Centar Informacijske Sigurnosti

Sigurno uklanjanje datoteka

CIS-DOC-2011-05-013

Upozorenje

Podaci, informacije, tvrdnje i stavovi navedeni u ovom dokumentu nastali su dobrom namjerom i dobrom voljom te profesionalnim radom CIS-ovih stručnjaka, a temelje se na njihovom znanju i petnaestak godina iskustva u radu u informacijskoj sigurnosti. Namjera je da budu točni, precizni, aktualni, potpuni i nepristrani.

Ipak, oni su dani samo kao izvor informacija i CIS ne snosi nikakvu izravnu ili posrednu odgovornost za bilo kakve posljedice nastale korištenjem podataka iz ovog dokumenta.

Ukoliko primijetite bilo kakve netočnosti, krive podatke ili pogreške u ovom dokumentu, ili imate potrebu komentirati sadržaj molimo Vas da to javite elektroničkom poštom na adresu info@CIS.hr.

O CIS-u

CIS izrađuje pregledne dokumente (eng. white paper) na teme iz područja informacijske sigurnosti koji će biti korisni zainteresiranoj javnosti, a u svrhu **podizanje njezine svijesti o informacijskoj sigurnosti** i **sposobnosti za čuvanje i zaštitu informacija i informacijskih sustava**. Pored toga, CIS razvija i održava mrežni portal www.CIS.hr kao referalnu točku za informacijsku sigurnost za cjelokupnu javnost; izrađuje obrazovne materijale namijenjene javnosti; organizira događaje za podizanje svijesti o informacijskoj sigurnosti u javnosti i pojedinim skupinama te djeluje u suradnji sa svim medijima.

CIS **okuplja mlade** zainteresirane za informacijsku sigurnost i radi na njihovom pravilnom odgoju i obrazovanju u području informacijske sigurnosti te pripremu za **profesionalno bavljenje informacijskom sigurnošću**.

Centar informacijske sigurnosti [CIS] nastao je 2010. godine na poticaj Laboratorija za sustave i signale[LSS] Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu, a kao posljedica 15togodišnjeg rada na istraživanju, razvoju i primjeni informacijske sigurnosti. LSS je među ostalim potaknuo osnivanje CARNetovog CERTa i sudjelovao u izradi Nacionalnog programa informacijske sigurnosti RH.

Smisao CISa je da bude **referentno mjesto za informacijsku sigurnost** za javnost, informatičare i posebno za mlade te da sustavno podiže njihovu svijest i sposobnosti u području informacijske sigurnosti.

Rad CISa podržava Ministarstvo znanosti, obrazovanja i sporta Republike Hrvatske, a omogućuju sponzori.

Prava korištenja

Sadržaj

1. Uvod

Kako vrijeme prolazi, ljudi su sve više upoznati s osnovama rada na računalu. Uz silne forenzičke serije, mnogi su već naučili i više od samih osnova, između ostalog da podaci ostaju na disku računala čak i kad korisnik misli da više nisu tamo.

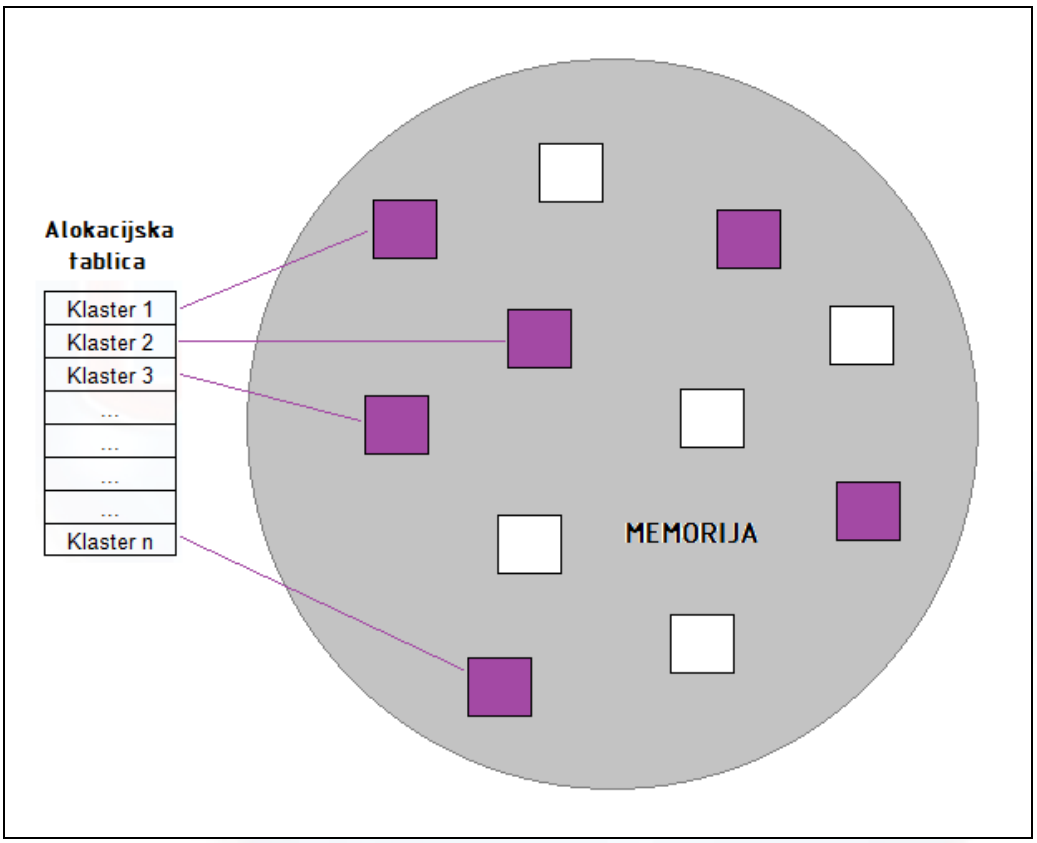
Ovo je možda najbitnija tema za vladine organizacije, velike korporacije kao i za sve ostale koji bi mogli izgubiti mnogo toga (financije, ugled i sl.) ako bi njihove tajne izašle u javnost. Stoga je potreban oprez.

Postoje razni komercijalni i besplatni alati koji omogućavaju korisniku da jednostavnim podešavanjem opcija i klikom na gumb „očiste“ svoje računalo od davno izbrisanih, ali nikad nestalih podataka.

Ovaj dokument će objasniti gdje se sve mogu „skrivati“ podaci, a da to korisnik ne očekuje, koje su to datoteke koje računalo samo stvara i pohranjuje, a koje sadrže ogromne količine podataka o korisnikovim akcijama na računalu te će se spomenuti najčešće korištene metode u sigurnom uklanjanju datoteka kao i alati koji te metode koriste.

2. Organizacija datotečnih sustava

Način na koji računalo pohranjuje podatke ovisi o datotečnom sustavu (eng. *filesystem*) diska za pohranu. Svaki datotečni sustav ima svoj tip organizacije podataka u alokacijske tablice koje operacijskom sustavu služe kao upute kako doći do određene datoteke. Tablica 1 prikazuje alokacijske tablice[1] pojedinih operacijskih sustava. Npr. FAT alokacijska tablica sadrži popis svih klastera te uz njih pohranjuje podatak o tome da li je klaster slobodan ili dodijeljen i slične informacije (Slika 1).



