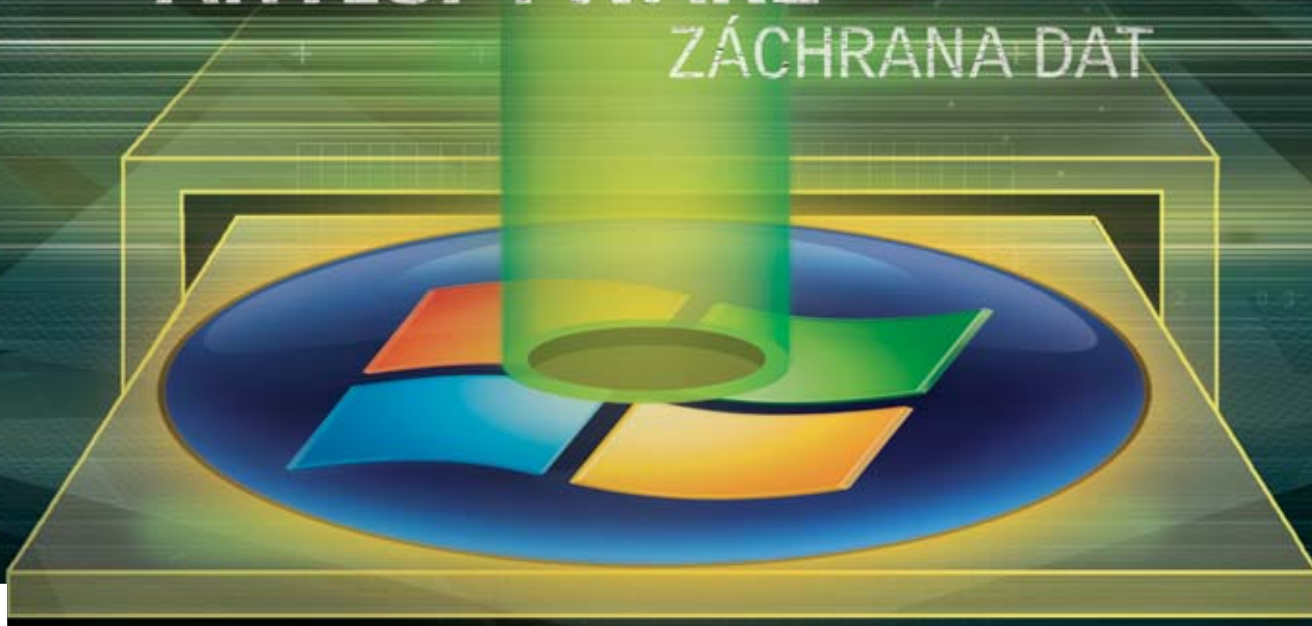


BOOTOVACÍ DISK
ANTIVIR
 DIAGNOSTICKÉ NÁSTROJE
ANTISPYWARE
 ZÁCHRANA DAT



Vista na DVD

Exkluzivně v Chipu: Díky našemu disku „Vista CHIP Edition“ získáte dokonalý záchranný disk – bootovací CD s jádrem z Visty. *Michael Eckstein, Valentin Pletzer, Vratislav Klega, vratislav.klega@chip.cz*

V tomto článku najdete

Tvorba bootovacího záchranného CD

Využití záchranného disku

Odstranění virů a rootkitů

Zadání nového hesla

Je flexibilní, komfortní, bootuje na každém počítači – a zcela zdarma: vaše osobní CD „Vista CHIP Edition“. Tato „Vista CE“ obsahuje bootovací Win PE 2.0 s jádrem z Visty a další užitečné

nástroje. Výhodou je to, že jádro Visty nemá problém se současným hardwarem jakéhokoliv počítače a bootuje nezávisle na nainstalovaném operačním systému. Originální instalační DVD Windows Vista nebudete potřebovat!

