Windows CE uređaja, digitalnih kamera, MP3 uređaja i sl. Sadrži podršku za operacijske sustave „Microsoft Windows", „Linux" i „Macintosh" te ne zahtjeva dodatne upravljačke programe.

4.4. Forenzički alati

Kratki opis nekoliko forenzičkih alata dan je u nastavku dokumenta:

- **„TCT“** (eng. The Coroner's Toolkit)

  Program za sigurnost računala koji su dizajnirali stručnjaci Dan Farmer i Wietse Venema. Namjena spomenutog programa je izvođenje forenzičke analize „Unix“ sustava nakon iznenadnog prekida napajanja računala. Neki dijelovi programa „TCT“ omogućuju analizu i obnovu podataka i nakon nekih drugih tipova pogrešaka. Moguće ga je pokrenuti na „FreeBSD“, „OpenBSD“, „BSD/OS“, „SunOS/Solaris“, „Linux“ te „HP-UX“ platformama. Na slici 9 dan je prikaz sučelja opisanog alata.



Slika 9. Program „TCT“

- **„TSK“** (eng. The Sleuth Kit)

  Skupina biblioteka i alata koji omogućujeju forenzičku analizu „Unix“ i „Microsoft Windows“ operacijskih sustava, a stvorio ih je Brian Carrier. Omogućuju pretragu i izdvajanje slikovnih datoteka na „Windows“, „Linux“ i „Unix“ platformama. Radi se o besplatnom alatu, otvorenog programskog koda koji pruža brojne specijalizirane naredbe.

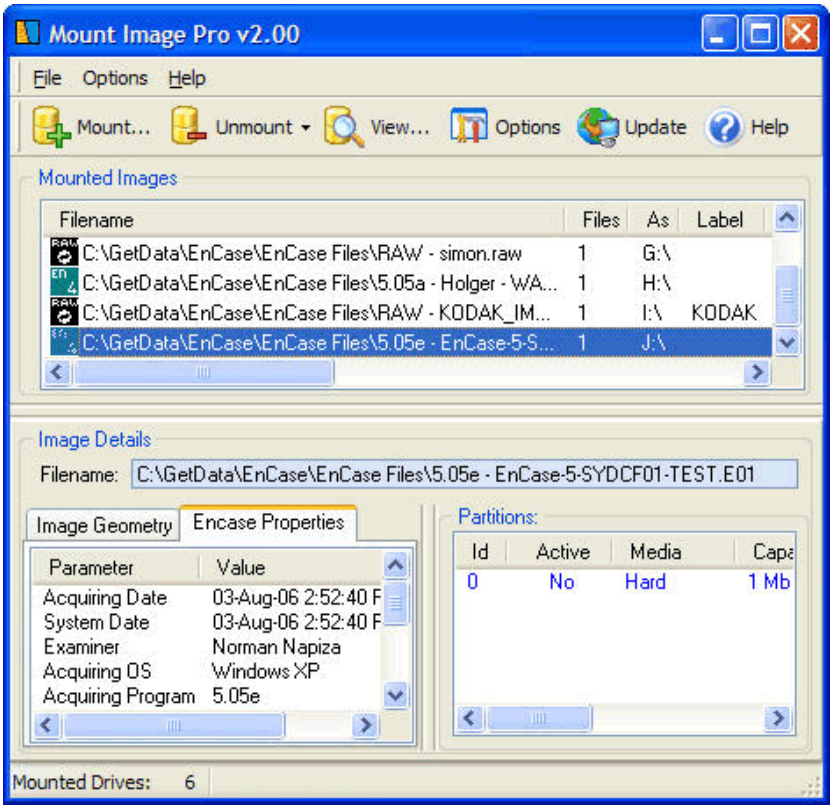
  Neki od alata koje TSK uključuje su:

  - „ils“ – ispisuje sve zapise meta-podataka (poput Inode),
  - „dls“ – prikazuje podatke zaključane u datotečnom sustavu,
  - „fls“ – ispisuje datoteke kojima je dodijeljena memorija unutar datotečnog sustava,
  - „fsstat“ – prikazuje statistiku o datotekama (medij za pohranu),
  - „ffind“ – pretražuje imena datoteka koje ukazuju na neki posebni zapis,
  - „mactime“ – stvara vremensku liniju svih datoteka prema MAC vremenu i
  - „disk_stat“ (trenutno samo na „Linux“ platformi) – otkriva postojanje HPA (eng. Host Protected Area) područja.

- **„EnCase“**

  Skupina alata za forenzičku analizu koju je proizvela organizacija Guidance Software (NASDAQ: GUID). Koristi se u mnogim agencijama za provedbu zakona diljem svijeta jer omogućuje kvalitetno snimanje podataka spremljenih na osobno računalo te njihovu obnovu. Postoji i mrežna inačica koja pruža mogućnost uzimanja tzv „snapshot“ uzoraka RAM memorije na ciljanom računalu.