Slika 1. *Pojednostavljeni prikaz funkcije alokacijskih tablica*

Alokacijska tablica	Operacijski sustav	Datotečni sustav
FAT (eng. *File Allocation Table*)	Windows Me, 98, 95 i stariji	FAT12, FAT16, FAT32, VFAT, exFAT
MFT (eng. *Master File Table*)	Windows NT, XP, Server 2003, Vista, Server 2008, 7	NTFS (eng. *New Technology File System*)
HFS (eng. *Hierarchical File System*)	Mac OS	HFS, HFS+
Superblok (eng. *Superblock*)	Linux	ext2/ext3/ext4, mnogi drugi

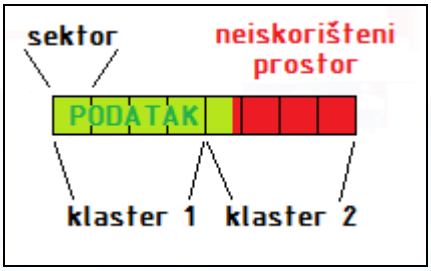
Tablica 1. *Nazivi alokacijskih tablica različitih operacijskih sustava*

[1] Alokacijska tablica se nalazi na disku na kojem je operacijski sustav, a sadrži lokacije svih klastera u kojima su pohranjeni pojedini podaci.

2.1. Pohranjivanje podataka na disku

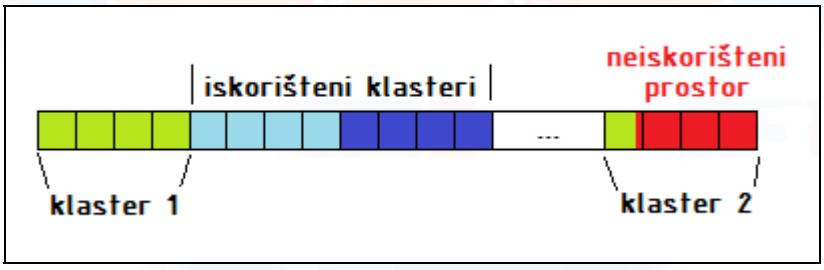
Da bi se shvatila organizacija podataka, prvo se mora shvatiti kako računalo pohranjuje podatke.

- Najmanja jedinica za pohranu podataka je **sektor**, veličine 512 okteta[2]. U slučaju operacijskog sustava Linux, ova jedinica se zove **blok**. Ako je neki podatak veličine 800 okteta, zauzeti će dva sektora/bloka od 512 okteta.
- **Klaster** (eng. *cluster*) sadržava jedan ili više uzastopnih sektora. Broj sektora u klasteru je uvijek potencija broja 2 (npr. 2^0=1,..., 2^{*3}=8, 2^4=16, ...). Broj sektora u klasteru ovisi o karakteristikama računala (Tablica 2). Kad se podatak pohranjuje, uvijek će mu se dodijeliti cijeli broj klastera makar podatak bio manji od ukupne veličine dodijeljenog prostora. Ako bi podatak zauzimao 5 sektora, uz klastere veličine 4 sektora, dodijelila bi mu se 2 klastera (Slika 2). Prostor u drugom klasteru koji je u tom slučaju ostao prazan se zove neiskorišteni prostor (eng. *slack space*).



Slika 2. *Pohranjivanje podatka u klastere*

- Podatak se uvijek nastoji pohraniti u uzastopnim klasterima. Ako susjedni klasteri nisu slobodni, traže se oni koji jesu. Tako pohranjen podatak je **fragmentiran** (Slika 3). Pritom gotovo uvijek dolazi do pojave neiskorištenog prostora. Iako su na disku pohranjene npr. 2 datoteke veličine 5 sektora (uz klastere veličine 4), zauzeće diska neće biti očekivanih 10 sektora već 16 sektora (4 klastera) jer će svaka datoteka zauzeti 2 cijela klastera.



Slika 3. *Fragmentirani podatak (zelena boja označava podatak koji se pohranjuje)*

[2] Veličina sektora se može promijeniti određenim programima za formatiranje i rad s particijama.

Veličina diska	FAT32	exFAT	NTFS
7 MB – 32 MB	Nije podržano	4 KB	4 KB
32 MB – 64 MB	512 B	4 KB	4 KB
64 MB – 128 MB	1 KB	4 KB	4 KB
128 MB – 256 MB	2 KB	4 KB	4 KB
256 MB – 8 GB	4 KB	32 KB	4 KB
8 GB – 16 GB	8 KB	32 KB	4 KB
16 GB – 32 GB	16 KB	32 KB	4 KB
32 GB – 16 TB	Nije podržano	128 KB	4 KB
16 TB – 32 TB	Nije podržano	128 KB	8 KB
32 TB – 64 TB	Nije podržano	128 KB	16 KB
64 TB – 128 TB	Nije podržano	128 KB	32 KB
128 TB – 256 TB	Nije podržano	128 KB	64 KB
> 256 TB	Nije podržano	Nije podržano	Nije podržano

Tablica 2. *Veličina klastera za pojedine datotečne sustave za inačice Windows 2000, XP, Server 2003, Vista, Server 2008*
Izvor: *Microsoft Help and Support*

2.2. Brisanje podataka s diska

Iako je u posljednje vrijeme postalo opće poznato da izbrisani podatak zapravo nije izbrisan. Kad se stvori datoteka, podaci o datoteci se zapisuju u alokacijsku tablicu (Tablica 1). Prilikom brisanja datoteke:

- prvo slovo u nazivu datoteke se mijenja u 'E5' (Windows),
- briše se zapis iz alokacijske tablice čime se sustavu daje do znanja da se lokacija obrisane datoteke može dodijeliti novoj datoteci,
- podaci ostaju fizički zapisani na disku sve dok se preko njih ne zapišu novi podaci.

Upravo zbog činjenice da se izbrisani podaci fizički ne uklanjaju s diska „sami od sebe“ valja biti izuzetno oprezan prilikom iznošenja diskova iz poslovnih prostora, poklanjanja rabljenih računala i sličnih situacija gdje drugi ljudi dolaze u dodir s potencijalno osjetljivim podacima.

Izbrisani podaci, podaci iz neiskorištenog i nealociranog prostora, kao i razne datoteke koje sustav kreira neovisno o znanju korisnika, mogu se pregledavati, ali i uništiti raznim alatima o kojima će biti riječ u poglavlju 5.