Poděkování náleží i Microsoftu. Softwarový gigant nabízí bezplatné stažení a volné používání všeho, co budete potřebovat. A navíc nebudete muset nic stahovat: vše najdete na příloženém DVD. Jeden skript pro freewareový WinBuilder jsme naprogramovali sami

a z microsoftské nabídky jsme tak vytvořili osobní záchranné CD či DVD. Podle toho, jaký software chcete na svých mobilních Windows používat, může mít balík třeba jen 200 MB, nebo až 4,5 GB. Ani programy jako Open Office, Firefox či PDF Reader nepracují na tomto systému s chybami.

„Vista CE“ je však především optimalizovaný záchranný disk, kterému je jedno, že na vašem počítači běží třeba XP. Nouzový disk s Win PE 2.0 je mnohem lepší než LiveXP nebo třeba Knoppix. XP mají →



Najdete na ChipDVD Microsoft WAIK freeware ■ WinBuilder freeware ■ Deamon Tools freeware



ZÁCHRANNÉ CD NA BÁZI VISTY

S naším výjimečným skriptem Chip-WinBuilder na přiloženém DVD vytvoříte bootovací disk s jádrem z Visty.

Pro své bootovací CD budete potřebovat Windows Automated Installation Kit (WAIK). Ten si můžete stáhnout ze stránek Microsoftu, jelikož má velikost téměř 1 GB, naleznete jej i na Chip DVD.

1 Příprava Windows AIK-DVD

Microsoft distribuuje WAIK jen jako DVD image. Proto je třeba soubor „vista_6000.16386.061101-2205-LRMAIK_EN.img“ buď vypálit na DVD, nebo nainstalovat z Chip DVD Deamon Tools a vytvořit virtuální jednotku. Pomocí virtuální jednotky budete moci k image disku přistupovat stejně jednoduše, jako by byl vypálen na DVD. Nainstalujte Deamon Tools, v System tray se objeví nová ikona se symbolem blesku. Klikněte na ikonu pravým tlačítkem myši a zvolte „Virtual CD/CD | Device O: [E:] No Media | Mount Image“. Otevře se nové okno. V řádku „Soubory typu:“ zvolte poslední položku – „All files *.*“, naleznete zmíněný image disku a potvrďte. Za pár sekund se k jednotce přiřadí obraz disku.

Upozornění: Deamon Tools obsahují Adware WhenU. Během instalace však můžete instalaci tohoto škůdce zaká-

zat. Ten se pak nenainstaluje a nástroj funguje nezávisle na jeho přítomnosti.

2 Instalace WAIK/MSXM

Jakmile se WAIK-DVD „přimountuje“ do systému, automaticky se spustí startovací okno „Windows Vista – Windows Automated Installation Kit“. Pokud se tak nestane, otevřete „Tento počítač“, pravým tlačítkem myši klikněte na virtuální jednotku a zvolte „Přehrát automaticky“. Pracujete-li v XP, spusťte „MSXML 6.0 Setup“. Je to předposlední položka v levém menu spuštěného okna. Ve Vistě není třeba tento balík instalovat. Poté klikněte na „Windows AIK Setup“. MSXML je microsoftská

knihovna ke čtení a zápisu XML souborů a WAIK ji potřebuje ke své činnosti. S instalací pomůže průvodce.

3 Instalace WinBuilderu

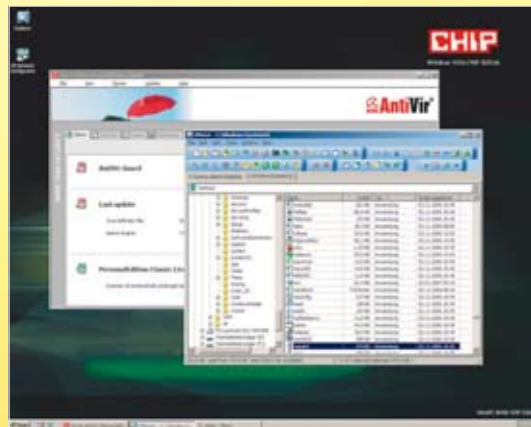
Nyní je třeba připravit WinBuilder, pomocí něhož si „Vista CE“ uzpůsobíte na míru. Z Chip DVD rozpakujte soubor „WinBuilder.zip“, například do složky „C:\Temp“. Poté spusťte soubor „WinBuilder.exe“ a vyberte záložku „Paths“. V řádku „Source directory“ klikněte na symbol složky a zvolte AIK – standardně v „C:\Program Files\Windows AIK“. Do řádku „ISO-File“ zadejte „C:\Temp\ISOfile\VistaCE.ISO“. To je místo, kam se uloží výsledný image.