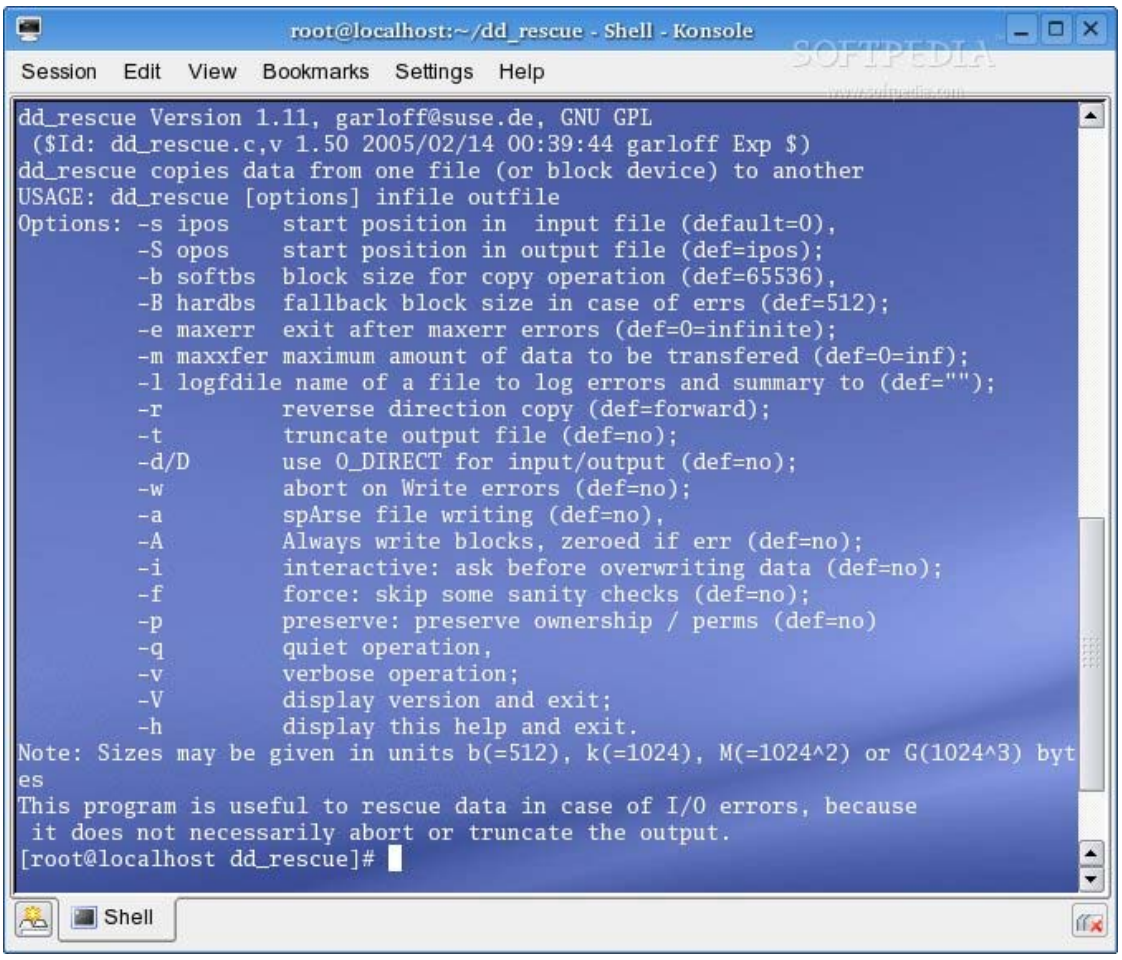
  Prvi korak prilikom uporabe programa je stvaranje slike medija (tvrdog diska ili CD diska). Slika se pohranjuje u vlasničkom formatu i sadrži MD5 ili SHA-1 vrijednost za provjeru autentičnosti. Sljedeći korak je ispitivanje datoteka pohranjenih na slici uporabom osnovnih alata (poput preglednika dokumenata i HEX urednika). Moguće je pregledati i dijelove datotečnog sustava poput izbrisanih zapisa datoteka, podataka za provjeru autentičnosti i dnevnika. Konačno, svaka datoteka može biti pohranjena na korisničko računalo, zajedno s podacima za provjeru autentičnosti i drugim meta-podacima.



Slika 10. Sučelje alata „EnCase“

4.5. Alati za izradu slike diska

Jedan od alata koji omogućuje stvaranje slike tvrdog diska je program „ddrescue“. Radi se o osnovnom alatu za kopiranje i pretvorbu podataka koji je namijenjen operacijskom sustavu „Unix“. Koristi se za kopiranje više okteta podataka ili blokova podataka, pri čemu obavlja pretvorbu podataka (iz EBCDIC u ASCII format). Ako se koristi opcija „logfile“ za obnovu podataka, podaci su vrlo efektivno obnovljeni te mogu biti korišteni i kasnije u bilo kojem trenutku. Još jedna pogodnost je automatsko upravljanje sigurnosnim kopijama. Prilikom pokretanja alata sa istom izlaznom datotekom alat pokušava popuniti praznine. Ako korisnik posjeduju više kopija iste oštećene datoteke te na svima pokrene alat s istom izlaznom datotekom, moguće je dobiti potpuno obnovljenu datoteku. To je posljedica činjenice da je vjerojatnost postojanja oštećenja na istom mjestu u više različitih datoteke vrlo mala. Osnovne operacije su u potpunosti automatizirane, što znači da ne treba čekati da se dogodi pogreška, zaustavljati program, čitati zapise i sl. Osim toga, služi i u forenzičke svrhe kada je potrebno cijeli disk prikazati kao kopiju točnih okteta podataka. Slika 11 prikazuje sučelje alata „ddrescue“.



Slika 11. Program „ddrescue“

5. Statistike

5.1. Novčani gubici

Novčani gubici uzrovani gubitkom podataka vezani su uz događaje koji su doveli do gubitka podataka. Osim toga, usko su povezani s vrijednošću izgubljenih podataka tj. gubitkom do kojeg dolazi zbog nedostupnosti potrebnih podataka. Prilikom računanja gubitka potrebno je uzeti u obzir cijenu:

