Obnova a mazání dat

Vymazáno? Ani náhodou!

Prodat starý pevný disk a přijít si tak na nějaké peníze, to není špatný nápad. Jenomže mnozí tak spolu s hardwarem vydražují i svá osobní data...

Text: Markus Mandau, *autor@chip.cz*

V tomto článku najdete

Roční příjem, placení výživného, platová třída – to jistě nejsou informace, které by o sobě člověk chtěl vytrubovat do světa. A přesto se na discích v bazarech často ocitají tak důvěrné informace, jako je třeba daňové přiznání. Denně tam mění majitele přes tisíce USB pamětí, pevných disků, paměťových karet a mobilních telefonů. A s použitým hardwarem také všechny personální informace, které jsou na něm ještě stále zapsány: daňová přiznání, hesla, intimní fotografie a videa nebo i důvěrné firemní dokumenty.

Předchozí majitelé se samozřejmě domnívají, že svou paměť před odprodejem vymazali. A opravdu to udělali. Jenomže „jednoduše“ vymazaná data se dají velice snadno obnovit. Stačí k tomu vhodný software; většina tzv. „recovery tools“ je dokonce zdarma k dispozici na webu.

Rozhodli jsme se to vyzkoušet a v jednom z bazarů jsme udělali docela objemný nákup: kromě pevných disků a USB „klíčenek“ také digitální fotoaparáty, paměťové karty a mobily. Samozřejmě jsme si naše nové akvizice prohlédli trochu důkladněji – a byli jsme upřímně překvapeni, kolik důvěr- ➔

NAJDETE NA CHIP DVD
TESTY A NÁVODY

- **Eraser 5.82**
  freeware
  www.heidi.ie/eraser
- **PC Inspector File Recovery 4.0**
  freeware
  www.pc-inspector.de
- **TestDisk 6.5**
  freeware
  www.cgsecurity.org
- **Photorec 6.5**
  freeware
  www.cgsecurity.org
- **Restoration 2.5.14 CZ**
  freeware
  www.aumha.org/a/recover.php

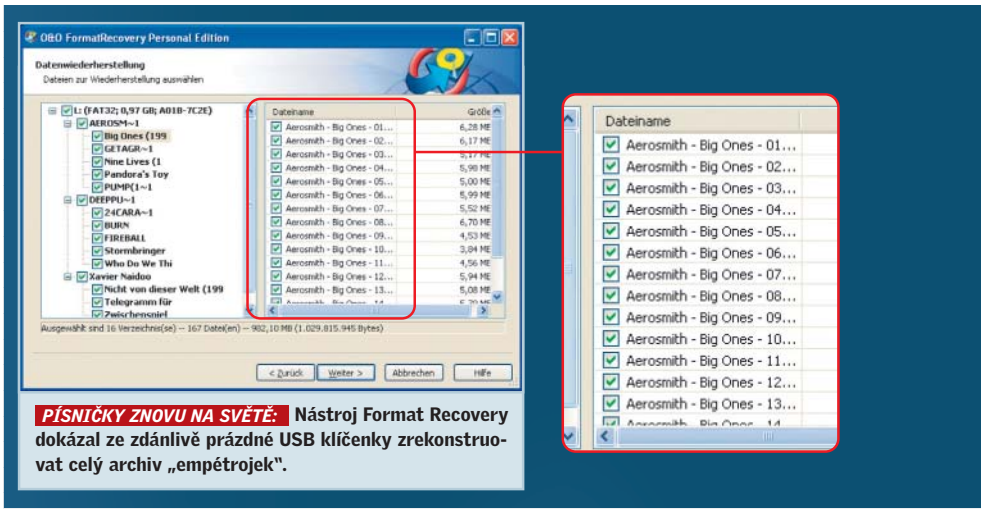
ných a snadno rekonstruovatelných údajů jsme na nich našli. Fotky z dovolených, pirátské kopie, kompletní SMS korespondenci včetně telefonních čísel, už v úvodu zmíněné daňové přiznání – předchozí majitelé nám tak dali do svého soukromého života nahlédnout opravdu hluboce.