4 Přidání vlastních nástrojů

Náš balík obsahuje nejdůležitější freewareové programy. Pokud byste však něco postrádali, můžete si skript sami upravit, buď přímo ve složce „WinBuilder\Projects\VistaCE_CHIP_Edition“, nebo pomocí programu WinBuilder.

5 Dokončení

Zvolte záložku „Scripts“ a klikněte na „VistaCE CHIP Edition“. Nyní klikněte na tlačítko „Play“. Spustí se proces, na jehož konci bude vytvořen ISO image záchranného disku. Celý proces trvá delší dobu. Po dokončení vypalte obraz souboru na CD/DVD.



PRAKTICKÉ: Pod „Vista CHIP Edition“ funguje řada užitečných nástrojů, jako je AntiVir nebo XPlorer.

→ problém s novými PC, ve kterých jsou SATA disky, a Knoppix si nerozumí se souborovým systémem používaným ve Windows – NTFS.

Jak záchranné CD/DVD vytvořit, to se dočtete v rámečku. Jak nástroje z našeho balíku správně použít, to se dočtete na následujících stránkách.

Příprava systému

„CHIP Edition“ startuje ve standardním rozlišení 800 x 600 pixelů a s 16bitovou barevnou hloubkou. Po nabootování si tedy nastavte takové rozlišení, které nejlépe vyhovuje vašemu monitoru. Otevřete „Start | System | Screen Resolution“ a zvol-

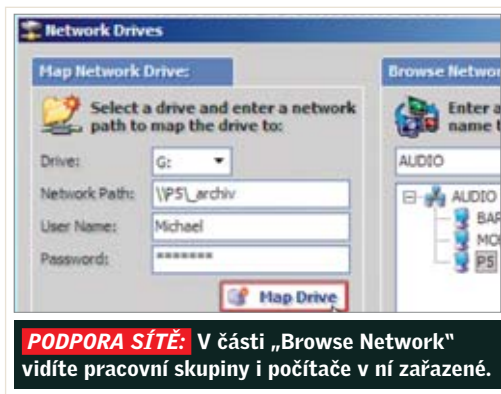
te požadované rozlišení. Ideální barevná hloubka je 32 bitů.

Nastavení sítě

Během bootování Win CE automaticky rozpoznají síťové karty v počítači a aktivují DHCP klienta, aby dostaly IP adresu. Toto nastavení však můžete později změnit v menu „Start | Programs | Network Tools | PENetCfɡ“ nebo pomocí ikony „PENetCfɡ“ na desktopu. V následujícím okně klikněte na „Network Identification“. Do políčka „Computer Name“ zadejte jméno počítače v síti a potvrďte kliknutím na „Set“. Do políčka označeného „Workgroups“ ještě zadejte jméno pracovní sku-

piny, ve které se počítač nachází. I zde je nutné nastavení potvrdit kliknutím na „Set“. Tlačítkem „Apply“ provedené změny aktivujete. Síťová karta začne v síti vyhledávat DHCP server, který by jí přidělil IP adresu. Tu většinou přiděluje ADSL router nebo vaše domácí brána.

Pokud nemáte v síti dynamické přidělování adres, klikněte na „IP-Adresses“ a zde můžete zadat vlastní pevnou IP adresu, například 192.168.1.10, a samozřejmě masku své podsítě, standardně 255.255.255.0. Pokud adresu neznáte, je nejlepší podívat se na konfiguraci jiného počítače v síti a podle něj nastavení opsat. IP adresa musí být samozřejmě unikátní. →



→ Abyste mohli ve své síti sdílet soubory, klikněte v PE Network Configurator na „File Sharing“ a vytvořte administrátorské konto včetně hesla. Poté přes „Start Sharing“ zvolte soubory ke sdílení a zavřete okno. Nasdílené soubory můžete zkontrolovat přes tlačítko „Network Drives“. Modrá ikona plus zobrazí počítače v pracovní skupině.

