BEZPEČNÉ MAZÁNÍ DAT: Žádný problém

Pokud víte, jak funguje obnova dat, budete schopni mazat citlivé informace z pevného disku tak, aby je už nikdy nikdo nedokázal přečíst.

MARKUS MANDAU, MICHAL BAREŠ

Základní pravidlo obnovy dat zní: Smazaná data nejsou zničená data. To může být jak výhoda, tak nevýhoda. Přestože jste například smazali nějaký důležitý soubor a při mazání jste ještě tiskli klávesu Shift, aby nešel ani do koše, můžete ještě situaci zachránit. Nástroje integrované do operačního systému Windows vám sice nepomohou, ale existuje řada specializovaných utilit pro obnovu smazaných dat. Potenciální možnost obnovy dat vás ale nepotěší, budete-li například chtít prodat starý počítač a bezpečně z něj smazat veškerý obsah pevného disku tak, aby se v budoucnu nemohl nikdo probírat vaší soukromou korespondencí či pracovními soubory. V podobném případě pomůže pouze několikanásobný přepis datových ploten, který vám nabízejí některé speciální mazací programy.

Obnova a mazání jsou dvě strany jedné mince

Mazání i obnova dat spolu souvisí. Přejete-li si bezpečně smazat data tak, aby je nedokázaly běžné softwarové nástroje opět obnovit, musíte si zvolit správnou metodu mazání. Pokud nejde o kriticky důležitá data, můžete se spolehnout na obyčejnější způsob mazání, který se sice dá v domácích podmínkách ještě obejít, ale je to poměrně složité a časově náročné. Pokud však mažete data, která by mohla v cizích rukou napáchat škodu, můžete zvolit i takovou metodu, na které si pravděpodobně vylámou zuby i specializované laboratoře.

Záleží na datovém médiu

V případě magnetických pevných disků si musíte dát při mazání dat pozor především na záludnosti souborového systému. U SSD a jiných disků s flashovými paměťovými buňkami se při pokusech o bezpečné smazání souborů budete pro změnu potýkat s ochrannými hardwarovými prostředky, které zabraňují opakovanému zápisu dat do stejných buněk a tím i předčasnému poškození flashového disku. Na bezpečnost starých dat si musí dát pozor i majitelé smartphonů a tabletů. Tato zařízení lze snadno uvést do původního továrního nastavení, ze kterého ale není problém data obnovit. Bezpečné odstranění dat z těchto zařízení vyžaduje přímý přístup k vnitřnímu úložišti, který vám ale prostředí OS Windows neumožní. Na následujících stránkách vám ukážeme, jak správně a bezpečně mazat všechna výše uvedená zařízení. Všechny potřebné SW nástroje najdete na našem DVD.

HDD: Skrytá data

Obnovu či bezpečné mazání dat komplikují na magnetických pevných discích skryté datové oddíly, ale lze je provést.

Magnetické disky jsou ideální datová úložiště pro pokusy s obnovováním nebo bezpečným mazáním dat, protože umožňují přímý přístup k fyzicky zaznamenaným bitům a bajtům. Přesné umístění a typ uložených souborů jsou zaznamenány v centrální tabulce systému souborů. V souborovém systému FAT se tento záznam nazývá alokační tabulkou a v systému NTFS nese název Master File Table (MFT). Jakmile smažete nějaký soubor, Windows fyzicky nevymažou sekvenci jeho jedniček a nul z plotny pevného disku, jen jej ve zmíněné tabulce označí za smazaný. Do okamžiku, než dojde k přepsání dat na plotně HDD jinými daty, tak lze smazaný soubor snadno obnovit.

OBNOVA DAT Stačí kliknout na tlačítko »Start«, a freewarový nástroj pro obnovu dat Recuva (na našem DVD) prohledá MFT tabulku a vypíše všechny záznamy označené jako smazané. V případě, že Windows smazala záznam o souboru v MTF tabulce, musíte v položce »Vlastnosti« povolit hloubkové skenování »Deep scan«. V tomto režimu bude Recuva skenovat kompletní povrch disku a vyhledávat shluk dat odpovídající hlavičce souborů. Tyto hlavičky bývají u určitých souborů stejné, například soubor s obrázky ve formátu JPEG vždy začíná posloupností bitů odpovídajících písmenům JFIF. Tyto informace pak většinou stačí k tomu, aby Recuva nalezla a obnovila smazaný snímek. Jediné, co je třeba zadat před vyhledáváním, je typ vyhledávaného souboru.

