

# „Skartování“ souborů

Jak se zbavit **CITLIVÝCH SOUBORŮ** v počítači? Obyčejné smazání nepomůže. Srovnali jsme programy, které se postarají o bezpečné smazání.

MARKUS MANDAU

**P**roč starý a nepotřebný harddisk neprodat prostřednictvím Aukra nebo eBay? Vám už nestačí, někdo jiný však za něj rád zaplatí. Ale pozor! Než dáte svůj disk pryč, nezapomeňte jej dobře smazat. Mohou být na něm uložena hesla, přístupy do banky, certifikáty, čísla kreditních karet nebo také soukromé fotografie. Americká společnost Kessler International zjistila, že 40% pevných disků, které jsou prodávány na eBay, obsahuje citlivé soubory původního majitele. Osobní dokumenty obsahovalo 36% náhodně zakoupených disků, interní firemní dokumenty pak obsahovalo 11% disků. 21% disků obsahovalo elektronickou poštu majitele a 13% fotografie. Majitel soubory buď vůbec nsmazal, nebo použil jednoduchou techniku mazání, která nesmaže soubory definitivně.

## Bezpečné přepsání

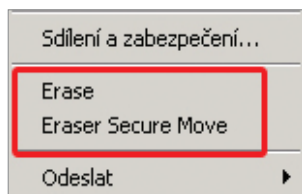
Ono totiž nestačí pevný disk jen zformátovat, to je pouze obecná představa uživatelů. Při formátování se totiž data nepřepisují, ale zůstávají zde uložena, jen se místo označí jako prázdné. Maximálně se může změnit velikost klastru. Ze zformátovaného disku obnovíte soubory velmi jednoduše, třeba použitím freewarového programu Recuva, který najdete na Chip DVD.

Chcete-li se souborů zbavit definitivně, je třeba je fyzicky skutečně přepsat. K tomu slouží speciální nástroje – „skartovačky“ souborů. Který z těchto nástrojů je nejlepší, to prozrazuje náš test. U čtyř placených a dvou freewarových programů jsme testovali jejich možnosti, funkce a schopnosti. Jejich pomocí jsme smazali partition na pevném disku a poté jsme disk předali do laboratoře společnosti Kroll Ontrack, což je specialista na obnovu ztracených dat. Jedná se o nejzná-

### INFO

#### Formátování nestačí

Kdo chce dát svůj datový nosič pryč, měl by z něj smazat veškeré informace, ať už se jedná o disk, nebo jen o paměťovou kartu z fotoaparátu. Bohužel pouhé přetažení souborů do koše nepomůže, a nepomůže dokonce ani naformátování. Účinné je jen smazání pomocí skartovacího nástroje, který soubory fyzicky přepíše, čímž zajistí, že soubory už nikdo z média nedostane.



**Bleskově:** Soubory lze bezpečně smazat i z kontextové nabídky Průzkumníka.

### MAZACÍ STANDARDY

**DoD 5220.22M** byl definován ministerstvem obrany USA. Soubory musí být přepsány trojnásobně – poprvé náhodnými hodnotami, podruhé hodnotami opačnými k hodnotám náhodným a potřetí zcela novými náhodnými hodnotami.

**Standard NATO** požaduje sedminásobný přepis. Šestkrát se střídají hodnoty 00 a FF, posedmě se zapisují hodnoty náhodné.

**VSITR** standard také požaduje sedminásobný přepis. Šestkrát se střídají hodnoty 00 a FF, posedmě se zapíše hodnota AA.

**Algoritmus Bruce Schneiera.** Tento bezpečnostní guru také doporučuje sedminásobný přepis. Nejprve 00, poté dvakrát FF a zbytek náhodnými hodnotami.

Samozřejmě existuje ještě mnoho dalších standardů, které požadují až 35násobný přepis.

vanější společnost zaměřenou na pátrání po ztracených souborech, jejíž služby využívají i státní úřady.