Ve stejném okně můžete také připojené síťové disky namapovat jako jednotky do systému. K tomu zvolte nalevo od „Drive“ písmeno jednotky a klikněte na „Network Path“. Poté zvolte odpovídající cestu. Nakonec ještě zadejte „User Name“ a „Password“ a klikněte na „Map Drive“. Nyní může jakákoliv aplikace přistupovat k této jednotce a pracovat se soubory.

Hledání a odstraňování virů

AntiVir

Jako nástroj pro odstraňování virů jsme zvolili AntiVir od společnosti Avira. Spusťte jej pomocí „Start | Programs | Antivirus Tools“. Klikněte na „Configuration“, abyste si přizpůsobili základní nastavení. Ve standardně spouštěném „Expert Mode“ nastavte, které soubory se budou kontrolovat. Otevřete stromovou strukturu „Scanner | Scan“ a zvolte „All files“. Význam má i aktivace volby „Additional Setting“. Tím bude antivir prohledávat také bootsektor a operační paměť. Dodatečně můžete také nastavit, aby program testoval i archivy. Zvolte proto „Archives“. Kliknutím na „OK“ se konfigurace potvrdí.

V hlavním okně klikněte na „Scanner“ a otevřete položku „Manual Selection“. Označte všechny své pevné disky, standardně se jedná o disk „C:\“. Klikněte na ikonu lupy a antivir ihned začne pracovat.

CD a v programu Rootkitty klikněte na „PE-Scan“. V „Compare“ pak vyjdou na povrch rozdíly. Pokud nástroj najde při PE-Scanu soubory, které byly pod Windows skryté, vypíše je.

Odpusťte si urychlené klikání na „Delete checked Item“, místo toho přesuňte tyto soubory do dočasné složky a vyzkoušejte, zda váš systém bez problémů bootuje a pracuje.

Spybot S&D

Tento program je evergreenem v oblasti antimalwarových nástrojů. Jeho použití je velice jednoduché. Zvolte „Language | Česky“, tím se celý program přepne do češtiny. Poté klikněte na tlačítko „Zkontrolovat“. Ve spodním řádku vidíte, co program právě provádí, které oblasti kontroluje. Po dokončení kontroly stačí kliknout na tlačítko „Opravit vybrané problémy“.

Ad-Aware SE

Dalším nástrojem pro odstranění malwaru je Ad-Aware. Spusťte program a zvolte „User-Profil“. Poté stiskněte v hlavním okně „Start“, v dalším kroku zvolte „Perform Full System Scan“ a samotný test spusťte kliknutím na „Next“.

Rootkitty

S tímto nástrojem budete obávaným rootkitům na stopě. Postup je bohužel trochu složitější. Nejprve nabootujte Windows z pevného disku a spusťte program Rootkitty. Poté, co se nástroj spustí, zadejte vedle „Path to Scan“ cestu k systémové partition. Kliknutím na „Win-Scan“ spustíte hledání, jehož výsledek zapiše nástroj do souboru „Windows-Files.txt“. Poté nabootujte ze záchranného

Remote RegEdit

Špatný klíč v registrech systému již nejednou způsobil řadě uživatelů problémy. S nástrojem „Remote RegEdit“, který se nachází přímo na ploše, můžete registry přímo editovat. V prvním kroku prohledává nástroj programy, které jsou na počítači nainstalované, a nabízí vám volbu, zda chcete provádět úpravy pro váš profil, nebo pro jiné konto v systému. Vyberte konto, které již není v perfektní kondici, a klikněte na „OK“. Nyní se otevře editor registrů, ve kterém můžete opravit libovolný klíč systému, který již nelze spustit.