3. Skrivene datoteke

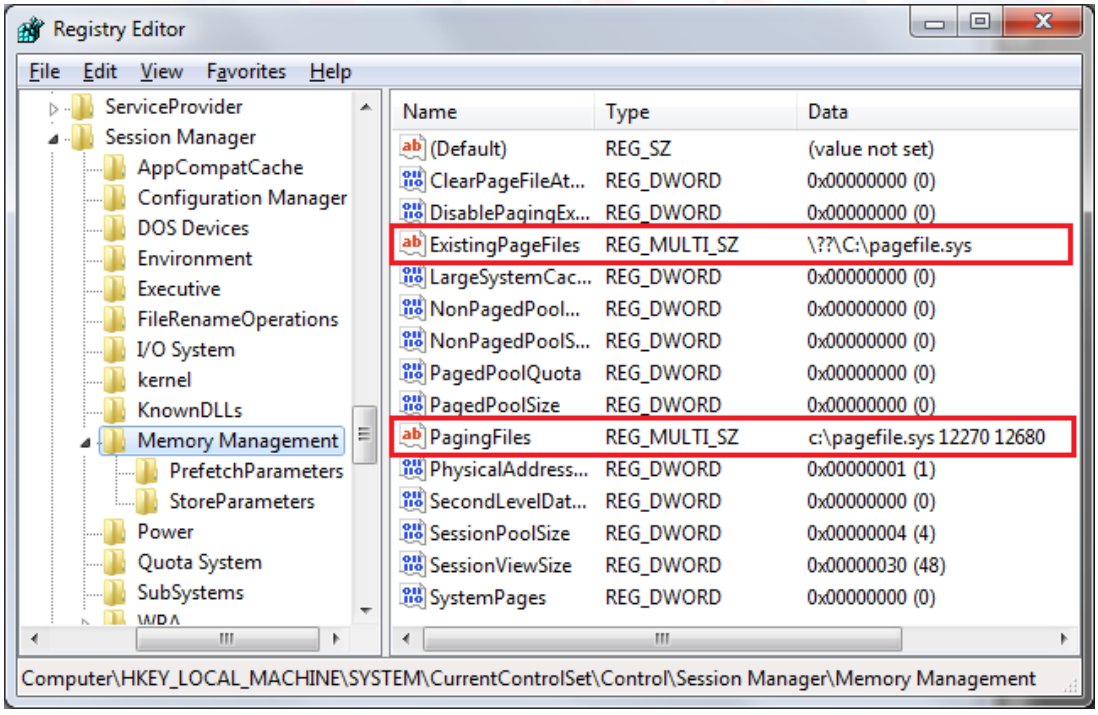
Operacijski sustav ponekad sam stvara datoteke, a da ih korisnik nije svjestan. Riječ je o datotekama kojima je svrha ubrzati rad računala ili osigurati pohranjivanje podataka u slučaju neočekivanih pogrešaka (gubitak struje, „pad“ sustava i sl.). U Linuxu [2] je jednostavno i vidjeti i pregledavati skrivene datoteke:pregled svih datoteka se postiže naredbama:

- '$ ls –a',
- ispis sadržaja datoteke se postiže naredbom '$ cat <ime_datoteke>'.

Datoteke u Windows operacijskom sustavu su manje očite i često ih korisnik ne može pregledati običnim tekstualnim uređivačima. Stoga će se u nastavku dokumenta dati pregled skrivenih datoteka Windows operacijskog sustava.

3.1. Swap i page datoteke

Kad operacijski sustav Windows treba više radne memorije od fizički raspoložive (RAM memorije računala), odredi dio prostora na disku kojeg onda koristi kao radnu memoriju (što se označava pojmom „virtualna memorija“) U slučaju inačica Windows 95 i Windows 98, taj prostor se zove ***Swap*** datoteka, a u slučaju inačica Windows NT, 2000 i XP ***Page*** datoteka (obje datoteke imaju istu funkciju, samo se drugačije zovu). S obzirom da se *Page* datoteka zapisuje na tvrdi disk, podaci iz Windows sjednice ostaju zapisani na disku kao i sve korisničke datoteke. Iz toga se mogu vidjeti detalji o dokumentima koje je korisnik uređivao, posjećene web stranice i slično. Ono zbog čega je *Page* datoteka potencijalno opasno mjesto curenja informacija je činjenica da se pri svakom uključivanju računala stvara nova *Page* datoteka što znači da se na računalu mogu naći datoteke s podacima o prethodnim sjednicama.



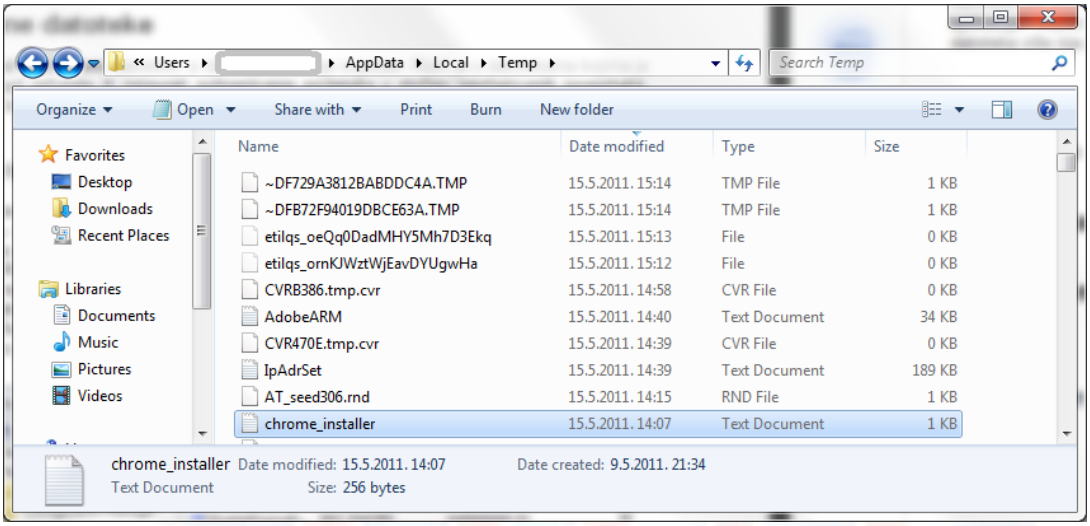
Slika 4. *Prikaz zapisa o Page datotekci unutar registara (Windows 7)*

3.2. Privremene datoteke

Kako bi se povećale performanse i efikasnost, mnoge aplikacije stvaraju **privremene datoteke** (eng. *temporary files*). Microsoft na svojim stranicama za podršku opisuje privremene datoteke [4] na sljedeći način:

> *„Privremena datoteka je datoteka koja je stvorena da privremeno pohrani podatke kako bi se oslobodila memorija za druge svrhe ili da bi poslužila kao sigurnosna rezerva protiv gubitka podataka dok aplikacija obavlja određene funkcije. Npr. Word[3] automatski određuje gdje i kada je potrebno stvoriti privremene datoteke. One postoje samo za vrijeme trajanja sjednice u Wordu. Kad se Word ugasi na predviđen način, sve privremene datoteke se prvo zatvaraju, a potom brišu."*

Kao što je spomenuto, privremene datoteke se brišu prilikom gašenja aplikacije, ali podaci iz tih datoteka se još uvijek mogu pronaći na disku jer se, kako je već objašnjeno, niti jedna datoteka u stvarnosti ne briše. Važno je zapamtiti da se podaci iz njih mogu pronaći na disku čak i kad originalna datoteka više nije pohranjena na računalu.