#### Metody: Hádky a argumenty

Kolikrát by se měl soubor přepsat, aby bylo možné jej považovat za bezpečně smazaný, o tom se uživatelé hádají na webových fórech. Proč vlastně? Konvenční pevné disky ukládají informace na disky pomocí magnetického záznamu. Plotny pevného disku jsou pokryty tenkou, magneticky měkkou vrstvou, která uchovává informaci. Plotny jsou rozděleny na stopy a sektory. Ty se ještě dále dělí až na nejmenší možnou informaci, kterou je možné uchovat, tedy hodnotu 0 nebo 1. Při čtení hodnoty získá hlavička disku analogový signál, který přeměňuje na digitální. A právě tato metoda otevírá prostor pro spekulace.

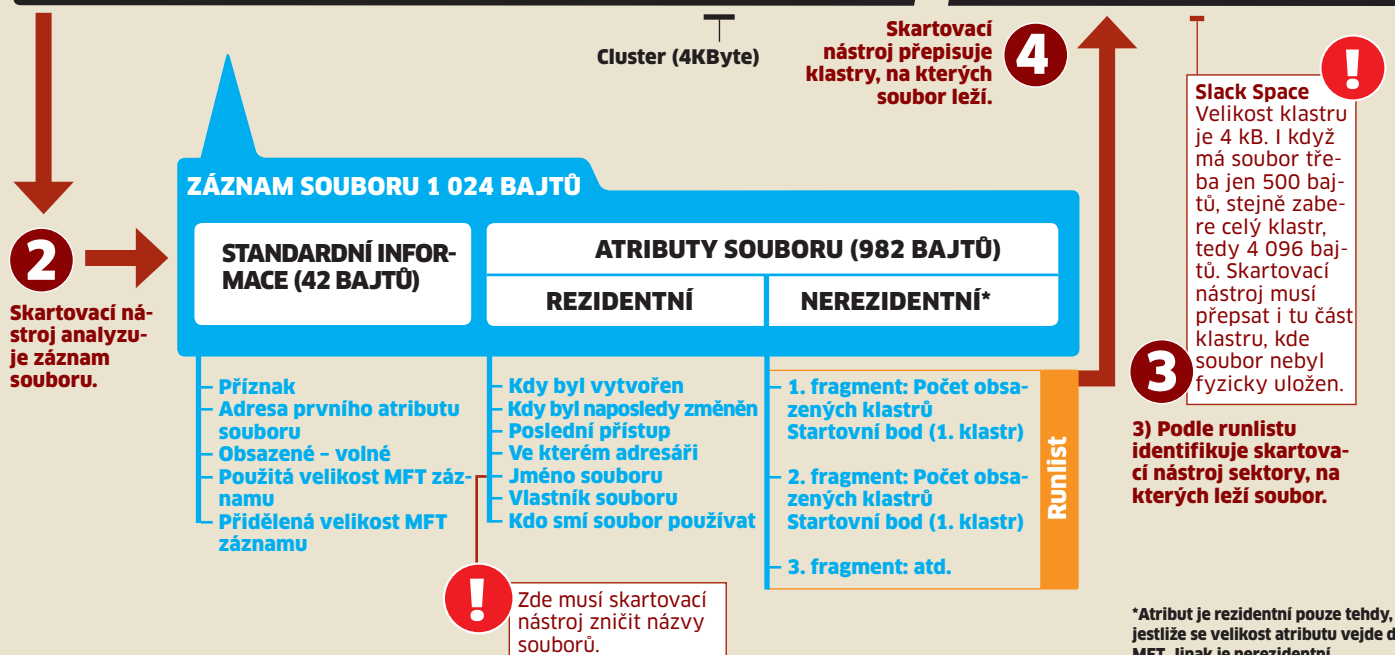
Někteří uživatelé argumentují tím, že síla magnetického pole z analogového signálu hlavičky při přepisování kolísá. Například pokud se 0 přepisuje na 1, analogová hlavička při čtení naměří signál o hodnotě 0,95. Pokud se 1 přepisuje na 1, úroveň signálu dosáhne hodnoty 1,05. Jsou-li hodnoty přepsány pouze jednou, je možné je získat zpět. A jedno přepsání by nezaručilo dostatečné bezpečné smazání. I proto byly vytvořeny speciální standardy pro mazání dat (viz infobox na nahoře).