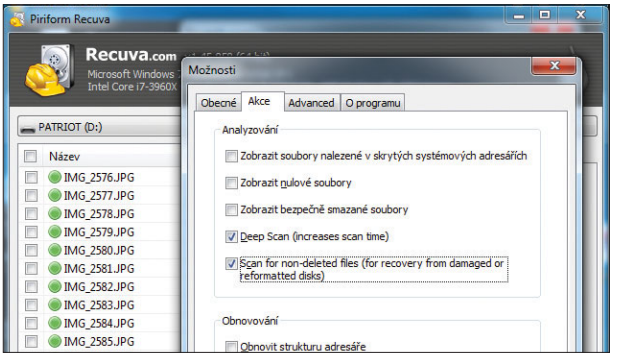
V případě silně fragmentovaných disků, na nichž se kusy jednotlivých souborů nacházejí ve větším množství oddělených bloků, běžné nástroje pro obnovu smazaných dat často selhávají. V takovém případě nastává čas na využití profesionální forenzní expertizy. Tu dokáže provést speciální software, využívající technologii zvanou Carving, například Digital Forensics Framework (**digital-forensic.org**). Po této analýze pak lze jednotlivé kousky fragmentovaných souborů snadno složit. Recuva toho ale také dokáže dost: pokud nenajde záznam hledaného souboru v současné MFT tabulce, pokusí se vyhledat stopy její předchozí verze. To se hodí, například pokud byl pevný disk nedávno přeformátován. Při formátování se totiž vytváří nová prázdná MFT tabulka, přičemž ta stará nemusí být přepsána. Freewarová utilita TestDisk dokáže oživit starší MFT a umožní i vyhledání a obnovu starších datových oddílů. Recuva dokáže pracovat s informacemi ze starší MFT tabulky, pokud v jejím nastavení zaškrtnete možnost »Scan for non-deleted files«.

SPOLEHLIVÉ MAZÁNÍ Jednoduše řečeno, pokud stará data přepíšete daty novými, nemělo by je být možné obnovit ani ve specializované laboratoři. Musíte si ale dát pozor a přemazat opravdu všechna data, protože na disku se mohou nacházet data, o kterých ani sami nevíte. Windows využívají ve spolupráci s NTFS funkci Alternate Data Streams, která se aktivuje, například pokud z internetu stahujete nějaký spustitelný soubor. Tato data přepíšete pouze v případě, že v nastavení programu Eraser zaškrtnete položku »Unused Disk Space«.

FOTO: NIKOLAUS SCHÄFFLER

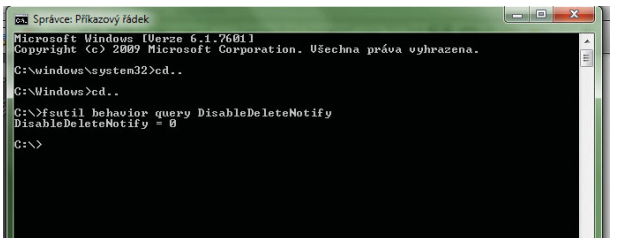
VYHLEDÁVÁNÍ ZTRACENÝCH DAT PROGRAMEM RECUVA

Tento freewarový program dokáže vyhledat smazané soubory pomocí údajů ze staré tabulky souborů. V případě potřeby ale umí provést i hloubkový sken a vyhledat ztracená data na disku pomocí signatur souborů.



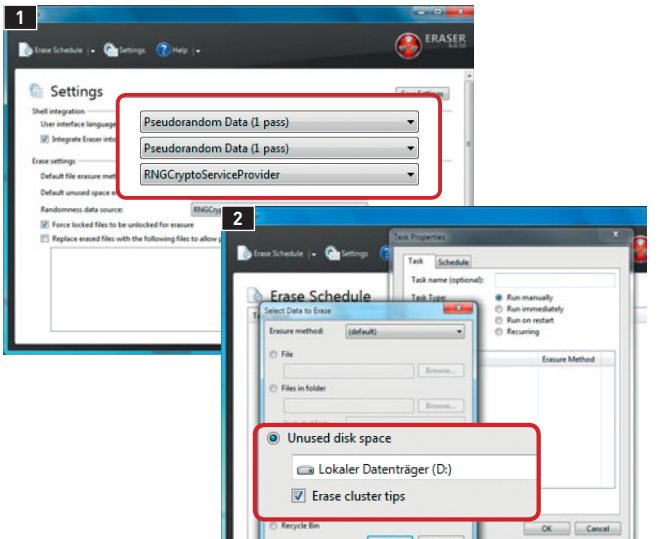
OBNOVA ZTRACENÝCH ODDÍLŮ POMOCÍ PROGRAMU TEST DISK