Slika 5. *Lokacija privremenih datoteka (Windows 7)*

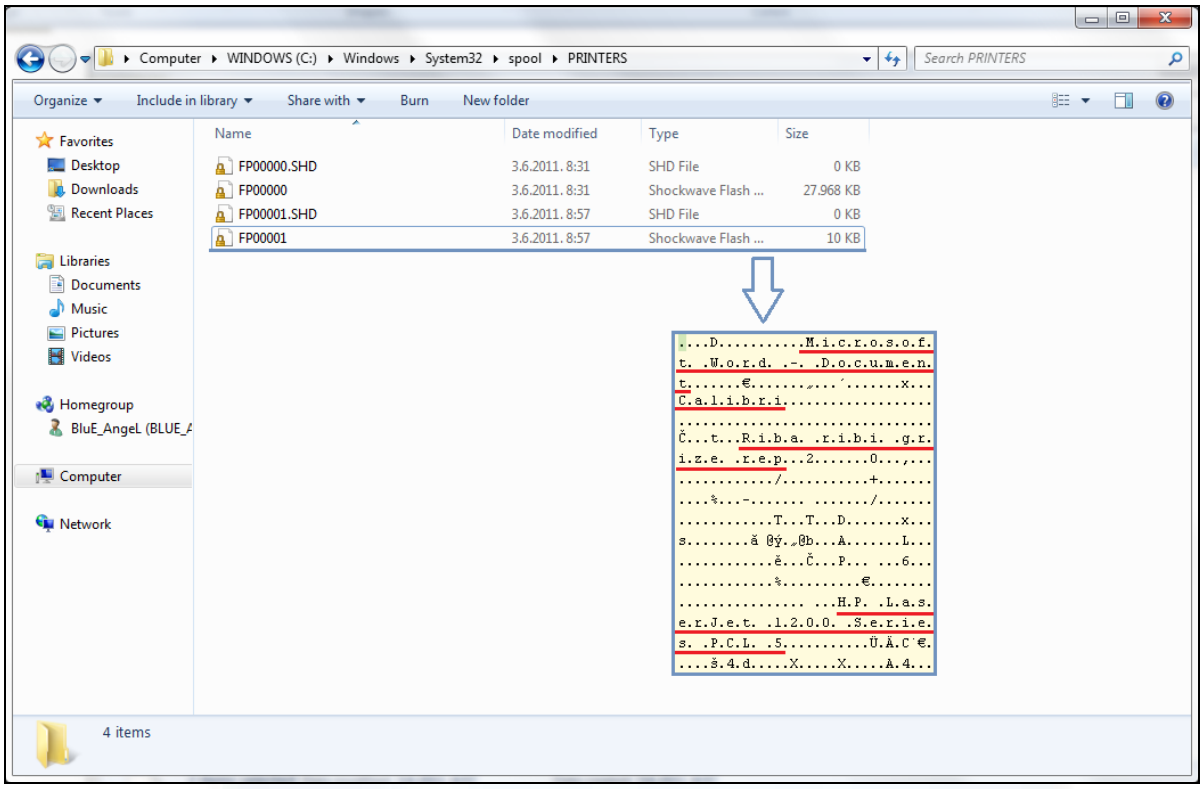
3.3. Red čekanja datoteka za ispis na pisaču

Standardna postavka u operacijskom sustavu MS Windows za pisače je da se datoteke privremeno pohranjuju u tzv. ***spool*** za brže ispisivanje. *Spool* (eng. *simultaneous peripheral operations online*), odnosno red čekanja, radi na taj način da računalo prvo pošalje datoteku na disk, a onda pisaču. Na taj način se procesor može baviti drugim poslovima sve dok pisač nije spreman za printanje. S obzirom da je datoteka prvo zapisana na disk, ona ostaje zapisana na njemu sve dok drugi podaci ne budu zapisani preko nje. Na taj način se ispisivani dokumenti mogu rekonstruirati pomoću forenzičkih alata koji mogu pregledavati napredne metadatoteke.

Slika 6 prikazuje lokaciju privremene pohrane datoteka u redu čekanja za ispis zajedno s djelomičnim pregledom jedne od datoteka s popisa[4]. Ono što se može uočiti jest da se u pregledu vidi aplikacija u kojoj je dokument napravljen („Microsoft Word"), ime dokumenta („Document"), font kojim je pisan tekst („Calibri"), čak i tekst („Riba ribi grize rep") te na kraju korišteni pisač („HP LaserJet 1200 Sereic PCL").

[3] Microsoft Word, op.a., tekstualni uređivač.

[4] Datoteka je otvorena heksadecimalnim uređivačem [24].



Slika 6. *Lokacija privremene pohrane datoteka u redu čekanja za ispis (Windows 7)*

3.4. Metapodaci

Metapodatke je najlakše opisati kao podatke o podacima. Iako sami metapodaci ne čine zasebnu datoteku, stvaraju se automatski npr. prilikom stvaranja MS Office datoteka (Word, Excell, Powerpoint itd.). Kad se shvati koliko informacija je sadržano u metapodacima, vidjeti će se i zašto te da li je uopće bitno ukloniti ih. Iz perspektive organizacije, metapodaci mogu sadržavati podatke koji ne bi trebali biti poznati izvan granica organizacije. Iz perspektive korisnika koji samo radi popis filmova koje želi pogledati, brisanje metapodataka bi predstavljalo gubitak vremena. Primjeri metapodataka MS Office dokumenta su:

- ime autora,
- inicijali autora,
- ime tvrtke ili organizacije,
- ime računala,
- ime mrežnog poslužitelja ili tvrdog diska na kojem je dokument pohranjen,
- imena prethodnih autora datoteke,
- revizije dokumenta,
- inačice dokumenta,
- skriveni tekst[5],
- komentari i dr.

Metapodaci su se pokazali toliko važnima da je Microsoft napravio dodatak za Office paket - *Remove Hidden Data Add-In for Office 2003/XP*, koji je besplatan za preuzimanje i koristi se za brisanje metapodataka iz dokumenata [5].

2005. godine je na američkom sudu završila tvrtka optužena da je otpuštala zaposlenike na temelju starosti. Sud je naredio da se dostave dokumenti koji su mogli imati utjecaja na presudu, ali je tvrtka prije dostavljanja upotrijebila alat za brisanje metapodataka. S obzirom da nije bilo

[5] Skriveni tekst je najčešće običan tekst kojemu je boja ista kao i boja pozadine.

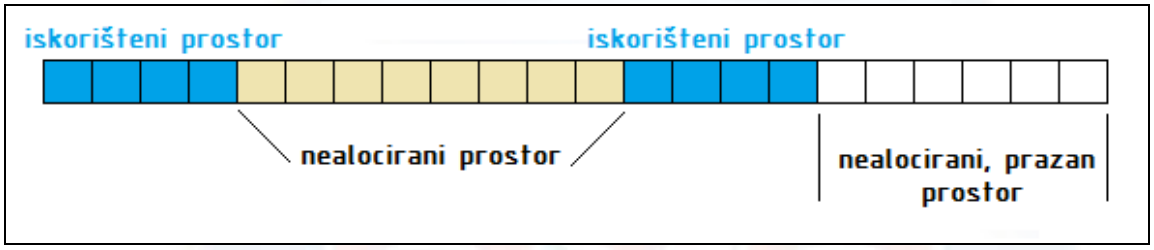
precizirano da se traže i metapodaci, tvrtka je prošla nekažnjeno, no ovaj slučaj je izazvao promjene u zakonu o elektronski pohranjenim podacima [6].

3.5. Podaci u „međuprostoru“

Osim navedenih podataka, korisno je navesti još 2 mjesta na kojima se mogu naći „zagubljeni“ podaci. Riječ je ranije spomenutom neiskorištenom (eng. *slack*) te nealociranom (eng. *unallocated*) prostoru.

Neiskorišteni prostor je dio klastera koji nije popunjen podacima u slučaju kad veličina podatka nije višekratnik veličine klastera (Slika 2).

Nealocirani prostor čine dijelovi diska (klasteri) koji su slobodni za pohranjivanje novih datoteka iako je, osim u slučaju sasvim novih diskova, rijetko kad prazan. Iz nealociranog prostora se mogu rekonstruirati datoteke koje su u jednom trenutku zauzimale taj prostor, ali su otad izbrisane. Slika 7 ilustrira dio memorije u kojem se nalaze trenutno aktivni podaci (plava boja), prazan prostor u kojem nikad ništa nije bilo zapisano (u praksi je moguć slučaj tek s istinski novim, nikad korištenim diskom) te nealocirani prostor u kojem je nekad bilo zapisanih podataka, ali je sad označen kao dostupan.