Diagnóza a správa hardwaru

Advanced PCI Info

Při hledání vhodného ovladače pro cizí počítač je praktické, pokud přesně znáte typ PCI/AGP karty. Tento nástroj vypíše všechny nainstalované komponenty, výrobce zařízení, identifikační číslo hardwaru, obsazenou sběrnici atd. Pro použití zvolte „IRQ | Routing Table“, na mnoha systémech to však vede k pádu systému.

HD Tune

Pomocí tohoto nástroje detailně analyzujete pevný disk, odhalíte chyby a zkontrolujete kondici. V horním řádku programu zvolte disk, který chcete testovat, vyberte záložku „Error Scan“ a klikněte na tlačítko „Start“. Vadné sektory označí nástroj jako červený obdélník. Pokud je v oblasti více červených obdélníků, bude nutné použít k obnově dat specializovaný nástroj (např. RawCopy) a poté se disku rychle zbavit.

Disk Check

Tento nástroj se velice detailně podívá na váš disk. Po spuštění vyberte →

ANTIVIR: Freewareový nástroj od Aviry vyhledává škodlivé kódy v celém počítači.

AD-AWARE: S nastavením „Perform Full System scan“ postupuje nástroj při hledání škůdců obzvláště pečlivě.

→ v „Disk Type“ položku „Hard Disk“ a jako „Disk Drive“ zvolte jednotku „C:\“. Kliknutím na tlačítko „Start“ začne test, který může podle velikosti disku trvat velice dlouho. V polích pod „Statistics“ naleznete výsledky programu. Kliknete-li na text pravým tlačítkem myši, můžete jej uložit do souboru.

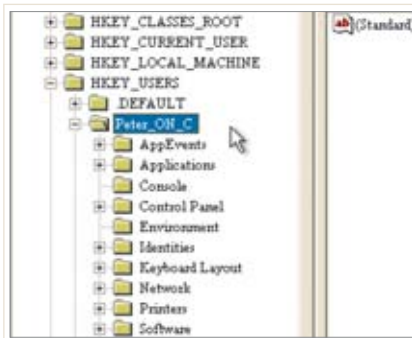
Zabezpečení a záchrana souborů



XPlorer

Jako základ našeho záchraného CD nevybral Microsoft žádný Explorer. To však není žádný problém – alternativní správce souborů XPlorer je stejně mnohem praktičtější. Pokud spustíte systém a nainstalujete síť tak, jak jsme popsali výše, můžete prostřednictvím tohoto (ale i jiného) souborového manažeru přistupovat k partition Windows, i když Windows už nebylo možné spustit. Pak je možné soubory zálohovat na jiný počítač.

Spusťte XPlorer a v navigačním okně se dostanete k těm souborům, které budete chtít zálohovat. Stisknutím [Ctrl] + [T] změníte vzhled na běžnější, který znáte z Explorera. Zkopírování můžete provést jednoduše přetažením.



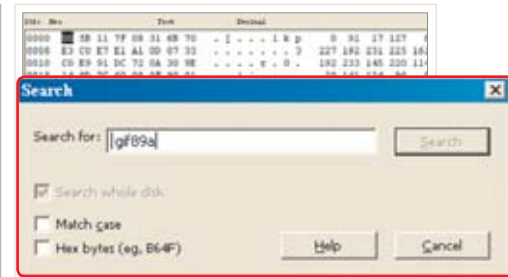
REMOTE REGEDIT: Pomocí tohoto nástroje můžete editovat registry i z jiné session Windows.

V případě potřeby je možné otevřít další kopii programu.



Handy Recover

Omylem smazaný, virem odstraněný, softwarovou chybou ztracený soubor – vše lze však obnovit, pokud máte k dispozici nástroj Handy Recovery, který podporuje souborové systémy FAT16/32, NTFS i NTFS5. Zvolte „Start | Programs | Data Recovery Tools“. Pod tlačítkem „Analyze“ zvolte jednotku, ze které chcete data obnovit, standardně je zvolen „Local Disk C:\“. Samot-



DISKINVESTIGATOR: Pokud na svém disku hledáte nějaký řetězec, tento nástroj vám jej pomůže najít.

nou analýzu, která trvá jen pár sekund, spusťte kliknutím na „Analyze“.