Nástroj Test Disk, který najdete i na našem DVD, dokáže opravit strukturu celého disku. Pomocí příkazu »Analyze« dokáže najít ztracené diskové oddíly, z jejichž souborových tabulek můžete následně obnovit i původní data.



SPOLEHLIVÉ MAZÁNÍ DAT POMOCÍ ERASERU

Program Eraser (na našem DVD) dokáže rychle a spolehlivě smazat data na disku tím, že je přepíše jinými daty **1**. Ještě bezpečnější je ale provést tento krok podruhé a při druhém průběhu přepsat i data v nepoužívaném diskovém prostoru (Unused Disk Space) **2**.



FLASH: Pozor na řadič

Zápis a čtení dat neřídí v případě SSD disků Windows, ale řadič samotného disku. Poslechne však příkaz k mazání.

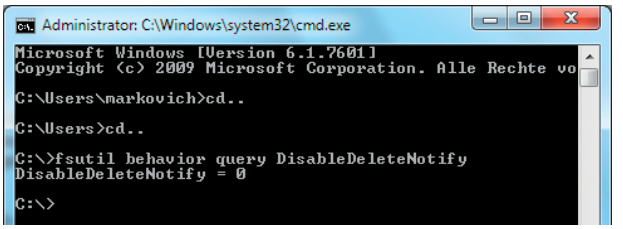
S příchodem SSD disků se změnila pravidla pro obnovu a spolehlivé mazání dat, protože v jejich případě neřídí zápis bitů a bajtů systém Windows, ale řadič samotného disku rozhoduje, jaké paměťové buňky ukládanými daty zaplní. To nemá velký vliv na obnovu smazaných dat, ale bezpečné mazací programy, jako je Eraser, už nemohou zařídit, aby byly všechny smazané buňky spolehlivě přepsány jinými daty a nemohl tak být jejich původní obsah obnoven. Místo toho, aby opravdu došlo k jejich přepsání, jsou tyto buňky pouze označeny v MFT jako smazané a řadič pak data, která do nich měla směřovat, uloží do jiných buněk, aby nedocházelo k jejich zbytečnému opotřebování (tzv. Wear Levelling).

OBNOVA DAT Co se týče obnovy dat, platí pro SSD disky stejná pravidla jako pro HDD disky. Proto také můžete k obnově smazaných a nepřepsaných dat použít i běžné nástroje, jako je Recuva. Ty však nemají přístup do jednoho oddílu SSD disku, kterým je vyhrazený rezervní prostor, který není viditelný pro operační systém. Tento prostor dnes většinou zabírá přibližně sedm procent celkové kapacity disku a je využíván pro práci řadiče. Další problém při obnově smazaných dat z SSD disku souvisí s tzv. příkazem TRIM, který podporují Windows 7. Prostřednictvím příkazu TRIM posílají Windows řadiči informace o tom, které soubory byly definitivně smazány, a řadič pak podle těchto informací smaže patřičné paměťové buňky, ve kterých byl soubor uložen. Tento způsob výrazně snižuje rychlost zápisu dat na SSD disk, protože řadič musí před zápisem obsah daných buněk vymazat. Právě kvůli vymazávání buněk příkaz TRIM dramaticky snižuje šanci na obnovu dat, která jste smazali před delší dobou.