Slika 7. *Nealocirani prostor*

4. Metode sigurnog uklanjanja datoteka

U prvom dijelu dokument je utvrđeno da se izbrisane datoteke mogu rekonstruirati. No je li moguće nepovratno izbrisati datoteku i sve pripadajuće skrivene datoteke? Osnovni korak u uništavanju podataka (tj. datoteka) je zapisivanje drugih, nevažnih podataka preko njih. Postoje pojedinci koji vjeruju da je jedno prepisivanje dovoljno, ali što se više puta prepiše preko podatka, to ga je teže rekonstruirati. Postoje priče o tome kako američke vladine agencije imaju mogućnost rekonstrukcije podataka koji su prepisani i do 21 put. Stoga je preporuka CIS-ovih stručnjaka da se podaci prepišu 30 puta što gotovo garantira nemogućnost rekonstrukcije.

Iz poslovne perspektive, pojedinac mora odlučiti jesu li podaci na disku dovoljno važni da opravdaju vremenski i financijski trošak koji treba biti uložen u uništavanje podataka. Za podatke od presudne važnosti za poslovanje organizacije se preporuča koristiti komercijalni umjesto besplatnog alata jer u tom slučaju ipak postoji netko tko jamči da će posao biti kvalitetno odrađen. S aspekta vremenskog troška treba biti svjestan činjenice da će računalo, ovisno o količini podataka koja se briše, određeno vrijeme biti zauzeto i neće se moći koristiti.

Slijede opisi najčešćih metode uklanjanja datoteka.

4.1. Single Pass

Podaci se prepisuju jednom s jedinicama, nulama ili pseudoslučajnim[6] podacima.

niz nula	0	0	0	0	0	0	0	0	0	0	0	0	0	0
originalni podatak	1	0	0	1	1	1	0	1	0	1	1	1	0	0	1

Slika 8. *Single Pass metoda s prepisivanjem nulama*

4.2. DoD

DoD metoda, odnosno metoda američkog Ministarstva obrane, u kojoj se podaci prepisuju 3 puta – prvo nulama, potom jedinicama i na kraju pseudonasumičnim podacima. Mnogi alati koriste ovu metodu s tim da ponavljaju prva dva koraka i do 3 puta prije prepisivanja pseudonasumičnim podacima.

pseudonasumični podaci	0	0	0	1	1	0	1	1	0	1	1	1	0	1	1
niz jedinica	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
niz nula	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
originalni podatak	1	0	0	1	1	1	0	1	0	1	1	1	0	0	1

Slika 9. *DoD metoda*

Ova metoda se temelji na priručniku Ministarstva obrane SAD-a 5220.22 M, poznat i kao NISPOM priručnik (eng. *National Industrial Security Program Operating Manual*) [7]. Priručnik sadrži korake za **čišćenje** i **dezinficiranje** ne-prijenosnog diska.

Da bi se disk **očistio**, potrebno je prepisati sve adresabilne lokacije s jednim znakom.

[6] Pseudoslučajno (eng. *pseudorandom*) znači da je poredak podataka slučajan, u ovom slučaju jedinica i nula. „Pseudo“ označava matematičku nemogućnost računala da generira podatak koji je uistinu nasumičan, s obzirom da svako generiranje radi po nekom (ponovljivom) uzorku.

Da bi se disk **dezinficirao**, potrebno je učiniti jedno od navedenog:

- demagnetizirati disk s demagnetizerom[7] tipa I (eng. *Type I Degausser*) [9],
- demagnetizirati disk s demagnetizerom tipa II (eng. *Type II Degausser*) [10],
- prepisati sve adresabilne lokacije s jednim znakom (0 ili 1), njegovim komplementom (1 ili 0) pa s nasumičnim znakovima te verificirati[8],
- uništiti – dezintegrirati, zapaliti, pretvoriti u prah, samljeti ili rastaliti disk.

4.3. NAVSO P9239-26

U NAVSO (eng. *Navy Remanence Security Guidebook*) priručniku piše da se mediji trebaju pročistiti tako da se u sve pohrambene lokacije upiše uzorak podataka, potom komplement tog uzorka, potom sa slučajnim uzorkom nakon čega će se podatak verificirati (po DoD 5200.28-M). Tom procedurom bi se magnetska polja na svakoj adresabilnoj lokaciji na disku trebala natjerati na oba polariteta. Program koji zapisuje podatke treba zapisivati u alokacijske tablice, direktorije, mape blokova, korišteni i nekorišteni prostor te u neiskorišteni prostor u klasterima. Program treba pisati kako u dobre tako i u loše (oštećene) sektore. NAVSO je u principu interpretacija DoD metode američke mornarice. Slične dokumente imaju i američka vojska i zračne snage.

4.4. PRNG

PRNG (eng. *Pseudo-random Number Generator*) je metoda generiranja niza pseudoslučajnih brojeva koji se zapisuju na ciljani disk. Pojam „pseudo“ označava matematičku nemogućnost generiranja istinski nasumičnog broja. Svaki generator mora imati broj s kojim počinje generiranje te algoritam kojim se generiraju brojevi. S obzirom na to da se svaki niz generiranih brojeva može ponoviti pod uvjetom da se krene od istog prvog broja, generator nije potpuno nasumičan.

Jedna od ranijih PRNG metoda, predložena od John von Neumanna 1946. godine, je imala korake:

1. uzeti bilo koji broj kao početni – npr. 1111,
2. kvadrirati broj – 1111^2 = 01234321 (kvadrat od 4 znamenke ima 8 znamenki),
3. uzeti srednje znamenke rezultata – 2343,
4. ponavljati korake 2 – 3.

Von Neumann je radio s deseteroznamenkastim brojevima, ali proces generiranja je isti. Iz ovog primjera se vidi da će svaki proces koji počne s istim brojem generirati isti niz.

4.5. GUTTMAN

Guttmanova metoda koristi 35 zapisivanja pseudonasumičnih brojeva na ciljani disk. Pritom se uzimaju u obzir razni kodirajući algoritmi koje koriste proizvođači sklopovlja: RLL (eng. *Run Length Limited*), MFM (eng. *Modified Frequency Modulation*), PRML (eng. *Partial Response, Maximum Likelihood*). Ovu metodu je predložio Peter Guttman 1996. U tih 35 prijepisa su sadržani scenariji svih tipova kodiranja arhitektura starih i do 30 godina pa sve do današnjih. Stoga ni u kojem slučaju nije potrebno obaviti svih 35 prepisivanja jer će to imati isti efekt kao da je obavljeno i samo nekoliko njih, a oduzeti mnogo više vremena [12].

Guttman tvrdi kako je nemoguće potpuno dezinficirati disk samim prepisivanjem podataka. Prepisani podaci se mogu rekonstruirati pomoću magnetske mikroskopije koja se bavi čitanjem magnetskih uzoraka na pločama diska, no ti postupci mogu koštati i do nekoliko milijuna dolara.

[7] Demagnetizeri su uređaji koji diskove izlažu magnetskom polju čime se onemogućava rekonstrukcija podataka s diska.

[8] Ova metoda nije odobrena za dezinficiranje medija koji sadrže tajne podatke.

5. Besplatni alati za sigurno uklanjanje datoteka

Uz mnoge komercijalne forenzičke alate koji mogu uništiti podatke na disku (npr. PGP Desktop [13], Evidence Eliminator [14], Drive Scrubber [15]), postoje i mnogi besplatni alati koji mogu poslužiti korisniku da izbriše ono što ne želi da drugi ljudi nađu na njegovom računalu. U nastavku teksta će se navesti nekoliko takvih alata.