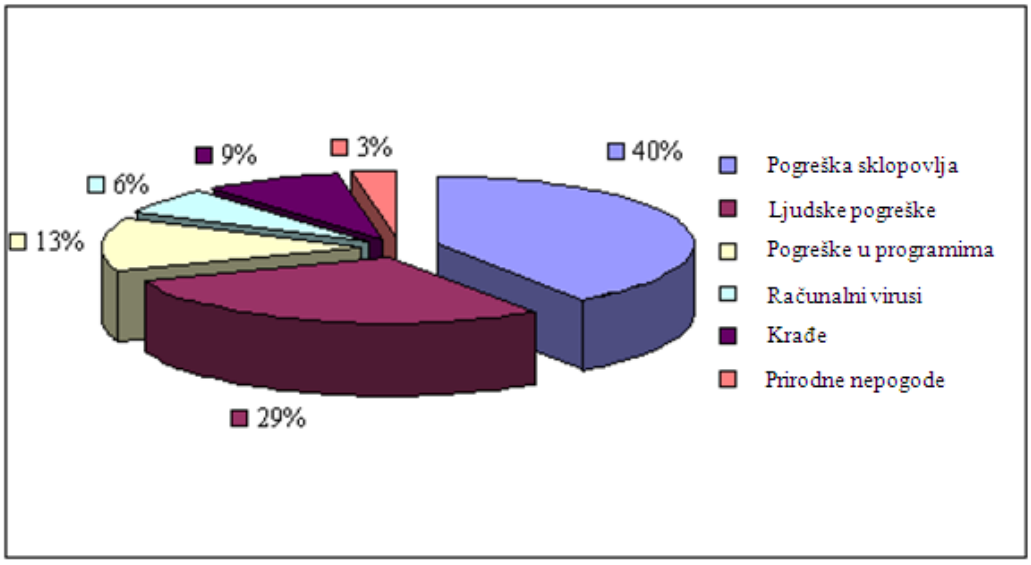
- daljnjeg rada bez podataka,
- ponovnog stvaranja podataka (uključujući obnavljanje podataka) i
- obavještavanja korisnika u slučaju zlouporabe ili nemogućnosti obnove podataka.

Kako bi se prikazala važnost pravilne brige o podacima u nastavku su dani statistički podaci prikupljeni iz raznih izvora:

1. 6% svih korisnika računala u svijetu imalo je neki gubitak podataka. Prema tome, uzimajući u obzir broj osobnih računala u SAD-u, 1998. godine bilo je oko 4,6 milijuna gubitaka podataka što donosi novčani gubitak od 11,8 milijuna dolara.
2. 30% svih poslovnih organizacija prestaje raditi u roku od jedne godine zbog gubitka svih podataka, a 70 % njih u roku od 5 godina.
3. 31% korisnika osobnih računala izgubi datoteke zbog događaja koji nisu pod njihovom kontrolom.
4. 34% tvrtki ne isptuje sigurnosne kopije, a od onih koji to čine 77% pronalazi pogreške na kopijama.
5. 60% tvrtki nakon gubitka podataka prestaje raditi u roku od 6 mjeseci nakon nesreće.
6. 93% firmi koje izgube podatke na 10 ili više dana zbog neke pogreške dolaze do stečaja u roku od jedne godine.
7. 50% poslovnih organizacija koje ostaju bez upravljanja podacima na neko dulje vrijeme dolaze do stečaja istog trenutka.
8. Američke poslovne organizacije izgubile su više od 7,6 bilijuna dolara kao rezultat štete nastale od zloćudnih programa tijekom prvih 6 mjeseci 1999. godine.
9. Jednostavno obnavljanje upravljačkog programa može koštati do 7,500 dolara, a uspjeh nije zajamčen.

5.1.1. Uzroci gubitaka

Gubitak podataka na računalu može imati uzrok u pogrešci sklopovlja ili programa. Skupljanjem podataka iz organizacija koje se bave osiguravanjem računala i obnovom podataka dobiveni su statistički podaci prikazani na slici 12. Prema njima, najčešći uzrok gubitaka podataka su pogreške u sklopovlju (fizičko oštećenje), koje zauzimaju oko 40% svih uzroka gubitaka podataka. Ljudske pogreške donose oko 30 % gubitaka podataka, a uključuju slučajno brisanje podataka te slučajno oštećenje sklopovlja (npr. ispuštanje prijenosnog računala). Pogreške u programima, poput štete nanijete programima za dijagnostiku, obuhvaćaju oko 13% uzroka gubitaka podataka. Zatim, 6% gubitaka podataka uzrokuju zloćudni programi, a 9% krađe računala (obično prijenosnih računala). Na kraju, najmanje gubitaka (oko 3%), donose prirodne nepogode poput poplava, požara i sl.



Slika 12. Udio pojedinog uzroka gubitka podataka

Izvori: Safeware, The Insurace Agency, Inc., „2000 Safeware Loss Study" 2001.

ONTRACK Dana International, Inc,. „Understanding Dana Loss", 2003.

Ovi podaci mogu se unijeti u tablicu kako bi se odredio broj gubitaka podataka koji se događa svake godine. Ako se uzme broj računala od 76,2 milijuna (broj računala u SAD-u), dobiju se podaci prikazani u tablici 1.

Vrsta gubitaka	Broj gubitaka
Pogreške sklopovlja	1 849 800
Ljudske pogreške	1 345 300
Pogreške u programima	588 600
Pogreške zbog zloćudnih programa	294 300
Krađe	403 000
Prirodne nepogode	126 100
Ukupno	**4 607 100**

Tablica 1. Broj gubitaka podataka zbog pogrešaka

U slučaju gubitka podataka oni mogu biti:

- trajno izgubljeni ili
- obnovljeni nekom od tehnika.

Prilikom računanja gubitka treba uključiti obje mogućnosti. Trajan gubitak podataka događa se prilikom krađe, dok se u drugim slučajevima podaci mogu pokušati obnoviti. Prema tome može se pretpostaviti da se u 84% slučajeva podaci mogu obnoviti.