Tím ovšem spekulace nekončí. Objevila se i myšlenka založená na teorii, že hlavičky disků nejsou dokonale přesné. Zapisují-li určitou hodnotu, ve skutečnosti ji zapisují na nepatrně jiné místo, než je uložena hodnota předchozí. Tím vlastně zůstanou na plotně disku informace o přepsané hodnotě a bylo

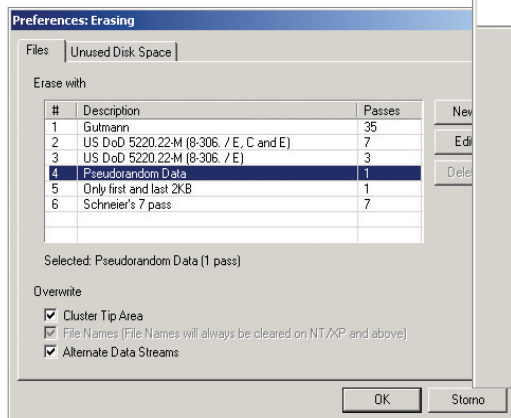
# Jak skartovací nástroje ničí soubory

Na příkladu NTFS partition o velikosti 2 GB vám ukážeme, jak skartovací nástroj ničí soubory. V tomto případě jsou soubory uloženy na klastrech o velikosti 4 KB. Skartovací nástroj musí rozpoznat, na kterých klastrech je soubor uložen, a ty musí přepsat.

- 1** Skartovací nástroj se podívá do indexu partition (Master File Table) a vyhledá záznam o souboru, který bude mazat.



**Metody mazání:**  
Programy nabízejí více metod přepsání dat. Jedno přepsání však bohatě stačí.


**O&O SafeErase průvodce**
**Co chcete udělat?**


O&O SafeErase průvodce je řešení pro bezpečné smazání citlivých dat a nabízí největší ochranu soukromí! Průvodce umožní smazat soubory, složky, disk/oddíl nebo celý počítač jednoduchým stiskem tlačítka!

- Smazat osobní soubory / složky
- Smazat volné místo disku
- Smazat hard disk / oddíl
- Smazat celý počítač

**Komfortní:** Aplikacím nechybí komfortní průvodce.

by možné je dostat zpět. Ani v tomto případě by tedy jedno přepsání nefungovalo.

Obě tyto teorie jsou vlastně správné a ověřené – jenže na disketách, a nikoliv na pevných discích. Na pevném disku totiž zůstane tak zanedbatelná stopa, že je prakticky nemožné předchodí informaci obnovit. Navíc tyto minuturní stopy dokážou rozházet vnější vlivy, jako jsou změny teploty uvnitř disku nebo magnetické pole, do kterého se disk může dostat. Ze stop tak vznikne jen zmeškaných indicií, které s původními daty nemají žádnou souvislost. Navíc vyčistit analogové signály 1:1 není tak jednoduché, jako tomu bylo před několika lety. Kvůli potřebě vysoké hustoty záznamu dat je síla analogového signálu mnohem nižší.

Aby bylo možné dosáhnout tak vysoké hustoty dat, dekóduje DSP (digitální signálový procesor) data načtená z plotny pomocí speciální modulace, jako je například EPRML (Extended Partial Response/Maximum Likelihood). DSP přitom vůbec nevyhodnocuje signálové špičky, ty vlastně při čtení nemají vůbec žádný význam.

Nedávno prováděl podrobný test soudní znalec Craig S. Wright. Měl přitom k dispozici velice moderní mikroskop magnetických sil, který používal místo hlaviček disku. Snažil se vypátrat, jaká byla hodnota pouze jedenkrát přepsaného bitu. Při rekonstrukci navíc musel paradoxně znát, jaká byla hodnota před přepsáním, aby dokázal určit správnou hodnotu bitu. Výsledek: Přepsané hodnoty dokázal potvrdit jen v 56 % případech. Vzhledem k tomu, že možnost trefit správnou hodnotu (0 nebo 1) je padesát na padesát, je šance rekonstrukce velmi nízká. Pravděpodobnost, že se mu takto podaří opravit celý bajt, je jen 0,97%, a to v případě, že znal původní hodnoty! Pokud původní hodnoty neznal, není na obnovu šance.