SPOLEHLIVÉ MAZÁNÍ Kompletní úložný prostor SSD disku (většinou i s vyhrazeným rezervním prostorem) můžete snadno přepsat tak, že do řadiče disku pošlete ATA příkaz »Secure Erase«. Jelikož se jedná o ATA příkaz, měl by být SSD disk připojen prostřednictvím rozhraní SATA. Externí USB disky musí podporovat konverzi SCSI příkazů (které používá rozhraní USB) do ATA, což splňují prakticky všechny disky vyrobené během posledních tří let. Pro provedení bezpečného mazání se hodí Live-System Parted Magic, který je založen na Linuxu. Parted Magic můžete na USB disku vytvořit z prostředí Windows pomocí softwaru UNetbootin. Jakmile jej vytvoříte, stačí nabootovat počítač z USB disku a z prostředí pracovní plochy spustit »Disk Eraser«. V okně, které se objeví, vyberte nejprve možnost »Internal: Secure Erase command« a v dalším okně pak zvolte SSD disk. Objeví se několik varování, která potvrdíte stisknutím tlačítka »OK«. Pokud by došlo k zatuhnutí systému, je nutné opakovat bootování z USB disku. Počítejte s tím, že samotný přepis všech buněk SSD disku pak zabere nějaký čas.

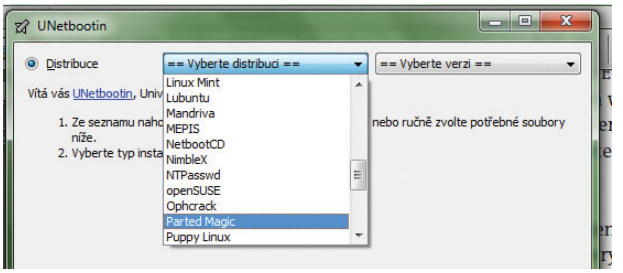
JAK ZJISTIT, ZDA SYSTÉM POUŽÍVÁ TRIM

Aktivaci funkce TRIM ve Windows prověříte tak, že do příkazové řádky zadáte příkaz »fsutil behavior query DisableDeleteNotify«. Pokud je tato funkce aktivní, nahlásí Windows parametr »0«. Aktivovaná funkce TRIM snižuje šance na obnovu dat.



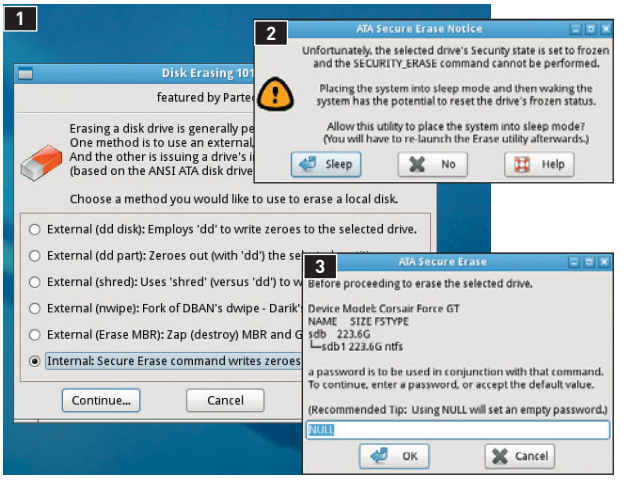
NÁSTROJ NA SPOLEHLIVÉ MAZÁNÍ SSD DISKŮ

Utilita UNetbootin (na našem DVD) dokáže z internetu stáhnout různé distribuce Linuxu a nainstalovat je na bootovatelný USB flash disk. Pro mazání SSD disků doporučujeme použít »Parted Magic«.



PŘEPSÁNÍ SSD DISKŮ POMOCÍ SECURE ERASE

Funkce Disk Eraser, obsažená v Parted Magic, nabízí možnost bezpečného smazání dat Secure Erase **1**. Objeví-li se hlášení o zatuhnutí systému **2**, restartujte počítač stisknutím tlačítka »Sleep«. Poté zadejte heslo **3**, a bezpečné mazání bude pokračovat.



PLACENÁ INZERCE

SMARTPHONY: Objížďka přes PC

Pro Android neexistují žádné vhodné utility na obnovu nechtěně smazaných dat. Je však možné ji provést pomocí počítače.

Každý Android nabízí možnost obnovy do továrního nastavení. Pokud si ale myslíte, že po takovém resetu můžete prodat svůj smartphone nebo tablet a nikdo se k vašim starým datům nedostane, jste na velkém omylu. Data se při resetu sice vymažou, ale nejsou přepsána jinými daty, a proto je tedy lze obnovit.