Prvi novčani gubitak prilikom obnove podataka povezan je s iznajmljivanjem specijalizirane podrške za takve radove. Ako takva osoba postoji u firmi, potrebno je uračunati sate utrošene u obnavljanje podataka. Prema zadnjim procjenama, računalni stručnjak zaradi oko 28,10 dolara po satu, ali vrijeme potrebno za obnovu podataka može jako varirati. U prosjeku je potrebno oko 6 sati da bi se obnovili izgubljeni podaci, što daje novčani gubitak od oko 170 dolara. Ako firma nema zaposlenog specijalista, iznajmljivanje specijalizirane firme može biti i tri puta skuplje (znači oko 340 dolara).

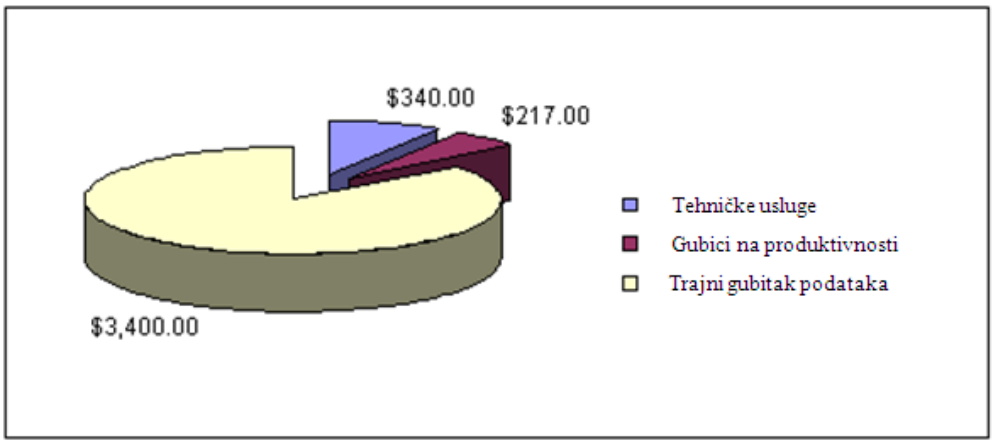
Tijekom razdoblja obnove podataka oni su neupotrebljivi, kao i računalo koje je oštećeno, što donosi smanjenu produktivnost i nove gubitke. Svaka osoba koja za rad koristi računalo zaradi oko

36,20 dolara po satu, što znači da prilikom obnove podataka (prosječno trajanje 6 sati) dolazi do gubitka od 217 dolara.

Konačni gubici moraju uključiti i gubitak podataka koji se ne mogu povratiti (17% slučajeva). Vrijednost podataka ovisi o njihovoj zamjenjivosti, vremenu potrebnom da ih se nadoknadi, a to može jednu firmu koštati čak i milijune dolara. Iako je teško mjeriti vrijednost podataka, neki izvori navode da je vrijednost 100 MB podataka oko 1 milijun dolara, što znači 10 000 dolara za svaki MB izgubljenih podataka. Ako se u račun uključi postotak takve vrste gubitaka ovi se iznosi znatno smanjuju (za 2 Mb izgubljenih podataka dobijemo gubitak od 3 400 dolara).

Kada se zbroje gubici zbog tehničkih usluga, izgubljene produktivnosti i vrijednosti podataka koji se ne mogu obnoviti, dobije se gubitak zbog svake pogreške od oko 3 957 dolara. Ipak treba napomenuti da oko 83% slučajeva rezultira s troškovima od 557 dolara, ali ostali daju prosjek od 20 557 dolara.

Dobiveni rezultati prosječnog novčanog gubitka po jednom gubitku podataka prikazani su na slici 13.



Slika 13. Novčani gubitak po pojedinom gubitku podataka

Izvori: Denise Deveau, „Lost all your dana? Time To Call the Experts“, The Globe and Mail, Feb 25, 2000.; Bareau of Labor Statistic, Employer Costs for Employee Compensation, March 2003.; Bareau of Labor Statistic Occupational Employment Statistic Survey, 2001.

Kada se informacije o broju gubitaka informacija spoje s novčanim gubicima zbog jednog gubitka, dobije se cjelokupna slika. Za broj gubitaka u SAD-u, koji se računa prema ukupnom broju računala, dolazi se do novčanog gubitka od 18,2 milijuna dolara. Također, primjećuje se povećanje ukupnog novčanog gubitka, jer je gubitak 1999. godine bio 11,8 milijuna dolara.

5.2. Primjeri prekršaja

U svibnju 2008. godine službenici Sveučilišta u Floridi obavijestili su 1900 pacijenata UF (eng. University of Florida) plastične kirurgije o nepravilnom upravljanju podacima te otkrivanju privatnih informacija o njihovom zdravlju. Dr. Francis Ong, asistent na UF College of Medicine-Jacksonville, nesigurno je pohranio fotografije i identifikacijske podatke (imena, datume rođenja, osobne brojeve i sl.) na računalo. Zatim je isto računalo posudio obiteljskim prijateljima u siječnju ili veljači 2008. godine. Jedan od prijatelja zamijenio je operacijski sustav na računalu, što je rezultiralo trajnim gubitkom većine informacija o pacijentima. Prema UF politici, povjerljive informacije treba pohranjivati u visoko osigurane poslužitelje na sveučilištu, a ne na osobna računala. Pohranom podataka na osobno računalo, dr. Ong je prekršio pravila Sveučilišta na Floridi.

Jedan od većih gubitaka podataka dogodio se u kolovozu 2008. godine kada je „Home Office" poduzetnik izgubio USB uređaj s nezaštićenim podacima o 84 000 zatvorenika u Engleskoj i Wales-u. Na uređaju je bilo pohranjeno sljedeće:

- osobni podaci o zatvorenicima (imena, datumi rođena, datum isteka kazne i sl.),
- podaci o 10 000 prijestupnika (imena, datumi rođenja) i
- podaci o programu istraživanja droga (inicijali prijestupnika).