Než tedy svá vyřazená paměťová zařízení zpeněžíte nebo se jich zbavíte jinak, měli byste zajistit, aby se v jejich paměti už skutečně žádná data nenacházela. Proč prosté odstranění souborů z koše ve Windows, a dokonce ani formátování disku k ochraně privátní sféry nestačí, to je vysvětleno v rámečku na straně 131. Je proto lepší věnovat této záležitosti nějaký čas a celou paměť přepsat. U 200GB pevného disku to sice trvá i několik hodin, ale tato oběť se vyplatí; vhodný software najdete na Chip DVD. A nyní si přečtěte, co všechno jsme ve vydražením hardwaru objevili – a jak příslušný typ paměti spolehlivě vymažete.

PEVNÝ DISK A USB PAMĚŤ

Pirátské kopie, archiv MP3 a daňové přiznání

Obnovit smazaná data není pro „recovery tools“ žádný problém – lhostejno, zda na pevném disku či v USB paměti. Obě tato paměťová média totiž používají stejné souborové systémy (FAT nebo NTFS) a Windows mají všechna zápisová práva potřebná pro přístup k relevantním údajům.



PÍSNIČKY ZNOVU NA SVĚTĚ: **Nástroj Format Recovery dokázal ze zdánlivě prázdné USB klíčenky zrekonstruovat celý archiv „empétrojek“.**

USB paměť: Náš první dojem po řadě zkušebních nákupů v bazaru: použité „flešky“ jsou levné – a jako zdroj dat docela vydatné. U mnoha z nich se našim nástrojům podařilo vymazané soubory vrátit na „světlo světa“, například písničky ve formátu MP3 a pirátsky zkopírovaný software. Zcela bez problémů to probíhalo například u 128MB paměti Q-Max. Všechno bylo samozřejmě vymazáno, ale už při krátké kontrole nástrojem Restoration *(www.aumha.org/a/recover.php)* vyšlo najevo 115 souborů. Z nich bylo 41 dosud neporušených, u zbývajících se jednalo o záznamy částečně přepsané. Mezi nálezy byla i provozuschopná pirátská kopie WinDVD 7. Tu jsme dokázali kompletně extrahovat – a přišli jsme tak zadarmo k novému funkceschopnému softwaru; pomocí „přiloženého“ prográmku „keygen.exe“ jsme si totiž k němu mohli i vygenerovat příslušné sériové číslo.

Trochu náročnější bylo dobývání smazaných dat z 1GB kolíčku značky Sharkoon, který bývalý majitel před odprodejem přeformátoval. V takovém případě už nástroj Restoration nepomůže: ten totiž neprovádí tzv. „RAW skenování“, a vymazané soubory tedy nemůže rozpoznat na základě bitových vzorů nebo souborových signatur. Je tedy odkázán jenom na položky označené v alokační tabulce (FAT) jako zrušené – ta je ale po přeformátování prázdná.

Sáhli jsme proto po speciálním programu FormatRecovery *(www.oo-software.com)*. Tento nástroj umí dokonce zrekonstruovat i názvy souborů. Stačilo jen nechat jej chvíli běžet a zanedlouho byla všechna data opět na světě. Pomohli jsme si tak k MP3 archivu s téměř 170 songy, počínaje skupinou Aerosmith a konče Pepíčkem Zímou – komentář k hudebnímu vkusu předchozího majitele si na tomto místě odpustíme.

Pevný disk: Při prodeji pevných disků se zdá bezpečnostní povědomí uživatelů přece jen trochu výraznější. Přesto jsme na 80GB disku od Maxtoru něco nalezli. Po jeho připojení k IDE kabelu jsme nejprve neviděli nic: žádná data, všechny oddíly smazány. Program „TestDisk“ (na Chip DVD) však poskytl jiný obraz: nástroj našel primární bootovací oddíl a tři logické diskové jednotky v přídavném oddílu. Jak se zdá, disk byl jednoduše „vyprázdněn“ nějakým diskovým editorem nebo příslušným nástrojem Windows.