Smazané soubory a složky, které budete chtít obnovit, označte v nástroji červeným křížkem. Poté klikněte na tlačítko „Recover“. V následujícím kroku vyberete, do které složky chcete obnovené soubory uložit. Na přání se Handy Recover snaží obnovit i adresářovou strukturu.



Unstoppable Copier

Toto je tak říkajíc Terminátor mezi kopírovacími programy. Zlatý hřeb: →



ZÁCHRANNÉ CD S WINDOWS XP

Pomocí LiveXP a Windows XP si vytvoříte plnohodnotné bootovací CD na bázi Windows XP – flexibilní alternativu pro skoro všechna přání.

Záchranné CD s Windows XP je alternativou k našemu disku s jádrem z Visty. Toto řešení sice není tak vyspělé, ale je mnohem více flexibilní. Díky velkému množství uživatelů existuje řada bezplatných řešení různých situací. Vše naleznete na stránce www.boot-land.net. K přípravě LiveXP budete potřebovat instalační CD Windows XP, které obsahuje soubory nutné k vytvoření projektu. Navíc díky jednoduchému nástroji budete mít k dispozici aktuální obraz disku. Spusťte WinBuilder, vyberte záložku „Update Center“, označte všechny položky, které chcete aktualizovat, a klikněte na „Download selected“.

1 Instalace

Spusťte WinBuilder z adresáře „C:\Temp“ (viz předchozí rámeček), v záložce „Scripts“ klikněte na „XP Live CD“ a zvolte záložku „Paths“. V řádku „Source directory“ vyberte adresář i386 z instalačního

CD Windows XP, např. „D:\i386“. Nyní se vraťte zpět na záložku „Scripts“ a ujistěte se, že pod „XP Live CD“ jsou zaškrtnuty všechny položky, tedy „Basic“, „Tweaks“,



LIVEXP: Velmi malé, ale výkonné záchranné CD je možné automaticky aktualizovat pomocí funkce „Update center“.

„Apps“, „Drivers“ a „Finish“. Skripty z položky „Tools“ budete potřebovat později k vypálení. Mnoho skriptů dovoluje expertní nastavení, to však pro běh LiveXP nebudete potřebovat. Klikněte proto na tlačítko „Play“ – tím dojde k automatickému zpracování skriptů a k vytvoření ISO image disku, který bude připraven k vypálení. Podle výkonu vašeho počítače bude vytvoření trvat asi 10 minut.

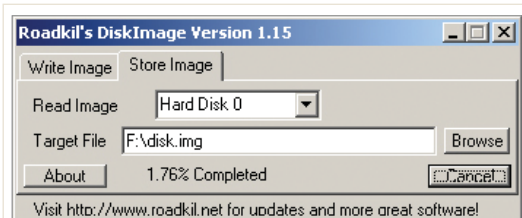
2 Vypálení LiveXP

ISO image se nyní nachází v adresáři „ISO“ spolu s WinBuilderem. Soubor se jmenuje „LiveXP.ISO“. Vypalte image na disk, například pomocí Nera nebo pomocí skriptu „BurnCD“, který naleznete v položce „Tools“. Projekt můžete vypálit i jako bootovací DVD, to je však zbytečné, protože velikost disku je asi 70 MB. Pokud nebudete na disk přidávat aplikace, dostanete se dokonce na 31 MB.