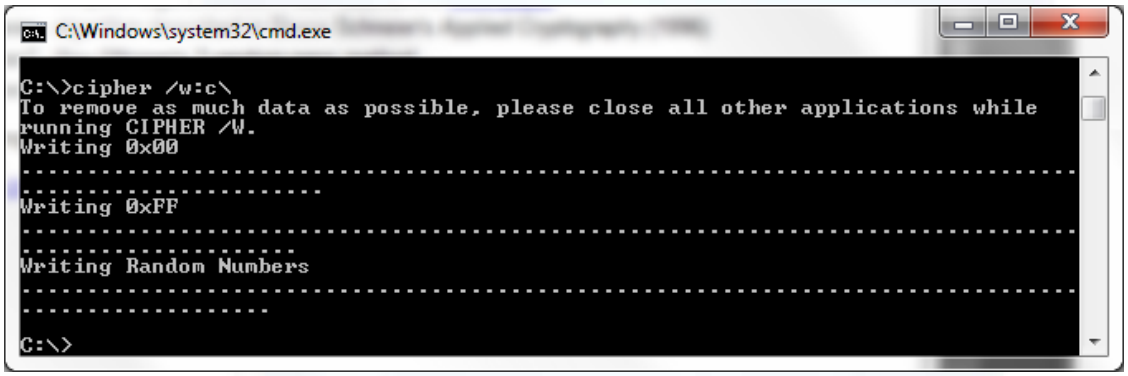
5.1. Cipher.exe

Cipher.exe je program ugrađen u operacijski sustav Windows (Windows 2000 SP 3 i kasnije inačice) sa svrhom prepisivanja preko nealociranih lokacija. Radi tako da prvo preko svih lokacija zapiše nule, potom jedinice te na kraju niz pseudoslučajnih brojeva (DoD metoda). Potrebno je:

1. Zatvoriti sve aplikacije.
2. Odabrati gumb Start → upisati „*run*“ → upisati „*cmd*“ → tipka enter
3. Upisati

```
cipher /w:'mapa'
```

gdje 'mapa' označava particiju, odnosno mapu na particiji, na kojoj se žele očistiti nedodijeljene lokacije (Slika 10).



Slika 10. *Rad alata cipher.exe*

5.2. Windows Sysinternals Sdelete

Windows Sysinternals Sdelete je još jedan alat za čišćenje nealociranih lokacija kao i brisanje datoteka i mapa. Alat se može preuzeti na web stranici alata [17], nakon čega se koristi iz komandne linije (Windows 2000 i kasnije inačice) na sljedeći način:

```
sdelete [-p passes] [-s] [-q] <datoteka ili mapa>,
sdelete [-p passes] [-z|-c] [slovo particije],
```

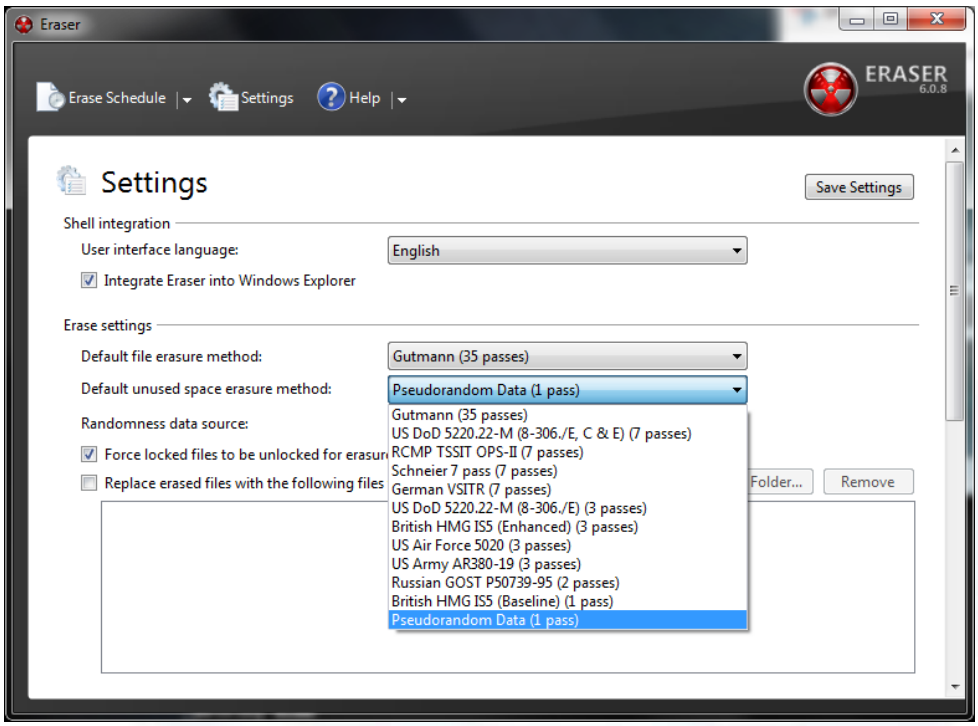
gdje su opcije:

- c	bez slobodnog prostora (dobro za optimizaciju virtualnog diska)
- p passes	precizira se broj prepisivanja podataka
- s	rekurzivno brisanje podmapa
- q	nemoj dojavljivati greške
- z	očisti slobodan prostor

5.3. Eraser

Alat koji omogućava potpuno uklanjanje osjetljivih podataka s diska tako što ih nekoliko puta prepiše s pažljivo odabranim uzorcima podataka. Eraser radi na inačicama Windows operacijskog sustava: XP (SP 3), Vista, 7 Server 2003 (SP 2), Server 2008 i Server 2008 R2. Može se preuzeti na web stranici proizvoda [16].

Osim brisanja datoteka i nealociranog prostora, Eraser ima mogućnost i brisanja neiskorištenog prostora u klasterima, prilikom čega korisnik sam bira metode postupaka (Slika 11). U opcijama se može podesiti da se alat pokreće samostalno prilikom svakog gašenja računala.