Zrušené jednotky označuje TestDisk písmenem „D“ (z anglického „deleted“). Dají se však pomocí atributu „L“ („logical“) změnit a prostřednictvím „Write“ obnovit. Po restartu byly oddíly na disku opět viditelné, data však ještě ne. Ta totiž původní majitel dodatečně vymazal. Obezřetné, ale nikoli dostatečně. Neboť od této chvíle už lze obnovit data obvyklým způsobem: vyvolat „recovery tool“, spustit analýzu a obnovit data. Nejšikovnější je přitom přístup zvenčí, aniž by operační systém znovu startoval a zapisoval přitom na disk.

Takže – nabootovat linuxový systém. Například Knoppix plus freewarové nástroje jako „fatback“ a „ntfsundelete“. Nevýhodou je tu však ovládání z příkazového řádku: je-li třeba rekonstruovat více souborů, stojí to hodně času. Proto jsme se rozhodli pro komerční linuxový software Data Rescue firmy Prosoft *(www.prosofteng.com)*. Snadno se obsluhuje v duchu zásady „založit, nabootovat, skenovat“ a má také tu přednost, že upozorňuje na hardwarové chyby. Pokračování by totiž za těchto okolností mohlo vést ke ztrátě dat. V takových případech může Data Rescue na přání kompletní disk naklonovat jako „image“. Data se pak obnovují odtud. To je

ostatně také metoda, jakou obvykle postupují profesionální záchranáři.

Po dokončení akce nám Data Rescue předložil tisíce souborů. V jednom z oddílů například pirátskou kopii filmového hitu „Šestý smysl“, v jiném zase diskový obraz kompletní instalace Windows – obojí jsme tak při nákupu harddisku dostali jako přídavek gratis.

Daleko zajímavější jsou ovšem dokumenty, které o původním majiteli prozrazují důvěrné informace. Jeden takový se stal přímo zlatým hřebem naší „recovery tour“: v oddílu označeném „Backup“ jsme narazili na několik PDF souborů, mezi nimi také na kompletní daňové přiznání za rok 2005. Kolik exmajitel disku Maxtor vydělává, vám zde samozřejmě neprozradíme – snad jen to, že jednal mimořádně lehkomyslně!

A jak tedy vymazávat správně? Použijte „skartovač“ souborů, jako je například Eraser. Ten nejprve přepíše volnou paměť a všechny úkryty dat. V druhém kroku jím pak ještě zničíte existující soubory.

DIGITÁLNÍ FOTOAPARÁT A SMARTCARD

Trapný autoportrét a fotky z dovolené

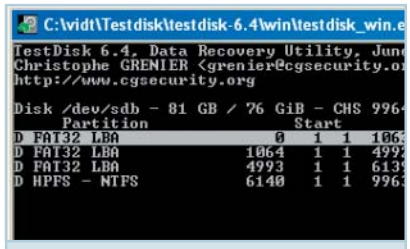
Amatérští fotografové přicházejí do styku s dvěma pamětmi: s interní uvnitř „digiťáku“ a s kartou typu SmartCard, například SD-Card nebo Memory-Stick. Obě paměti byste před odprodejem bezpodmínečně měli správně vymazat, a to každou jiným způsobem.

Paměť digitálního aparátu: Tady je fotograf v obtížné situaci. Neboť i kdyby chtěl, vnitřní paměť fotoaparátu často přepsat nedokáže. Nástroje jako Eraser většinou nefungují – jako programům pro Windows jim prostě chybějí zápisová práva. Samotný aparát sice mívá funkci pro mazání snímků, ta ale pracuje stejným způsobem jako Windows. To znamená, že všechna data v paměti zůstávají, jenom se už nezobrazí. Proto jsme také u čerstvě zakoupeného Nikonu Coolpix L6 s 16 MB interní paměti hned napoprvé uspěli.

Přístup z PC nám snadno zajistil USB kabel. Rychlé prohledání opensourcovým nástrojem „Photorec“ specializovaným na obnovu fotografií vyneslo „na světlo boží“ šest JPEG fotografií ve vysokém rozlišení, mezi nimi i poněkud přehnaně lichotivý portrét minulého majitele. Jeho štěstím bylo, že přístroj zřejmě nebyl často používán a brzy byl odprodán: vnitřní paměť byla zaplněna jen z poloviny.