Budući da nije postojala sigurnosna kopija podataka niti su podaci bili zaštićeni na odgovarajući način, ovim gubitkom nanesena je ogromna šteta cijelom kaznenom sustavu Engleske.

U siječnju 2009. godine izgubljeni su podaci „JournalSpace" platforme za pohranu blogova. Do gubitka podataka je došlo kada je prepisan sadržaj diska na kojem je smještena cijela baza podataka. Problem je bio u tome što sustav za izradu sigurnosnih kopija nije radio. Poslužitelj je bio postavljen sa zrcalnim RAID sustavom. U slučaju rušenja diska sekundarni disk bi trebao obnoviti primarni, što je dosta rizično jer štiti samo od rušenja jednog diska. Kada se dogodi brisanje/prepisivanje podataka na jednom disku, ista situacija provodi se i na drugom. Upravo to je pogodilo „JournalSpace" sustav, a tim stručnjaka nije uspio povratiti izgubljene podatke.

6. Mjere zaštite

Postoje mnogi načini zaštite od gubitka podataka kao što su: izrada sigurnosnih kopija, slika diska, uporaba datotečnih sustava s dnevnicima ili RAID sustava i sl. Neke od metoda zaštite opisane su u nastavku dokumenta.

6.1. Sigurnosne kopije

Izrada sigurnosnih kopija (eng. backup) označava stvaranje kopije podataka koju je moguće iskoristiti za obnovu izvornih podataka nakon nekog od događaja koji uzrokuju njihov gubitak.

Osnovna namjena sigurnosnih kopija je:

- obnova sustava nakon pogrešaka i
- obnova datoteka nakon što su slučajno obrisane ili ugrožene.

Mediji koji se mogu iskoristiti za pohranu sigurnosnih kopija podataka su:

- Magnetske trake – dugo su bile osnovni medij za pohranu kopija
- Tvrdi disk – kapacitet je uveliko povećan tijekom povijesti pa tako i popularnost
- Optički disk – CD ili DVD tehnologije dosta su jeftine pa su zato i često u upotrebi
- Diskete - korištene tijekom 80-ih i 90-ih godina
- Čvrsti mediji za pohranu (eng. Solid state storage) – USB tehnologije, SmartMedia, Memory Stick, Secure Digital kartice i sl. - obično su skupi, ali jednostavni za uporabu.
- Udaljene sigurnosne kopije – stvaranje kopija putem Internet mreže na udaljena računala postaje sve popularnije razvojem širokopojasnog Internet pristupa.

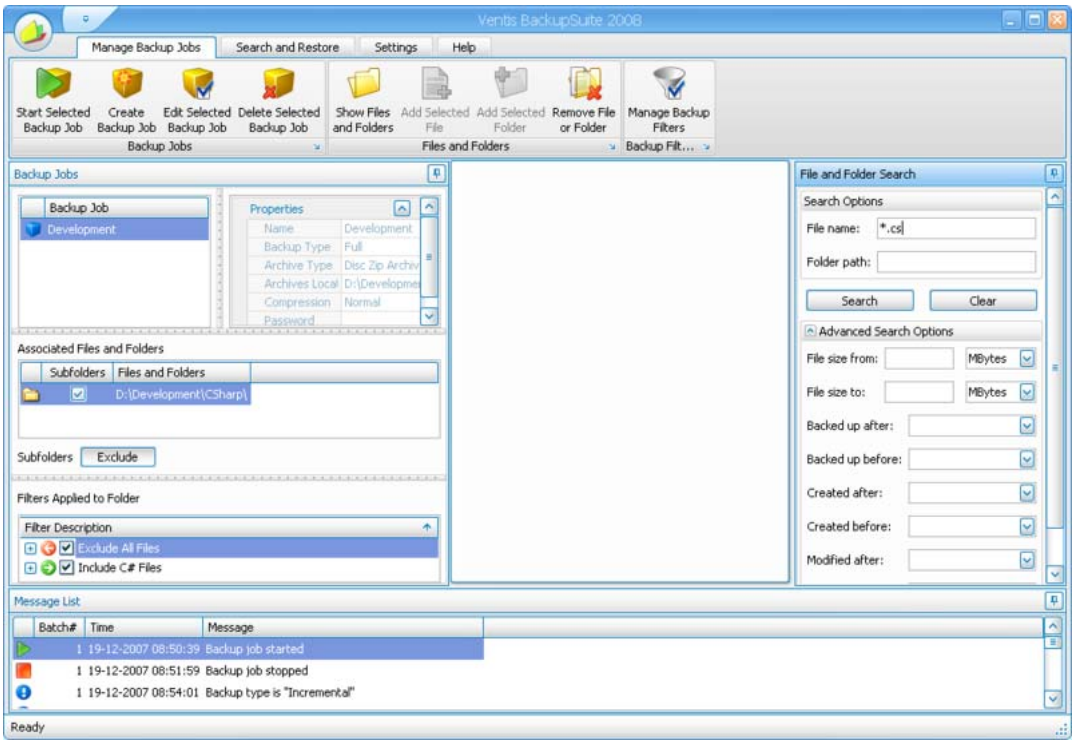
Postoje i razni programski alati specijalizirani za izradu sigurnosnih kopija. Neki od popularnijih su::