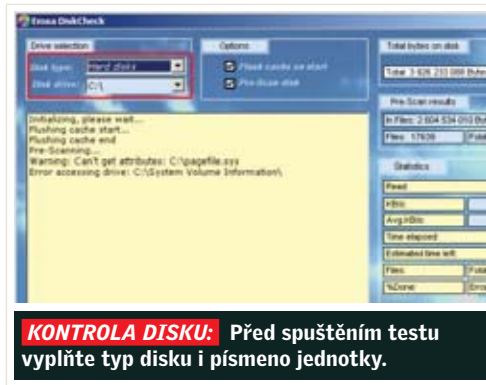
nástroj hned během kopírování kontroluje soubory a poškozené nahrává znovu. Stačí zvolit zdroj a cíl kopírování a zatrhnout položku „Include Sub Folders“. Dále zvolte záložku „Settings“. Zde můžete aktivovat vytváření logu a také navolit kvalitu kopírování. Jezdce přesuňte úplně vlevo k nápisu „Best Data Recovery“. Rovněž zatrhněte volbu „Auto Skip Damaged Files“. Tím zajistíte, že pokud je soubor opravdu nečitelný a neopravitelný, nebude se jej program snažit do nekonečna opravovat. Kliknutím na „Copy“ na úvodní stránce se spustí kopírovací proces.

DiskImage

Tento nástroj převádí obsah pevného disku do image souboru. Ovládání programu je velice jednoduché. Na záložce „Store Image“ zvolte zdrojovou partition a určete cíl, kam image uložit. Toto místo může být klidně i na síti. Kliknutím na „Go“ se spustí proces vytváření image. Buďte však trpěliví, čím větší disk, tím déle kopírovací proces trvá. Program zvládá i proces opačný, stačí zvolit záložku „Write Image“. Pak zvolte odpovídající image, vyberte partition a opět klikněte na „Go“.

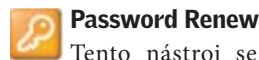


DISKIMAGE: Do řádku „Target File“ v záložce „Store Image“ zadejte místo, kam má být image partition uložena.



KONTROLA DISKU: Před spuštěním testu vyplňte typ disku i písmeno jednotky.

Obnovení hesla



Password Renew

Tento nástroj se specializuje na heslo do Windows. Je nápomocen, pokud chcete kontu ve Windows nastavit nové heslo. Klikněte na „Renew existing user password“. V poli „Account“ zvolte toho uživatele, kterému chcete nové heslo nastavit. Poté zadejte nové heslo a potvrďte.

Pomocí „Create new Administrator user“ vytvoříte nové uživatelské konto s administrátorskými právy. Stačí zadat jméno, heslo a potvrdit. Funkce „Turn existing user to Administrator“ nastaví zvolenému uživateli administrátorská práva. Po všech potřebných nastaveních klikněte na „Install“. Tím se aktivují všechny provedené změny.

UPOZORNĚNÍ: Stránce „Advanced task“ se velkým obloukem vyhněte: snadno byste mohli svůj systém vyřadit z provozu.

TIP NA ZÁVĚR: Záchraně CD vytvořte co nejdříve. Až budou vaše Windows nefunkční, bude pozdě vytvářet záchraný disk.

M. Eckstein, V. Klega

LIVE CD INTERAKTIVNĚ

„CHIP Edition“ je jedním z nejlepších live a záchraných CD. Nic ovšem není dokonalé a stejně jako záchrané CD „BartPE“ (Windows XP) nebo „Knoppix“ (Linux) se bude dále vyvíjet. K tomu je třeba vyslechnout názory komunity – tedy i vás.

Užitečná fóra

Pokud budete mít připomínku, návrh na vylepšení, dokonalejší skript nebo třeba jen dotaz, navštivte naši vlastní diskusi na www.chip.cz/diskuze.

Skvělé je i fórum na stránce <http://www.boot-land.net/forums/Vista-PE-f51.html>. V anglickém jazyce zde naleznete řadu návodů, vysvětlení i řešení nejrůznějších problémů.

Vývoj vlastních plug-inů

Doplnění programů a nástrojů do našeho projektu je velice jednoduché, neboť skripty jsou psány velice jednoduše a snadno jim porozumíte. Připomínají BAT soubory z DOS, jsou v textovém formátu.

Velice dobrou dokumentaci naleznete na Wiki stránce programu WinBuilder, konkrétně na www.boot-land.net/wiki. Řešením je prozkoumat naše vlastní skripty a na jejich základě pochopit strukturu. Ve stylu open-source dáváme naše skripty k dispozici na Chip DVD. Nejsou však ke komerčnímu použití, jen pro volné užití.