Smartcard: Starší modely digitálních přístrojů nemají vnitřní paměť a všechny snímky ukládají přímo na paměťovou kartu. Obnovení fotek vymazaných na těchto médiích je dětská hračka a funguje principiálně stejně jako u USB pamětí. Také souborový systém je zpravidla stejný, totiž FAT.

Díky jedné použité SmartCard kartě jsme mohli zrekonstruovat jistou zajímavou rodinnou dovolenou v Las Vegas: na 1GB SD-Card jsme našli 104 fotek, dílem ve formátu TIF, dílem v JPEG, všechny ve vysokém rozlišení a v nejlepší kvalitě. Jen jsme se museli obrnit trochou trpělivosti: na obnovu všech snímků potřeboval Photorec asi hodinu. Poznamenejme ještě, že co funguje s SD-Card, podaří se i s jinými paměťovými kartami.



ODHALENÍ DISKOVÝCH ODDÍLŮ: Nástroj TestDisk vyslídí dokonce i zrušené logické jednotky a zviditelní je.

Jak vymazávat správně: U karet SmartCard postupujte stejně jako v případě USB pamětí – přepište je programem Eraser. Obsah interní paměti digitálního fotoaparátu zlikvidujete nejlépe tak, že ji zaplníte bezvýznamnými fotografiemi.

SMARTPHONE A MOBILNÍ TELEFON

Zprávy SMS a telefonní čísla

Mobilní telefony lze rozdělit do dvou tříd: U té první, zahrnující tzv. smartphony, je vypátrání smazaných dat snadné. Zato průměrný

Proč výmaz dat ani přeformátování disku nestačí

Když pod Windows odstraníte soubor, ocitne se v „odpadkovém koši“. Pokud ten vyprázdníte, soubor už sice neuvidíte, ale ještě zdaleka není zničen.

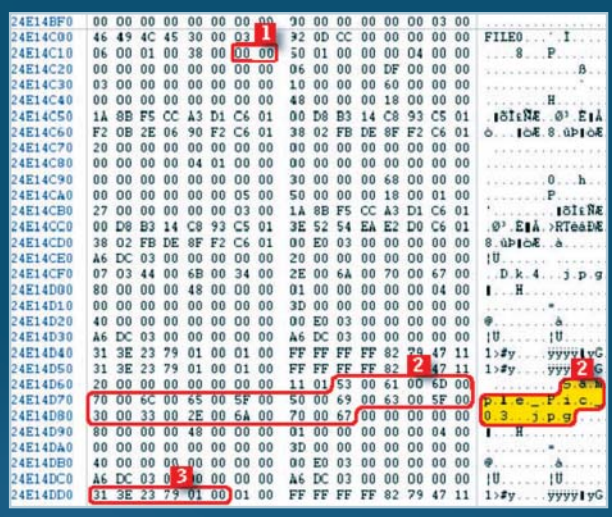
Jednoduchý případ

Při „vysypávání“ souboru z koše se děje toto:

1 V alokační tabulce souborů změní Windows pouhé dva bajty. Ty pak oznamují, že soubor je vymazán.

2 Všechny ostatní údaje zůstanou na disku zachovány, mezi nimi i název souboru.

3 Díky tomu si může software pro obnovu dat v tabulce snadno přečíst, ve kterých klastrech jsou data uložena. Oblast s těmito informacemi se jmenuje „Dataruns“ a obsahuje údaje o tom, kolik klastrů soubor celkem zabírá, na kolik fragmentů je rozdělen a ve kterém klastru data začínají. Na základě těchto informací dokáže „recovery tool“ každý soubor zrekonstruovat.