Zařízení s Androidem mohou používat dva druhy úložišť: interní flashovou paměť a externí paměťové karty. SD karta nepředstavuje z hlediska obnovy či mazání dat problém, prostě ji stačí vložit do čtečky a vzhledem k tomu, že většinou bývá naformátována na systém FAT, lze z s daty pracovat pomocí nástrojů, jako je Recuva nebo Eraser. Data z karet umí obnovovat androidová aplikace Hexacomb Recovery-Lite a pro jejich přepis lze použít Forever Gone. O něco složitější je mazání dat z interní paměti, která bývá naformátována na linuxový systém ext4 a pro přístup k paměťovým buňkám vyžaduje dostatečná administrátorská práva. Proto také nelze provést spolehlivé přemazání dat ve smartphonu či tabletu ani prostřednictvím Windows, ani za pomoci specializovaných androidových aplikací. Existuje ale jedno řešení.

Příprava Androidu na obnovu dat

Připojíte-li k počítači se systémem Windows tablet s Androidem, jako například Google Nexus 7, můžete z něj snadno přenášet data i na něj zapisovat. Kopírování dat probíhá nepřímo pomocí protokolu MFT, ale nástroje určené pro obnovu či mazání dat musí mít přímý přístup k souborovému systému, což je možné pouze prostřednictvím Android Debug Bridge (ADB). Prostřednictvím ADB a kombinace aplikací určených pro Windows i Android je možné přesunout fyzickou image interní paměti tabletu nebo smartphonu do PC, kde ji lze snadno upravit.

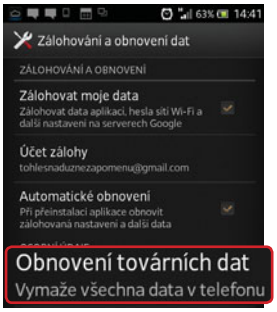
Pro následující operace budete potřebovat administrátorská práva, takže musíte Android nejprve rootovat. Na zařízeních Google to jde snadněji za pomoci toolkitu. Během rootování se do zařízení nakopíruje BusyBox se servisními nástroji. BusyBox si můžete stáhnout i z Obchodu Play. V dalším kroku budeme potřebovat terminálovou aplikaci, jako je např. Android Terminal Emulator. Přihlašte se jako administrátor (»su«) a příkazem »ls« zjistěte, kde se nachází oddíl, se kterým budete pracovat. Na tabletu Nexus 7 je oddíl s uživatelskými daty (UDA) označen jako »mmcblk0p9«. V tabletu či telefonu pak v nabídce »Nastavení | Možnosti pro vývojáře« aktivujte položku »Ladění USB«.

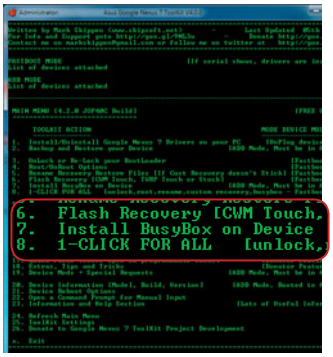
Příprava nástrojů pod Windows

Do kořenového adresáře (C:\) počítače s Windows 7 nainstalujte program Cygwin (ze stránek **cygwin.com**), což je programová knihovna, která dokáže v terminálovém okně spustit linuxové programy kompilované pro Windows. Tyto programy zajistí

OBNOVA DO TOVÁRNÍHO NASTAVENÍ BEZ PŘEPISU DAT

Při resetu smartphonu nebo tabletu s Androidem do továrního nastavení sice smažete všechny aplikace i uživatelská data, ale jelikož nedojde k jejich přepsání jinými daty, je poměrně snadné je znovu obnovit pomocí několika nástrojů pro Linux a Windows.



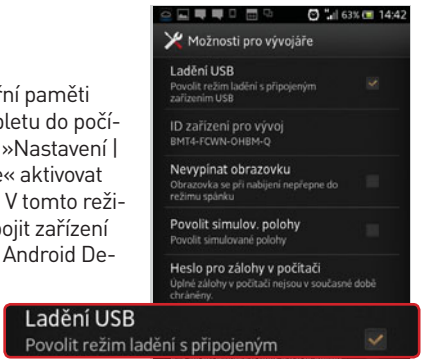


OBNOVA DAT VYŽADUJE ROOTOVÁNÍ

Chcete-li z chytrého telefonu nebo tabletu obnovit omylem smazaná data, budete muset provést root Androidu. Pro zařízení značky Google, jako je například Nexus 7, existují hotové rootkity, které obsahují i užitečné systémové nástroje, jako je BusyBox.