Slika 11. *Sučelje alata Eraser - mogućnosti izbora metode čišćenja*

5.4. Freeraser

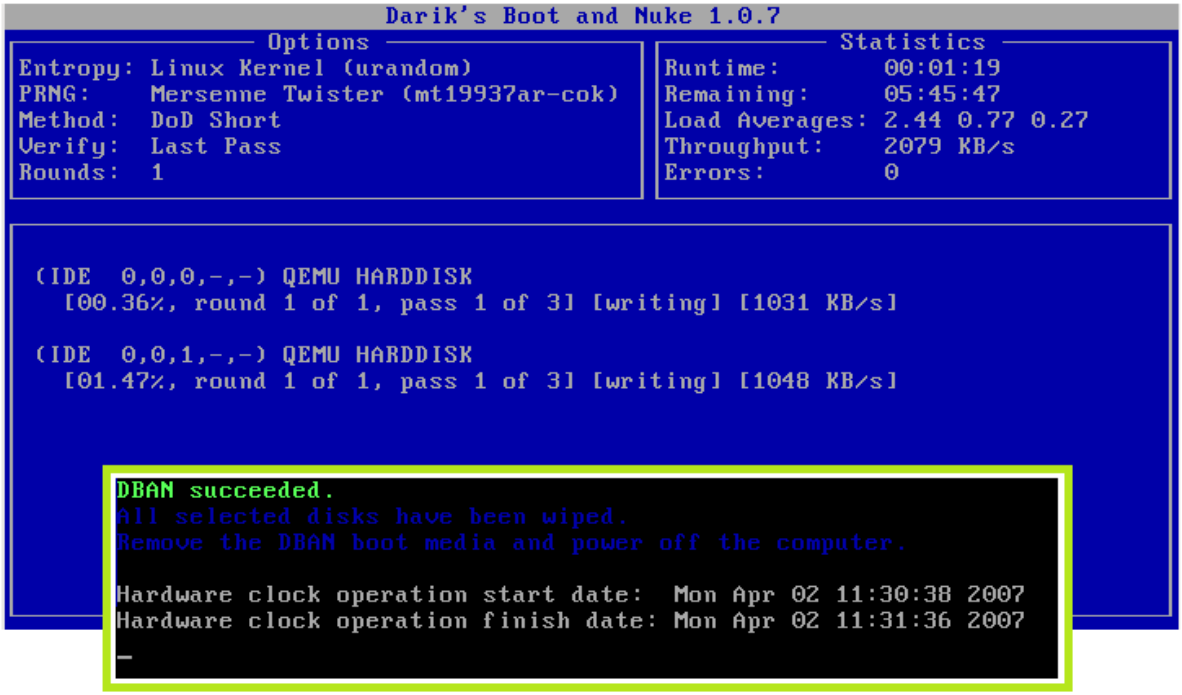
Freeraser je alat za brisanje osjetljivih podataka. Nakon preuzimanja s web stranice alata [18], alat se može pokrenuti pri čemu se na ekranu pojavi slika koša za smeće. Desnim klikom na sliku koša se pojavljuje izbornik pomoću kojeg se biraju datoteke koje se žele uništiti. Pri tome se koristi jedan od 3 moguća načina:

- brzo uništavanje (1 prepisivanje nasumičnim podacima),
- prisiljeno uništavanje (3 prepisivanja po DoD 5220.22M standardu) te
- konačno uništavanje (35 prepisivanja u skladu s Guttmanovim algoritmom).

Slika 12. *Freeraser koš za smeće - dok čeka i dok uništavapodatke*

5.5. DBAN

Vrlo popularan alat za fizičko brisanje diska. Linux paket, dolazi na disku (CD i *floppy*) spreman za pokretanje, DBAN će automatski i potupno izbrisati sadržaj bilo kojeg diska kojeg može detektirati zbog čega je dobro rješenje za hitno brisanje velikih količina podataka [20].



Slika 13. *Sučelje alata DBAN*

5.6. Fizičko brisanje diska

Standardni alat na svakoj distribuciji Linuxa i Unixa je 'dd'. Jedan od načina korištenja tog alata je da u svaku lokaciju na disku zapiše nulu ili slučajan znak. Naredbe izgledaju ovako:

```
# dd if=/dev/zero of=/dev/hda          - zapisuje nule
# dd if=/dev/random of=/dev/hda        - zapisuje slučajne znakove
```

pri čemu *'if'* znači *input file* ili datoteka iz koje se zapisuje, a *'of' output file* ili datoteku u koju se zapisuje (što je u ovom slučaju cijeli disk *hda*). Za korištenje ovog alata je potrebno imati operacijski sustav Linux – instaliran ili pokrenut s CD-a prilikom paljenja računala (u kojem slučaju ga nije potrebno imati instaliranog).

5.7. Disk scrub utility

Disk scrub je alat za Linux/Unix okruženje koje prepisuje diskove, datoteke i ostale uređaje s ponavljajućim uzorcima podataka čime se otežava rekonstrukcija izvornih podataka.

Nakon instalacije potrebno je napraviti pomoćni direktorij za *disk scrub* koji će se nakon cijelog postupka izbrisati. Potrebno je upisati naredbe:

```
$ sudo mkdir /pom_dir
$ scrub -X /pom_dir/svasta
$ sudo rm -f /pom_dir/svasta
```

Scrub koristi nekoliko ranije spomenutih metoda za čišćenje kao i neke koje nisu toliko poznate:

- U.S. NNSA Policy Letter NAP-14.1-C,
- DoD 5220.22-M,
- U.S. Army AR380-19,
- metoda njemačkog centra za sigurnost u informacijskim tehnologijama,
- Guttmanov algoritam [12],
- Schneierov algoritam [25],
- Pfitznerova metoda [26] 7 zapisivanja nasumičnih podataka te
- Pfitznerova metoda 33 zapisivanja nasumičnih podataka.

5.8. Shred

Shred je alat za Linux/Unix okruženje koji može prepisati prostor na disku i do 25 puta ako se ne specificira drugačije. Primjer naredbe koja će na disk *hda* 2 puta zapisati nasumične podatke (umjesto 25), završiti proces zapisivanjem nula te dojavljivati napredak:

```
# shred –n 2 –z –v /dev/hda
```

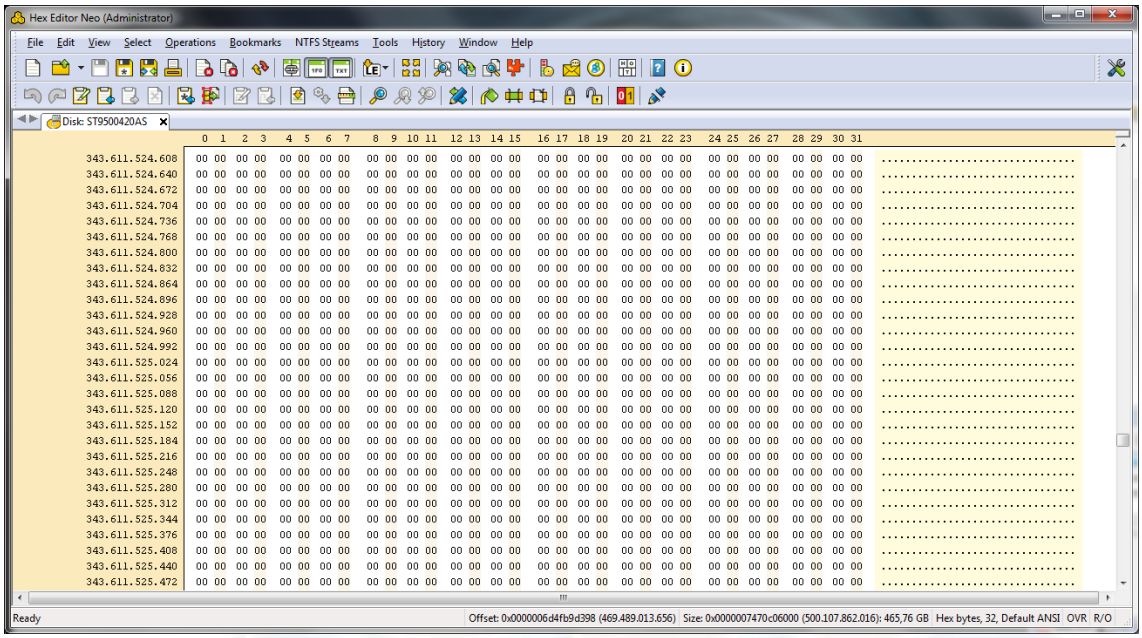
Alat	OS	Podržane funkcije
Cipher.exe	Windows	Brisanje datoteka, čišćenje nealociranog prostora
SDelete	Windows	Brisanje datoteka, čišćenje nealociranog prostora
Eraser	Windows	Brisanje datoteka, čišćenje nealociranog i neiskorištenog prostora
Freeraser	Windows	Brisanje datoteka
DBAN	Linux/Unix	Brisanje svog prostora na disku
dd	Linux/Unix	Brisanje svog prostora na disku
Disk Scrub	Linux/Unix	Brisanje svog prostora na disku
Shred	Linux/Unix	Brisanje svog prostora na disku

Tablica 3. *Pregled mogućnosti besplatnih alata za sigurno uklanjanje datoteka*

6. Verifikacija zapisa

Iako se svi alati na Internetu nude kao odlični, efikasni i općenito bolji od konkurencije, ne preporuča se slijepo im vjerovati. Nakon što je alat obavio svoj dio posla, potrebno je potvrditi da je sve obavljeno kako je obećano. To je najsigurnije napraviti s heksadecimalnim uređivačem – alatom koji pruža direktan pogled u stanje memorijskih lokacija na disku [24]. Ako je alat kojim se brisao disk trebao prvo sve prepisati jedinicama, potom nulama, heksadecimalni uređivač će pokazati da li su sve lokacije uistinu prepisane nulama.