Komplikovaný případ

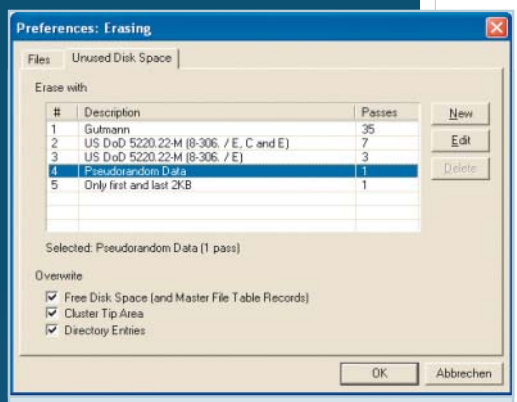
Složitější situace nastane, jestliže příslušnou položku ve zmíněné tabulce už operační systém přepsal novými informacemi nebo byla-li jednotka přeformátována (pak jsou položky „vynulovány“). Pak musí obnovovací software relevantní datovou oblast podrobně prozkoumat a na základě „vzorků souborů“ zjistit, o jaký typ souboru se jedná a kolik klastrů jeho data zabírají. I takto náročný úkol je v mnoha případech realizovatelný. Vezměme si například soubor ve formátu JPEG: Jeho hlavička obsahuje na začátku identifikátor „JFIF“, vlastní obrazová data končí prozaickým příznakem „EOI“, tedy „End of image“. Pouze u souborových formátů, které nezná, musí nástroj svůj úkol vzdát.

Jak totálně zničit všechna data

Dříve než použitý datový nosič odprodáte nebo i odevzdáte do odpadu, měli byste jej jednou kompletně přepsat. Pak už z něj nedokáže nic vytáhnout ani záchranná laboratoř. Nástrojem, který tuto úlohu spolehlivě zastane a objeví i všechny úkryty dat, je program Eraser. Najdete jej i na našem Chip DVD.

Eraser se začlení do kontextového menu v Průzkumníku Windows a je tak neustále k dispozici. Zlikviduje jak obsah volné paměti, tak existující složky a soubory. (Na vysvětlenou: Volná paměť je oblast disku, která neobsahuje platné soubory. Mohou se v ní však pochopitelně nacházet data dříve „vysypaná" z koše.)

TIP: Chcete-li proces výmazu urychlit, změňte nejprve v Eraseru metodu, kterou má pro likvidaci dat použít. Přednastaven je trojnásobný přepis, což zbytečně zdržuje. Jestliže v Preferences Erasing změníte metodu na Pseudorandom Data, zhostí se Eraser svého úkolu za třetinu času.



NASTAVENÍ „SKARTOVAČE": V Eraseru změňte metodu, kterou má pro ničení dat použít. Při správném nastavení pracuje třikrát rychleji.

běžný mobil působí podstatně víc potíží, ale i zde existuje cesta k úspěchu.

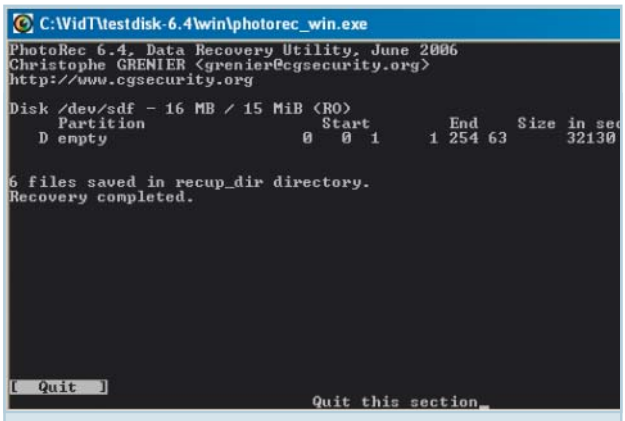
Smartphone: Jak snadno se lze „vloupat" do přístrojů této třídy, o tom jsme se přesvědčili na příkladu Nokie E61. Po připojení k počítači v režimu datového přenosu ji Widows automaticky rozpoznají jako další mechaniku a povolí k ní přístup libovolnému recovery softwaru. A proč by ne? Vždyť ve smartphonu koneckonců běží operační systém SymbianOS. Ten jako souborový systém dovoluje FAT – a víc obnovovací programy pro načtení celé vnitřní paměti smartphonu nepotřebují.