## Šest skartovacích nástrojů v testu

Co uvedený pokus znamená? Proti skartovačkám dat je jakákoliv laboratoř zcela bezmocná. Abychom to potvrdili, nechali jsme pevné disky, které jsme poslali do laboratoří Kroll Ontrack, skartovačkami souborů smazat pouze jedním přepisem. Tedy žádnými složitými algoritmy nebo několikanásobným přepisem. Ani tak nedokázali specialisté obnovit žádný soubor. Kroll dokázal pouze zjistit, jakou metodou byly soubory smazány, ale nic víc. Dokonce i Slack Space (viz grafika na předchozí straně) byl správně smazán, aby nebylo možné žádné soubory

vypátrat. Co se tedy bezpečnosti týče, všichni kandidáti splňují svůj primární účel.

Přesto jsme našli některé nedostatky. Disk Doctor's Data Shredder, O&O Safe Erase a freewarový Space Eraser nesmažou název souboru z Master File Table. Na základě toho je možné obnovit názvy souborů, které se na disku nacházely před smazáním.

Space Eraser má zase omezenou funkčnost. Po spuštění vyberete jakoukoliv logickou jednotku (včetně disky nebo USB disku) a kliknete na »Start!«. Program přepíše všechno volné místo, které na disku je. Aby byl tedy program účinný i v případě souborů, je třeba je nejprve smazat, případně vysypat koš, a až poté spustit Space Eraser. Je-li

### INFO

## Mazání souborů na flash discích

Nové SSD ukládají soubory elektricky. Proto je třeba použít jiný způsob skartace.

Solid state disks (SSD) jsou tady. Jsou rychlé, robustní, s nízkou spotřebou, zkrátka ideální pro přenosné počítače. Pro skartovačky souborů ale znamenají tyto disky problém. Nelze přesně určit, která oblast má být přepsána.

### BEZMOCNÉ SKARTOVACÍ NÁSTROJE

Životnost jednotlivých buněk u flash disku je omezená. Řadič proto rovnoměrně rozděluje ukládání dat po celém disku, aby používání buněk bylo co nejrovnoměrnější. Tím se zvyšuje životnost SSD. Díky tomu ovšem nemůže žádný program (a dokonce ani přímo

Windows) ovlivnit, na který klastr budou data fyzicky zapsána.

Uživatel pak vlastně nemá šanci uložené soubory zničit. Softwarově není vůbec možné ovlivnit zápis jednotlivých souborů, protože přímo řadič na SSD se stará o fyzickou organizaci.

Přesto máme jeden tip, jak celý SSD smazat. Výhodou SSD je, že jsou malé. Stačí je tedy několika soubory zaplnit až „po okraj“. Pokud bude disk plný nesmyslných souborů (např. velkých filmů), tak se všechny předchozí hodnoty musí přepsat. A tím, že jej zaplníte celý, budete mít jistotu, že jste změnili data všech sektorů.



## NA DVD

### Skartovačky

- SystemUp Eraser 2009 ► skartovačka
- abylon Shredder ► skartovačka
- Heidi Eraser ► skartovačka
- O&O SafeErase ► skartovačka
- Space Eraser ► skartovačka
- Recuva ► obnova smazaných dat

► **NA DVD:** Programy k tomuto článku najdete na DVD pod indexem **SKARTOVAČKY**.

## PLNÁ VERZE

### East-Tec Eraser 2008



Plnou verzi skartovacího nástroje East-Tec Eraser 2008 jsme vám přinesli již minule, a i tentokrát ji na Chip DVD najdete. Aplikace nabízí velmi vysoký komfort, protože likviduje i aplikační data – e-maily, dočasné soubory, soubory prohlížečů apod. Lze ji tedy použít i jako zametač stop pro udržení soukromí. Samozřejmě nechybí kompletní přemazání disků, souborů i adresářů.

místo na disku označeno jako volné, program jej skartuje. Nemusíte se bát o svoje vlastní soubory, ty zůstanou nedotčeny.