Iako neki od alata nude postupak verifikacije nakon prepisivanja podataka, greške u programima nisu rijetke i moguće je da korisnik dobije obavijest da je sve prošlo glatko i po planu, a da je zapravo dio diska preskočen u postupku. Verifikacija zapisa je još jedna od prednosti komercijalnih alata. Tvrtke koje prodaju svoje proizvode su obično posvećenije poboljšavanju performansi svojih proizvoda te je lakše vjerovati učinkovitosti takvih alata.



Slika 14. *Sučelje heksadecimalnog uređivača Free Hex Editor*

7. Zaključak

Ljudi prečesto vjeruju da je njihovo računalo sigurno mjesto za pohranu podataka. Računala, kao i diskovi su ranjivi i podložni krađi. A u današnje vrijeme mnogobrojnih besplatnih kao i komercijalnih forenzičkih alata, gotovo svatko s imalo poznavanja računala može doći do izbrisanih podataka na disku. Zato je bitno obratiti pažnju na ovaj problem. Potrebno je odvagnuti koliko vremena i novaca se isplati uložiti u zaštitu podataka.

U većini slučajeva je ipak riječ o korisnicima koji ne žele da im šefovi, roditelji, kolege i drugi ljudi u neposrednoj blizini računala otkrivaju osobne podatke, no ne treba zanemariti ni slučajeve kad web aplikacije pohranjuju osobne podatke kao što su brojevi kreditnih kartica, imena, prezimena, adrese i slično.

O kojoj god situaciji da je riječ, i koliko god korisnik vjerovao da nema ništa za sakriti, uvijek se može naći određeni komadić informacije koji može, ako ne nanijeti monetarnu štetu, onda barem osramotiti korsinika.

Poanta priče je ta da se sigurnost na računalu kao i na Internetu treba shvatiti ozbiljno. Trajno i sigurno uklanjanje podataka s diska je prvi korak prema sigurnijem radu na računalu kao i preduvjet za poklanjanje ili odbacivanje starog diska.

8. Leksikon pojmova

Datotečni sustav

Datotečni sustav (eng. *filesystem*) se može smatrati tablicom sadržaja ili bazom podataka koja sadrži fizičke lokacije svih podataka na tvrdom disku.

http://pcsupport.about.com/od/termsf/g/filesystem.htm

Metapodaci

Metapodaci opisuju kako, kad i tko je napravio određeni skup podataka (npr. dokument) te kako su ti podaci uređeni. Najčešća definicija metapodataka je „podaci o podacima“.

http://www.webopedia.com/TERM/M/metadata.html

Blowfish

Simetrični kriptografski algoritam za šifriranje blokova podataka, stvorio da je Bruce Schneier 1993. godine. Radi sa blokovima veličine 64 bita i podržava ključeve do 448 bita. Trenutno ne postoji učinkovit način razbijanja ovog algoritma, no dolaskom algoritma AES sve slabije se koristi.

http://www.webopedia.com/TERM/B/Blowfish.html

9. Reference

[1] Microsoft Help and Support: Default cluster size for NTFS, FAT and exFAT, http://support.microsoft.com/kb/140365, kolovoz 2009.

[2] LINFO: Hidden File Description, http://www.linfo.org/hidden_file.html, lipanj 2011.

[3] TechNet Blogs: What is the page file for anyway?, http://blogs.technet.com/b/askperf/archive/2007/12/14/what-is-the-page-file-for-anyway.aspx, prosinac 2007.

[4] Microsoft Help and Support: Description of how Word creates temporary files, http://support.microsoft.com/kb/211632, svibanj 2010.

[5] Microsoft Download Center: Office 2003/XP Add-in: Remove Hidden Data, http://www.microsoft.com/downloads/en/details.aspx?FamilyID=144e54ed-d43e-42ca-bc7b-5446d34e5360&DisplayLang=en, kolovoz 2008.

[6] Electronic Discovery Law: Williams v. Sprint/United Mgmz. Co., http://www.ediscoverylaw.com/2005/10/articles/case-summaries/order-to-produce-electronic-spreadsheets-as-kept-in-the-ordinary-course-requires-production-with-metadata-intact-spreadsheet-cells-to-remain-unlocked/, kolovoz 2005.

[7] DoD 5520.22-M National Industrial Security Program Operating Manual (NISPOM), http://www.usaid.gov/policy/ads/500/d522022m.pdf, srpanj 1997.

[8] Wikipedia: Degaussing, http://en.wikipedia.org/wiki/Degaussing, svibanj 2011.

[9] Data Security Inc: Type I Degausser, http://www.datasecurityinc.com/degausser/degausser_type1.html, 2010.

[10] Data Security Inc: Type II Degausser, http://www.datasecurityinc.com/degausser/degausser_type2A.html, 2010.

[11] Linda Volonino, Reynaldo Anzaldua: Computer Forensics for Dummies, Wiley Publishing Inc., 2008.

[12] Peter Guttman: Secure Deletionof Data from Magnetic and Solid-State Memory, http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html, srpanj 1996.

[13] PGP Encryption Products, http://www.symantec.com/business/theme.jsp?themeid=pgp, lipanj 2011.

[14] Evidence Eliminator, http://www.evidence-eliminator.com/, lipanj 2011.

[15] Iolo DriveScrubber, http://www.iolo.com/ds/3/, lipanj 2011.

[16] Eraser Home Page, http://www.heidi.ie/eraser/, svibanj 2011.

[17] Windows Sysinternals, http://technet.microsoft.com/en-us/sysinternals/bb897443.aspx, svibanj 2011.

[18] Destroy Secret Files With Free Data Shredder, http://www.freeraser.com/home/82-freeraser.html, svibanj 2011.

[19] PC Support: How To Boot your Computer from a Bootable CD or DVD, http://pcsupport.about.com/od/tipstricks/ht/bootcddvd.htm, svibanj 2011.

[20] Darik's Boot and Nuke, http://www.dban.org/, svibanj 2011.

[21] Ubuntu forums: Securely Clear Free Hard Drive Space with Scrub, http://ubuntuforums.org/showthread.php?t=333309, siječanj 2007.

[22] Google code: diskscrub, disk overwrite utility, http://code.google.com/p/diskscrub/, svibanj 2011.

[23] The Hard Disk Shred/Wipe page, http://www.digitalissues.co.uk/html/os/misc/shred.html, studeni 2005.

[24] Free Hex Editor, http://www.hhdsoftware.com/free-hex-editor, svibanj 2011.

[25] Bruce Schneier – The Blowfish Encryption Algorithm, http://www.schneier.com/blowfish.html, lipanj 2011.

[26] PC Support: Pfitzner Method, http://pcsupport.about.com/od/termsp/g/pfitzner-method.htm, lipanj 2011.