Vděčnými oběťmi jsou také mobilní telefony firmy Sony Ericsson. Model K610i jsme připojili pomocí dodané soupravy PC-Suite. Dokud ta běží, mají k mobilu přístup také aplikace Windows. Freewarový nástroj PC Inspector File Recovery od firmy Convar zde objevil několik smazaných fotek a videí z letní dovolené u Středozemního moře. Byly uloženy v adresáři „100MSDCF", do nějž foťáček v mobilu obvykle ukládá vlastní nafocený materiál.

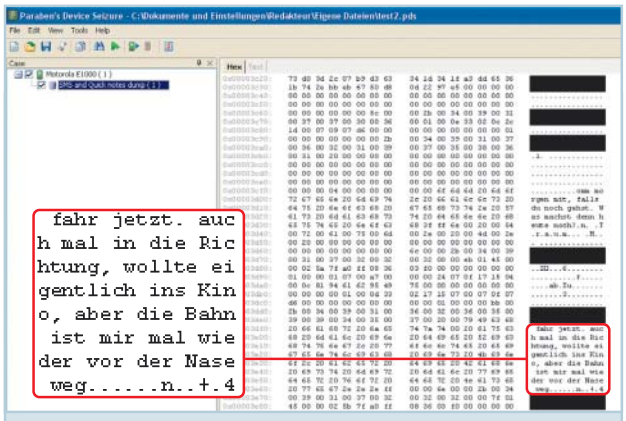
Běžný mobil: U mobilních telefonů, které se nepřipojují jako jednotka pod Windows, je náš úkol obtížný – každý výrobce totiž používá vlastní operační systém. Většinou dokonce několik, pro každou výrobní řadu jiný – a ten se s každým novým modelem znovu obměňuje. Z těchto důvodů také neexistuje obvyklý recovery software pro obnovu vymazaných údajů v mobilu. Co však existuje, jsou programy, které se v soudní praxi používají pro zajišťování důkazních materiálů. Jsou zpravidla velmi drahé a používají je například policejní vyšetřovatelé nebo laboratoře pro záchranu dat. Přední hráč v tomto oboru Kroll Ontrack *(www.krollontrack.de)* používá například produkt firmy Paraben *(www.paraben-forensics.com)*. Její parádní program Device Seizure stojí 800 dolarů a disponuje plug-iny pro mnoho modelů velkých výrobců. Vymazaná data software podle daného modelu vyslídí pomocí tzv. fyzického plug-inu, který uloží přesný bitový obraz paměti mobilu. Ten pak lze v integrovaném hexadecimálním editoru podrobně vyhodnotit.

Museli jsme si ovšem nainstalovat USB ovladač příslušného telefonu, neboť Device Seizure zvládá pouze spojení po kabelu, s Bluetooth nebo infračerveným přenosem nepracuje. Nejprve jsme založili nový „Case", abychom pak mohli spustit skenovací funkci programu. Pak už nám „physical plugin" forenzního softwaru předložil všechna data ukrytá v mobilu. V modelu Motorola E1000 jsme tak například odhalili vymazanou SMS korespondenci, včetně příslušných telefonních čísel.

Jak vymazávat správně: Před tímto druhem datové špionáže se normální „mobilista" může chránit jen obtížně. Ostatně jakým softwarem by mohl vnitřní paměť telefonu přepsat? Na to žádný mazací program prostě neexistuje. Na druhou stranu jsou však forenzní nástroje potřebné pro rekonstrukci dat z mobilních telefonů drahé, nesnadno se obsluhují a pracují vždy jen s určitými přístroji konkrétní modelové řady. Ani to však zatvrzelé zloděje osobních kontaktů nebo intimních SMS zpráv nemusí od pokusů o jejich načtení odradit. Kdo se tedy rozhodne pro odprodej svého mobilu a obává se možnosti zneužití v něm uložených údajů, má jedinou spolehlivou cestu: celou vnitřní paměť přístroje fyzicky přepsat, to jest zaplnit ji bezvýznamnými informacemi.



TAJEMSTVÍ FOTOAPARÁTU: Nástroj Photorec umí z interní paměti digitálního fotoaparátu zrekonstruovat vymazané snímky.



PROZRAZENÉ „ESEMESKY": Pomocí softwaru Device Seizure se dají v mobilním telefonu odhalit vymazané SMS a telefonní kontakty.