- Besplatni alati:
  - "Areca Backup" – program otvorenog koda razvijen u programskom jeziku Java i licenciran GPL (eng. General Public License) licencom. Dostupan je za „Linux", „Windows" 2000 / „Windows" XP i „Windows Vista" operacijske sustave, a zahtjeva posjedovanje „JRE" (eng. Java Runtime Environment) okruženja.
  - „FlyBack" – uslužni program razvijen u programskom jeziku Python i izdan pod GPL (eng. General Public License)licencom. Razvio ga je Derek Anderson, a namijenjen je operacijskim sustavima „Linux/Unix".
  - „ZRM" (eng. Zmanda Recovery Manager) – program namijenjen stvaranju sigurnosnih kopija „MySQL" baze podataka. Razvijen je u programskom jeziku Perl te licenciran GPL (eng. General Public License) licencom.
- Komercijalni alati:
  - „GRBackPro" – program za izradu sigurnosnih kopija namijenjen operacijskom sustavu „Microsoft Windows".
  - „EMC Legato NetWorker" – program namijenjen „Linux", „Windows", „Macintosh", „NetWare", „OpenVMS" i „Unix" okruženjima.
  - „Ventis BackupSuite 2008" – alat namijenjen „Windows XP" i „Windows Vista" platformama, a omogućuje stvaranje kopija na tvrdim diskovima, USB uređajima, lokalnim direktorijima, CD/DVD uređajima i dr. Sučelje programskog alata prikazuje slika 14.

Popis ostalih popularnih alata moguće je pronaći na sljedećoj poveznici:

http://en.wikipedia.org/wiki/List_of_backup_software

Osim toga, korisnici mogu napraviti vlastiti program ili skriptu koji će koristeći naredbe operacijskog sustava kopirati podatke i tako raditi njihovu kopiju. Ovakav pristup se sve češće koristi na poslužiteljima unutar interne infrastrukture firme.



Slika 14. **„**Ventis BackupSuite 2008“ programski alat

6.2. Izrada slike diska

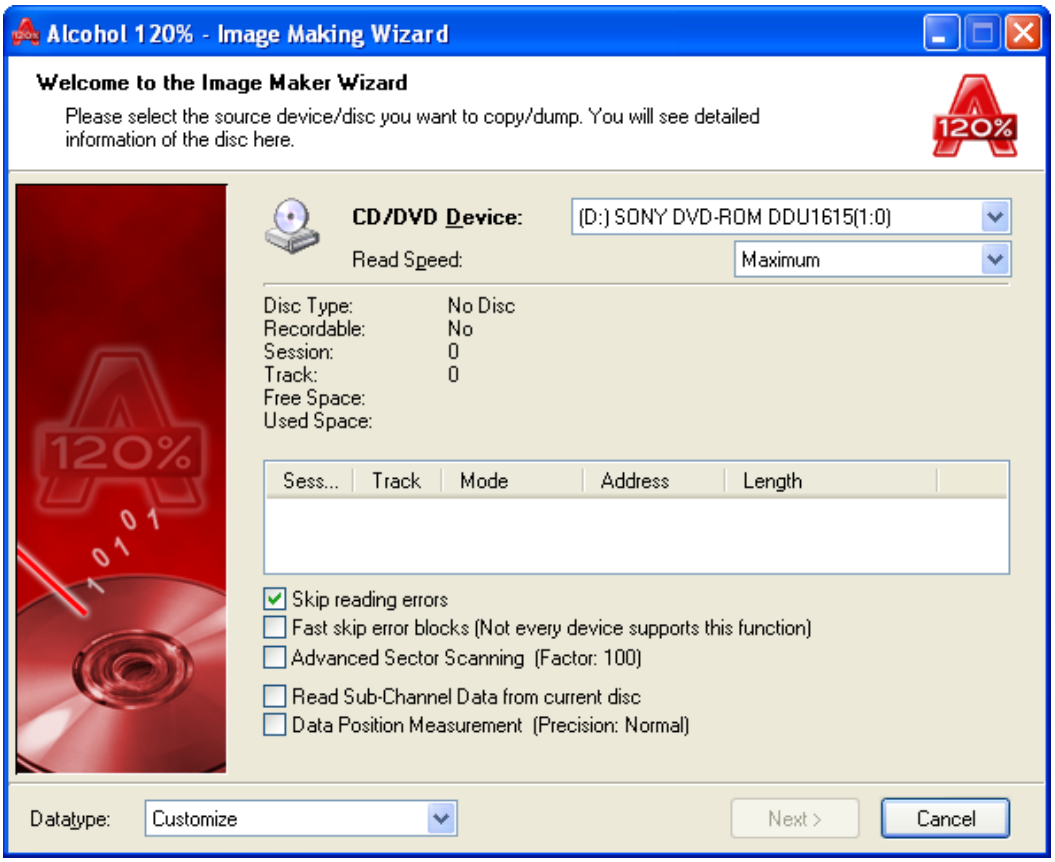
Slika diska predstavlja jednu datoteku ili uređaj za pohranu koji sadrži cjelokupni sadržaj i strukturu podataka nekog uređaja za pohranu. To mogu biti tvrdi diskovi, diskete, CD ili DVD mediji. Obično se stvara kopiranjem „sektor po sektor“ izvornog medija pa zbog toga savršeno predstavlja njegovu strukturu.

Originalno se tehnika koristila za stvaranje sigurnosnih kopija i kopija diskova. Prilikom stvaranja slike tvrdog diska postoje tri osnovna područja fokusa:

- Forenzičko stvaranje slika – cijeli sadržaj diska se preslikava u datoteku i dodaje se vrijednost za provjeru integriteta.
- Kopiranje – obično se koristi za stvaranje kopija sadržaja diska za uporabu na drugom sustavu
- Stvaranje slike za obnovu podataka – preslikavanje svakog sektora izvornog diska na drugi medij s kojeg podaci mogu biti obnovljeni.