PROPOJENÍ S POČÍTAČEM

Pro přenos dat z vnitřní paměti smartphonu nebo tabletu do počítače je nutné v menu »Nastavení | Možnosti pro vývojáře« aktivovat režim »Ladění USB«. V tomto režimu bude možné propojit zařízení s PC prostřednictvím Android Debug Bridge (ADB).



VYHLEDÁNÍ ODDÍLU S UŽIVATELSKÝMI DATY

Diskový oddíl obsahující uživatelská data můžete najít pomocí terminálové aplikace. Přihlaste se jako administrátor (»su«) a zadejte příkaz pro výpis partic (»ls«). V Nexusu 7 jsou uživatelská data uložena pod označením UDA na diskovém oddílu »mmcblk0p9«.

```
u0_a68@android:/ $ su
u0_a68@android:/ # ls -l /dev/block/platform/sdhci-tegra.3/by-n
lrwxrwxrwx root     root              2012-12-14 14:29 APP ->
lrwxrwxrwx root     root              2012-12-14 14:29 CAC ->
lrwxrwxrwx root     root              2012-12-14 14:29 LNX ->
lrwxrwxrwx root     root              2012-12-14 14:29 MDA ->
lrwxrwxrwx root     root              2012-12-14 14:29 MSC ->
lrwxrwxrwx root     root              2012-12-14 14:29 PER ->
lrwxrwxrwx root     root              2012-12-14 14:29 SOS ->
lrwxrwxrwx root     root              2012-12-14 14:29 UDA ->
lrwxrwxrwx root     root              2012-12-14 14:29 USP ->
u0_a68@android:/ #
```

propojení androidových zařízení s Windows a umožní mezi nimi přenášet data. Cygwin má on-line instalátor (»setup.exe«), pomocí něhož můžete stáhnout jen požadované balíčky. Jakmile se zobrazí výběr balíčků »Select Packages«, zadejte do vyhledávacího okénka »search« výrazy »pv« a »util-linux«. Kliknutím se stav vyhledaných balíčků změní z položky »Default« na »Install«. Poté v pravé horní části aktivujte položku »exp« (starší balíčky), do okénka zadejte »nc« a stáhněte Netcat. Dále budete potřebovat program »adb.exe« a soubory potřebné pro nastavení Cygwin. Dále můžete buď nainstalovat Android Toolkit, nebo můžete do vyhledávače Google zadat dotaz „adb tools“ a stáhnout již rozbalený ADB balíček. Všechny soubory tohoto balíčku překopírujte do adresáře »bin« programu Cygwin a vytvořte si v tomto adresáři složku, do které budete později zálohovat data z tabletu. My jsme tuto složku pojmenovali »nexus«. Nyní budete ještě potřebovat nástroj VdhTool, který můžete stáhnout ze stránek Microsoftu.

Přenos diskového oddílu do PC

Pomocí USB kabelu propojte tablet s počítačem a ujistěte se, že běží ADB. V »bin« adresáři spusťte příkazovou řádku Windows a zadejte do ní příkaz »adb devices«. Zobrazí se číslo, pod kterým je zařízení připojeno. Nyní vytvořte v Cygwin terminálu adb propojení pomocí některého nepoužívaného portu. Příkaz zní takto: »adb forward tcp:5555 tcp:5555«. Následně spusťte na zařízení s Androidem Cygwin »adb shell« a přihlaste se jako »su«. Následujícím příkazem nastavíte přenos datového oddílu »mmcblk0p9« do PC: »/system/xbin/busybox nc -l -p 5555 -e /system/xbin/busybox dd if=/dev/block/mmcblk0p9«. Nyní opět otevřete Cygwin Terminal, aktivujte připojení pomocí adb a přejděte do vytvořeného adresáře »cd /nexus«. Kopírování se spustí pomocí příkazu »nc 127.0.0.1 5555 | pv -i 0.5 > mmcblk0p9.raw«. Takto zkopírujete disk tabletu na disk počítače.