### Překážka: Chráněné soubory

Problémem je složka označovaná jako »System Volume Information«. Je to adresář, do kterého si Windows ukládají body obnovy a jiné systémové soubory. Vlastně zde žádné citlivé soubory nenajdete. Body obnovy totiž obsahují jen seznam změn, záznamy v registrech, DLL knihovny a podobné typy souborů. Trochu jiná je situace, používáte-li Vistu Ultimate, která soubory brání. V tomto případě nedoporučujeme používat nástroj Space Eraser, který se snaží přepisovat

volné místo, čímž také sahá do zabezpečené oblasti. To se samozřejmě Vistě nelíbí a snaha se mine účinkem. Všechny ostatní aplikace si ale se »System Volume Information« poradí, mohou do tohoto adresáře přistupovat a mazat jeho obsah.

Ani skartování systémové partition není úplně jednoduché. Nástroje totiž nemohou jednoduše zničit partition se systémem. Ani jeden z freewarových nástrojů, stejně jako Disk Doctor, nenabízejí žádné řešení pro smazání systémové partition. Uživatel proto musí spustit jiný systém, aby mohl systémovou partition přemazat. Všechny ostatní nástroje si se smazáním nějakým způsobem poradí.

V zásadě je možné tyto nástroje použít i pro SSD disky nebo flash disky, je však třeba vědět jak. Na těchto discích funguje ukládání dat jiným způsobem. Jakým, to se dočtete v samostatném infoboxu.

Problémem pro programy jsou také ty oblasti disku, které nejsou připojeny do systému. Může se jednat třeba o staré partition, které byly odstraněny, na disku ale stále existují. Problém vzniká u programů, které vlastně mažou konkrétní písmeno jednotky. Nemá-li partition písmeno přidělené, není vlastně ani co mazat. Jediným programem, který si s tímto problémem poradí, je Safe-Erase od O&O, který umí smazat jakoukoliv část disku. V případě ostatních nástrojů je třeba jednotku do systému přimountovat.

### Rychlost: Velké rozdíly

Doba, za kterou dokážou programy zničit soubory, je značně odlišná. Je to velmi překvapivé, protože nástroje vlastně nedělají nic jiného, než že na klastry zapisují data. Program Disk Doctor potřebuje na přepsání 2GB partition 20 minut, což je nesnesitelně dlouho. Pomocí tohoto nástroje bychom terabajtový disk opravdu mazat nechtěli, vždyť by to trvalo celý týden! Nejrychlejší byly v testu freewarové programy. Ten nejlepší zvládl smazat 2 GB za 34 sekund. Ostatní aplikace ale nebyly nijak výrazně pomalejší a i mazání velkého disku bylo snesitelné. **AUTOR@CHIP.CZ**

## Záruka skartovacích nástrojů: Již po prvním přepsání jsou data pryč

**VÍTEZ TESTU**  
06/2009

	1. MÍSTO	2. MÍSTO	3. MÍSTO	4. MÍSTO	5. MÍSTO	6. MÍSTO
Produkt	SystemUp Eraser 2009	abylon Shredder	Heidi Eraser	O&O SafeErase	Disk Doctors Data Shredder	Space Eraser
Výrobce	zoneLink	abylonsoft	Heidi Computers	O&O Software	Franzis	Patrick Hollerbach
Internet	www.zonelink.de	www.abylonsoft.com	www.heidi.de	www.oo-software.com	www.franzis.de	www.holliesoft.de
Cena	30 eur	25 eur	freeware	615 Kč	30 eur	freeware
Celkové hodnocení	97,6 	97,4 	95,2 	93,2 	86,6 	86,0 
Laboratorní kontrola: soubory	smazáno	smazáno	smazáno	smazáno	smazáno	smazáno
Laboratorní kontrola: jména/popisy	smazáno/smazáno	smazáno/smazáno	smazáno/smazáno	-/-	-/-	-/-
Laboratorní kontrola: smazání slack space						
Doba mazání (mins)*	2:29	1:05	0:43	1:34	20:33	0:34
Mazání prázdného místa						
Mazání System Volume Information						
Mazání systémových souborů	-				-	
Mazání disku/partition	/●	/●	/●	-/-	/●	-/-
Mazání nepřipojených jednotek	-	-	-	-		-

\*Mazání partition o velikosti 2,1 GB s 6 326 soubory

Spíčková třída (100-90)

Střední třída (74-45)

Všechna hodnocení v bodech (max. 100)

Vyšší třída (89-75)

Nelze doporučit (44-0)

ano

ne