Nekoliko programskih alata koji služe za stvaranje slike:

- tvrdog diska:
  - „EnCase“ – omogućuje kvalitetno forenzičko kopiranje podataka spremljenih na osobno računalo. Mrežne inačice mogu stvarati tzv. „snapshots“ uzorke RAM memorije ciljanog računala.
  - „Portlock SMART“ (eng. System Management and Recovery Toolkit) – alat namijenjen operacijskom sustavu „Microsoft Windows“.
  - „ntfsclone“ – alat za efektivno obnavljanje ili kopiranje „NTFS“ datotečnog sustava u datoteke, uređaje za pohranu i sl.
- optičkog diska:
  - „Alcohol 120%“ - program za kopiranje sadržaja CD/DVD uređaja namijenjen operacijskom sustavu „Microsoft Windows“. Sučelje navedenog programa prikazuje slika 15.
  - „PowerISO“ – programski alat za stvaranje slika CD i DVD uređaja za operacijske sustave „Microsoft Windows“, „Mac OS X“ i „Linux“.



Slika 15. Sučelje alata „Alcohol 120%“

Popis ostalih alata koji se mogu iskoristiti za stvaranje slike diska moguće je pronaći preko poveznice:

http://en.wikipedia.org/wiki/List_of_disk_imaging_software

6.3. Datotečni sustavi s dnevnikom

Datotečni sustavi s dnevnikom bilježe promjene u dnevniku prije izvršavanja istih na glavnom datotečnom sustavu. Takvi sustavi imaju manju vjerojatnost ugrožavanja u slučaju pogreške ili rušenja sustava.

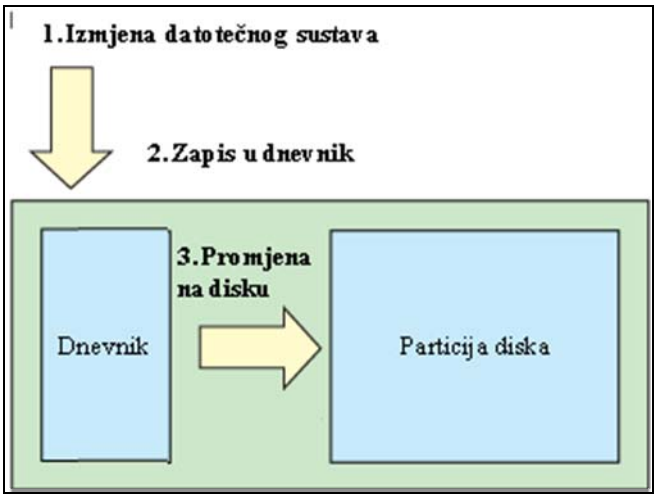
Obnavljanje datoteka sustava kako bi prikazivale promjene datoteka i direktorija obično zahtijevaju mnogo odvojenih operacija pisanja što lako može dovesti do nepravilnog stanja. Na primjer, brisanje datoteka na operacijskom sustavu „Unix“ uključuje:

- uklanjanje zapisa direktorija i
- označavanje mjesta datoteke kao slobodnog.

Ako se dogodi rušenje između navedenih koraka, dolazi do gubitka pohrane (eng. storage leak). Ako se prije rušenja izvede samo druga radnja, datoteka koja nije obrisana označena je kao da jest pa dolazi do mogućnosti prepisivanja podataka.

U datotečnim sustavima koji ne sadrže dnevnike, otkrivanje i oporavak od takvih nekonzistentnosti zahtjeva prolazak kroz podatkovnu strukturu. Takav postupak može trajati jako dugo ukoliko se radi o velikim sustavima.

U datotečnom sustavu s dnevnikom promjene se bilježe u dnevnik. Nakon rušenja, obnova se provodi izvođenjem promjena koje su zapisane dok se sustav ne dovede u konzistentno stanje. Rad datotečnog sustava koji sadrži dnevnik nalazi se na slici 16.



Slika 16. Datotečni sustav s dnevnikom

Primjeri ovakvog sustava su:

- „JFS“ (eng. Journaled File System) - stvarala ga je organizacija IBM (eng. International Business Machines Corporation). Dostupan je pod GNU GPL (eng. General Public License) licencom za operacijske sustave „AIX“, „eComStation“, „OS/2“ i „Linux“.
- „XFS“ – stvarala ga je organizacija Silicon Graphics za „IRIX“, a kasnije i „Linux“ te „FreeBSD“ operacijske sustave.
- „NTFS“ (Windows NT File System) – datotečni sustav namijenjen operacijskom sustavu „Windows NT“, ali uključuje podršku i za stare inačice - „Windows 2000“ te novije: „Windows XP“, „Windows Server 2003“, „Windows Server 2008“, „Windows Vista“ i „Windows 7“.
- „ext3“ (eng. third extended filesystem) – datotečni sustav namijenjen „Linux“ distribucijama.

6.4. RAID tehnologija

RAID (eng. Redundant Array of Inexpensive Disks ili Redundant Array of Independent Disks) tehnologija omogućuje korisnicima računala arhiviranje pohranjenih podataka s komponenti tvrdog diska putem tehnika uređivanja u nizove za redundanciju. Danas se izraz RAID koristi za spremište podataka koje može podijeliti i umnožiti podatke na više tvrdih diskova. Osnovni cilj tehnologije je:

- povećanje sigurnosti podataka i
- povećanje ulazno/izlaznih performansi.

Kada se više diskova postavi u RAID tehnologiju, oni se nalaze u RAID listi koja distribuira podatke preko više diskova, a korisnicima se prikazuje kao jedinstven disk.

Redundancija je ostvarena:

- pisanjem istih podataka na više uređaja ili
- pisanjem dodatnih podataka preko liste na način da pogreška u jednom disku ne utječe na druge.

Organiziranjem diskova u redundantne liste smanjuje se raspoloživi kapacitet za pohranu. Postoje različite inačice kombinacije uređenja liste koje pružaju drugačiju razinu zaštite od gubitka podataka, kapacitet i brzinu.