Nástroj VdhTool zkopírujte do stejného adresáře jako RAW data a spusťte jej příkazem »VhdTool.exe /convert mmcblk0p9.raw« (místo mmcblk0p9.raw použijte název vlastního oddílu). Po dokončení operace bude diskový oddíl viditelný pro OS Windows a budete jej moci připojit jako virtuální disk. Připojení nastavíte ve »Správě disků« příkazem »Akce | Připojit virtuální pevný disk«. Pravým tlačítkem myši klikněte na nový diskový oddíl, inicializujte jej a vyberte možnost »Nový jednoduchý svazek«. Nyní můžete oddíl zformátovat – vyberte souborový systém »FAT32«. Kopie diskového oddílu vašeho tabletu je nyní připojena jako disk Windows a pomocí hloubkového skenu programem Recuva z ní můžete obnovit smazané soubory.

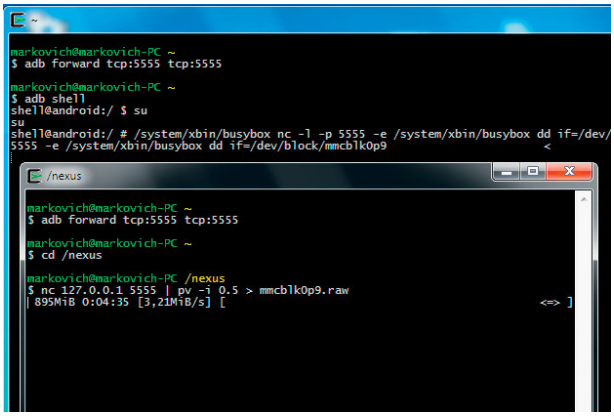
Spolehlivé mazání

Podobnou metodu, kterou jsme použili pro obnovu dat ze zařízení s Androidem, bohužel nelze použít pro bezpečné mazání. Paměťové buňky jsou stejně jako u SSD řízeny řadičem, ale přepsat celý obsah disku pomocí Secure Erase, není možné, protože by se tím neodstranila jen soukromá data uživatele, ale i instalační oddíl Androidu. Pokud tedy plánujete starý smartphone nebo tablet prodat a chcete mít jistotu, že se do světa nedostanou vaše soukromá data, můžeme vám doporučit jedinou, ale jednoduchou a spolehlivou radu. Smažte všechna osobní data a poté kompletně naplňte obsah interního úložiště například tak, že necháte přes noc běžet záznam z videokamery, nebo je zaplňte daty posílanými z počítače. Poté ještě jednou proveďte reset do továrního nastavení.

AUTOR@CHIP.CZ

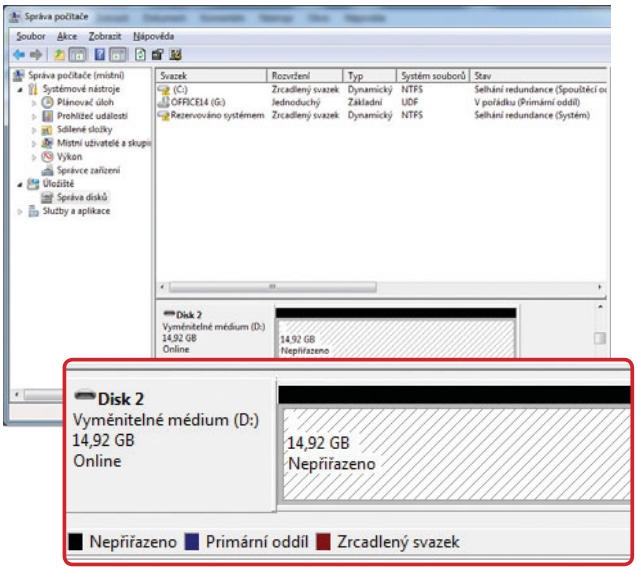
KOPÍROVÁNÍ UDA ODDÍLU DO WINDOWS

V prvním okně konzole Cygwin (na pozadí) propojíte Android zařízení s Windows v režimu ADB. V druhém okně konzole (na popředí) zadáte příkaz ke zkopírování image oddílu uživatelských dat do PC.



PŘIPOJENÍ IMAGE UDA ODDÍLU JAKO DISKOVÉ JEDNOTKY WINDOWS

V okně »Správa | Správa disků« můžete pod Windows 7 připojit kopii oddílu obsahujícího uživatelská data Android zařízení jako virtuální disk a poté s ním pracovat jako s jakoukoliv jinou diskovou jednotkou



OBNOVA SMAZANÝCH DAT POMOCÍ PROGRAMU RECUVA

Díky možnosti hloubkového skenování dokáže Recuva prohledat i přeformátovanou jednotku a obnovit z ní požadovaná data.