Tri ključna koncepta u RAID tehnologiji su:

- zrcaljene (eng. mirroring) – kopiranje podataka na više od jednog diska,
- podjela (eng. striping) – podjela podataka preko više od jednog diska i

- ispravljanje pogrešaka (eng. error correction) – kada su pohranjeni redundantni podaci, kako bi se omogućilo otkrivanje i ispravljanje pogrešaka.

Postoje mnogobrojne primjene opisane tehnologije temeljene na operacijskom sustavu pa se pojavljuju kod operacijskih sustava „Mac OS X Server“, „FreeBSD“, „MidnightBSD“, „Linux“, „Microsoft Windows“, „NetBSD“, „OpenBSD“, „OpenSolaris“ i „Solaris 10“.

7. Zaključak

Korisnici osobnih računala, Internet usluga, kao i razne organizacije, firme i ustanove svakodnevno pohranjuju povjerljive podatke na tvrdi disk računala. Oštećivanjem neke komponente računala, bilo fizički ili logičkom pogreškom, nastupa gubitak pohranjenih informacija. Često su takve informacije ključne za poslovanje i rad organizacija te njihov gubitak povlači i novčane gubitke, kao i pad produktivnosti, kredibiliteta i sl. Tehnikama oporavka moguće je obnoviti podatke koji nisu u potpunosti uništeni, ali takvi postupci obično zahtijevaju dodatne znanja i vještine.

Danas su razvijeni brojni alati u koje su ugrađene neke od tehnologije obnove podataka. Takvi programski alati omogućuju jednostavnu obnovu podataka, izradu sigurnosnih kopija, provjeru konzistentnosti sustava i dr. Budući da neke podatke nije moguće obnoviti ni uporabom spomenutih alata, kako bi se osigurala pouzdanost i dostupnost pohranjenih podataka, potrebno je uvesti mjere zaštite. Postoji više načina osiguravanja sustava u slučaju gubitka podataka, a jedan od osnovnih je izrada sigurnosnih kopija. Takva praksa omogućuje jednostavnu zamjenu ugroženih podataka te nastavak rada bez prekida. Ostale metode oslanjaju se na rješenja poput bilježenja događaja radi njihovog ispravka u slučaju pogreške, stvaranju slike uređaja za pohranu sa svim podacima i sl.

Budući da statistički podaci pokazuju rast novčanih troškova uzrokovanih gubitkom podataka radi neke vrste oštećenja, potrebno je uključiti opisane mjere zaštite u sustav. Također, daljnjim razvojem tehnologije očekuje se poboljšanje tehnologija i alata za obnovu podataka.

8. Reference

[1] Obnavljanje podataka, http://en.wikipedia.org/wiki/Data_recovery, travanj, 2009.

[2] Gubitak podataka, http://en.wikipedia.org/wiki/Data_loss, travanj, 2009.

[3] Gubitak podataka, http://en.wikipedia.org/wiki/Data_erasure, travanj, 2009.

[4] Daniel Dickerman: Advanced data carving, http://sandbox.dfrws.org/2006/dickerman/Dickerman%20DFRWS%202006%20Challenge%20Final%20Submission.pdf, srpanj 2006.

[5] Knoppix, http://en.wikipedia.org/wiki/Knoppix, travanj, 2009.

[6] Ubuntu Rescue Remix, http://ubuntu-rescue-remix.org/, travanj, 2009.

[7] SystemRescueCD, http://en.wikipedia.org/wiki/SystemRescueCD, travanj, 2009.

[8] Selkie Rescue Data Recovery, http://selkie-rescue-data-recovery.en.softonic.com/, travanj, 2009.

[9] CHKDSK, http://en.wikipedia.org/wiki/CHKDSK, travanj, 2009.

[10] Disk First Aid, http://en.wikipedia.org/wiki/Disk_First_Aid, travanj, 2009.

[11] Disk Utility, http://en.wikipedia.org/wiki/Disk_Utility, travanj, 2009.

[12] fsck, http://en.wikipedia.org/wiki/Fsck, travanj, 2009.

[13] PhotoRec, http://en.wikipedia.org/wiki/PhotoRec, travanj, 2009.

[14] SanDisk RescuePRO, http://en.wikipedia.org/wiki/SanDisk_RescuePRO, travanj, 2009.

[15] The Coroner's Toolkit, http://en.wikipedia.org/wiki/The_Coroner%27s_Toolkit, travanj, 2009.

[16] The Sleuth Kit, http://en.wikipedia.org/wiki/The_Sleuth_Kit, travanj, 2009.

[17] EnCase, http://en.wikipedia.org/wiki/EnCase, travanj, 2009.

[18] ddrescue, http://en.wikipedia.org/wiki/Ddrescue#Recovery-oriented_variants_of_dd, travanj, 2009.

[19] Statistički podaci, http://www.bostoncomputing.net/consultation/databackup/statistics/, travanj, 2009.

[20] The Cost of Lost Data, http://gbr.pepperdine.edu/033/dataloss.html, travanj, 2009.

[21] Home Office loses data on 84,000 prisoners, http://www.silicon.com/publicsector/0,3800010403,39274254,00.htm, kolovoz, 2008.

[22] JournalSpace Drama: All Data Lost Without Backup, Company Deadpooled, http://www.techcrunch.com/2009/01/03/journalspace-drama-all-data-lost-without-backup-company-deadpooled/, siječanj, 2009.

[23] Sigurnosne kopije, http://en.wikipedia.org/wiki/Backup, travanj, 2009.

[24] Andrei Shirobokov: Disk Imaging: A Vital Step in Data Recovery, http://www.deepspar.com/pdf/DeepSparDiskImagingWhitepaper3.pdf, 2006.

[25] Journaling file system, http://en.wikipedia.org/wiki/Journaling_filesystem, travanj, 2009.

[26] RAID, http://en.wikipedia.org/wiki/Redundant_array_of_independent_disks, travanj, 2009.